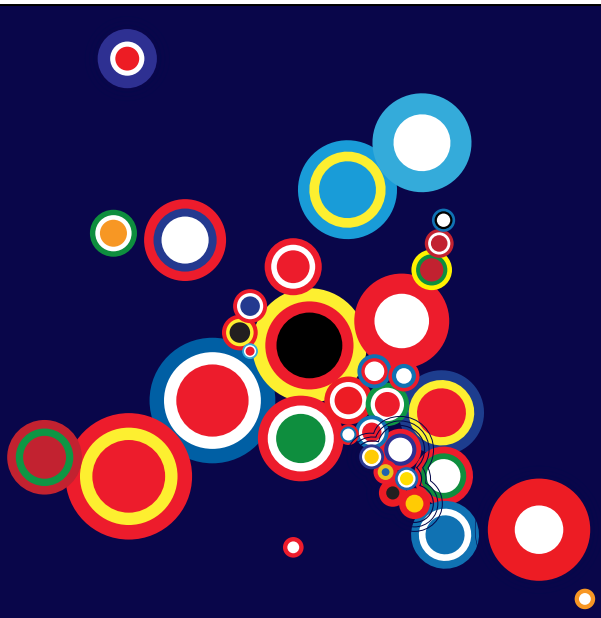
INSTRUMENT FOR PRE-ACCESSION ASSISTANCE (IPA II) 2014-2020

MULTI-COUNTRY

Cooperation on Cybercrime



Action Summary

The objective of the Action is to strengthen the capacity of authorities in Western Balkans and Turkey to search, seize and confiscate cybercrime proceeds and prevent money laundering on the Internet.

This is to be achieved through seven expected results related to public reporting systems, legislation, interagency cooperation, risk management and guidelines for financial sector entities, public/private information sharing, judicial training and international cooperation.

Action Identification	
Programme Title	IPA II Multi-country action programme 2014
Action Title	**Cooperation on Cybercrime: targeting crime proceeds on the Internet (CyberProceeds@IPA)**
Action Reference	IPA 2014/031-603.05 /MC/cybercrime
Sector Information	
ELARG Sectors	Rule of law and fundamental rights
DAC Sector	15113
Budget	
Total cost (VAT excluded)[1]	EUR 5.5 million
EU contribution	EUR 5 million
Management and Implementation	
Method of implementation	Direct management
Direct management: **ELARG unit in charge**	ELARG D.3
Implementation responsibilities	At the Council of Europe: Cybercrime Programme Office of the Council of Europe (C-PROC) in Bucharest, Romania
Location	
Zone benefiting from the action	Western Balkans and Turkey
Specific implementation area(s)	Albania, Bosnia and Herzegovina, Montenegro, Serbia, the former Yugoslav Republic of Macedonia, Turkey and Kosovo*
Timeline	
Deadline for conclusion of the Financing Agreement	*N.A.*
Contracting deadline	*31 December 2015*
End of operational implementation period	*31 December 2019*

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

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

1. RATIONALE

PROBLEM AND STAKEHOLDER ANALYSIS

Cybercrime and crime proceeds

Worldwide, most cybercrime reported and investigated by criminal justice authorities is related to different types of fraud and other offences aimed at obtaining illegal economic benefits. Vast amounts of crime proceeds are thus generated – and often laundered – on the Internet and through the use of ICT. ICT are exploited for a wide range of serious and organised crime activity with a "dynamic relationship between online and off-line organised crime[2]." This is also the case for the Western Balkans and Turkey.

Major standards regarding cybercrime and crime proceeds include the Budapest Convention on Cybercrime (CETS 185)[3] and the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS 198)[4] of the Council of Europe (CoE). Both treaties and the related assessment or monitoring mechanisms are most relevant for countries covered by this Action. In fact, the beneficiaries are expected to comply with the *EU acquis* and relevant Council of Europe conventions and standards.

The Action will be part of a new framework for cooperation between the Commission and the CoE on human rights, democracy and rule of law for the period 2014-2020. The Commission and the CoE signed an agreement in April 2014 that will enable the two organisations to work together in a more strategic and result-focused manner not only in the beneficiaries, but also in the neighbourhood regions based on the Council of Europe's binding international conventions, monitoring bodies and assistance programmes.

In March 2012, the Council of Europe adopted a typology study with a detailed analysis and a set of recommendations on how to address criminal money flows on the Internet, among other things, by making use of these treaties.[5] Council of Europe is the only organisation performing such an analysis worldwide.

The issue of criminal money flows was furthermore one of the components of the joint EU/CoE project CyberCrime@IPA[6]. Activities included assessments of the current situation and of needs in the beneficiary countries[7]. Some of these activities informed the above typology study.

According to the analyses carried out so far and information received from counterpart institutions in the region, key challenges in this region include:

- Public authorities have only limited information on threats and trends regarding criminal money flows on the Internet in relation to online fraud and other types of cybercrime. Public reporting mechanisms are not yet in place. In most beneficiaries, criminal justice statistics are not available on cybercrime and related fraud.

[2] See EUROPOL report on Internet facilitated organised crime (2011)
https://www.europol.europa.eu/sites/default/files/publications/iocta_0.pdf
and the EU Serious and Organised Crime Threat Assessment 2013
https://www.europol.europa.eu/sites/default/files/publications/socta2013.pdf

[3] Albania, Bosnia and Herzegovina, Montenegro, Serbia and The former Yugoslav Republic of Macedonia are Parties. Turkey has not yet ratified it. The Cybercrime Convention Committee (T-CY) assesses implementation of this treaty (www.coe.int/tcy).

[4] Albania, Bosnia and Herzegovina, Montenegro, Serbia and The former Yugoslav Republic of Macedonia are Parties. These States are monitored by MONEYVAL (www.coe.int/moneyval). Turkey has signed it.

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

[6] The project IPA 2010/248-578 started in November 2010 and came to an end in June 2013.

[7] http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy%20project%20balkan/2467_Assess_Rep%20v51_public.pdf
http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/CyberCrime@EAP/2523_2467_IWS_actrep%20Kyiv%2027-29%20FEB_%20V5a.pdf

- While legislation on cybercrime and on money laundering was strengthened considerably in recent years, in most beneficiaries further reforms may be needed to allow for financial investigations and confiscation of cybercrime proceeds. Compliance with data protection requirements, in particular in relation to international cooperation, remains a major challenge.
- Measures against cybercrime and related criminal money flows require interagency cooperation, in particular between specialised cybercrime units, financial investigation/economic crime units and financial intelligence units. Protocols or procedures on interagency cooperation need to be established to ensure that cybercrime investigations are systematically accompanied by parallel financial investigations.
- Financial sector entities obliged to report suspicious transactions may need additional guidelines to assess risks, and prevent and control criminal money flows.
- Public/private information sharing would need to be enhanced to prevent threats and enhance knowledge of threats and trends.
- The control of cybercrime and the confiscation of related crime proceeds will only be possible if judges are sufficiently trained. It will be essential that training academies incorporate modules on cybercrime, online fraud and electronic evidence into their curricula so that over time the broadest possible number of judges and prosecutors are trained.
- Cybercrime, electronic evidence and criminal money flows are transnational in nature. Enhanced and efficient regional and international cooperation will be essential to secure volatile electronic evidence.

The topic remains on the agenda of governments of South-Eastern Europe. In May 2014, the Ministers of Justice and Interior of states participating in the SEECP (South-East European Cooperation Process) adopted a joint declaration agreeing to:

> "(…) strengthen the capacity of criminal justice authorities to address the challenges of cybercrime and electronic evidence, including the confiscation of proceeds from online crime; to this effect seek partnerships with the Cybercrime Programme Office of the Council of Europe in Bucharest, Romania."

The Action is to address these challenges and to assist countries in the implementation of recommendations made. It will help address the gaps and challenges identified with respect to cybercrime and related criminal money flows. It will build on the work carried out so far, including in particular under the CyberCrime@IPA project.

Organised crime and cybercrime

It should be underlined that cybercrime and electronic evidence are transversal challenges. Most offences – in particular serious and organised crime – involve information and communication technologies (ICT) and thus evidence on a computer system in one way or the other. Law enforcement and criminal justice authorities need to be able to deal with electronic evidence. Any investigator, prosecutor or judge will sooner or later be confronted with such 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;
- create vulnerabilities at all levels of society and the economy that are exploited by criminal groups;
- facilitate logistics, anonymity and reduce risks of criminal groups;
- are used for money laundering;
- facilitate global outreach of criminal groups;

- 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.

RELEVANCE WITH THE IPA II MULTI-COUNTRY STRATEGY PAPER AND OTHER KEY REFERENCES

Specific objectives of IPA II include the fight against organised crime and thematic priorities for assistance include establishing independent, accountable and efficient judicial systems and developing effective tools to prevent and fight organised crime.

The IPA II Multi-country Indicative Strategy Paper (MCSP) 2014-2020[8] (hereafter referred to as Strategy Paper) notes that in the sector Rule of Law and Fundamental Rights, most beneficiaries need in particular to join forces and cooperate to fight organised crime. This involves strengthening cooperation with international law enforcement organisations operating in criminal justice, police investigations and witness protection, thus enabling effective exchange of information and evidence during investigations and prosecutions. There is a need of close cooperation and coordination with relevant EU agencies, as well as with EU Member States and international organisations.

In its needs analysis the Strategy Paper also notes that the beneficiaries are expected to build up their administrative, institutional and judicial capacities for the adoption and correct implementation of the Union *acquis*, including compliance with relevant Council of Europe conventions and standards, such as the Convention on Cybercrime, also known as the Budapest Convention.[9]

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).
- 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.

With regard to international standards on money laundering and crime proceeds, the 2005 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism ("the Warsaw Convention", CETS 198) is of relevance for countries covered by IPA II. The "Warsaw Convention", was opened for signature on 16 May 2005 and came into force on 1 May 2008. The Convention covers, among other things, confiscation (article 3), investigative and provisional measures (article 4), freezing, seizure and confiscation (article 5), management of frozen or seized property (article 6) and investigate powers and techniques (article 7), the criminalisation of laundering offences (article 9), the establishment of financial intelligence units, financial intelligence units (FIUs) (article 12), preventive measures (article 13), the postponement of domestic suspicious transactions, international requests for information on bank accounts (article 17),

[8] C(2014) 4293, 30.06.2014

[9] As indicated above, Albania, Bosnia and Herzegovina, Montenegro, Serbia and the former Yugoslav Republic of Macedonia are Parties. Turkey has not yet ratified it.

on banking transactions (article 18), for monitoring of banking transactions (article 19), for the execution of provisional measures (articles 21 and 22) and for confiscation (articles 23 and 24) and co-operation between FIUs (article 46) 10.

While the international community has diverse views on the governance of the Internet and in particular with regard to matters concerning security in cyberspace, there is broad agreement on the need to enhance capacity building as the most effective way ahead to address cybercrime and strengthen cybersecurity. The Action is thus in line with the "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace"[11] which – among other things – calls for:

- "global capacity-building in third countries … to prevent and counter cyber threats, including … cybercrime and cyber terrorism…"
- Strong and effective legislation on the basis of the Budapest Convention (the Convention is a binding international treaty that provides an effective framework for the adoption of national legislation).

LESSONS LEARNED AND LINK TO PREVIOUS FINANCIAL ASSISTANCE

Operational activities: According to the various evaluations and IPA 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)" and this Action, programme coordination and involvement of the Beneficiaries was ensured at the identification phase of the Action.

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 should 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.[12]

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,

[10] As indicated above, Albania, Bosnia and Herzegovina, Montenegro, Serbia and the former Yugoslav Republic of Macedonia are Parties. Turkey has signed it.

11 http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

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

by 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 Action 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"[13].

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

2. INTERVENTION LOGIC

LOGICAL FRAMEWORK MATRIX

OVERALL OBJECTIVE	OBJECTIVELY VERIFIABLE INDICATORS (OVI)	SOURCES OF VERIFICATION	
To contribute to the strengthening of the rule of law through the fight against corruption and organised crime.[1]	- Number of information requests addressed to another country linked to a criminal investigation - Government effectiveness (Rank)		
SPECIFIC OBJECTIVE	**OBJECTIVELY VERIFIABLE INDICATORS (OVI)**	**SOURCES OF VERIFICATION**	**ASSUMPTIONS**
To strengthen the capacity of authorities in the beneficiaries to search, seize and confiscate cybercrime proceeds and prevent money laundering on the Internet.	- Extent of financial investigations and prosecutions related to cybercrime and proceeds from online crime. - Level of compliance with international standards on cybercrime, money laundering and the search, seizure and confiscation of proceeds from crime (Council of Europe Conventions ETS 185 and 198).	- Performance review workshops carried out - Initial situation report at the outset of the Action to establish baseline data - Assessment report towards the end of the Action to determine progress made - MONEYVAL and T-CY reports	The ability to carry out financial investigations and confiscate proceeds from online crime essential for the rule of law and fight against organised crime.
RESULTS	**OBJECTIVELY VERIFIABLE INDICATORS (OVI)**	**SOURCES OF VERIFICATION**	**ASSUMPTIONS**
Result 1: Public reporting systems (with preventive functions) on online fraud and other cybercrime established in each beneficiary.	- Presence and performance of public reporting mechanisms in terms of receiving and processing reports and publishing analyses in each beneficiary.	- Performance review workshops carried out under the Action - Reports published by reporting mechanism	Public reporting mechanism will inform authorities on cybercrime and related fraud. This will provide leads for investigations and overall intelligence on threats and trends.

[1] http://ec.europa.eu/enlargement/pdf/financial_assistance/ipa/2014/231-2014_ipa-2-reg.pdf
Article 2.1(a) (v) of the REGULATION (EU) No 231/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 March 2014 establishing an Instrument for Pre-accession Assistance (IPA II)

Result 2: Legislation strengthened regarding the search, seizure and confiscation of cybercrime proceeds and the prevention of money laundering on the Internet in line with data protection requirements.	- Number and quality of relevant draft amendments to laws made available to bring legal frameworks of each beneficiary in line with international standards.	- Performance review workshops carried out under the Action. - Reports by MONEYVAL and Cybercrime Convention Committee (T-CY).	Draft amendments are adopted by Parliaments. A clear legal basis will allow for criminal justice action that meets rule of law requirements.
Result 3: Cybercrime units, financial investigators and financial intelligence units cooperate with each other at the domestic level in the search, seizure and confiscation of online crime proceeds.	- Increase in the number and degree of relevance of cybercrime investigations in each beneficiary accompanied by parallel financial investigations.	- Performance review workshops carried out under the Action. - Reports by cybercrime units, FIUs, financial investigation/economic crime units.	Interagency cooperation will provide the conditions for effective measures on criminal money flows on the Internet.
Result 4: Guidelines on the prevention and control of online fraud and criminal money flows for financial sector entities developed and disseminated.	- Increase in the number of financial sector entities that have published indicators based on these guidelines.	- Performance review workshops carried out under the Action. - Websites of financial sector entities, financial intelligence units and regulators.	Such guidelines will help prevent criminal money flows but also improve reporting of suspicious transactions to FIUs.
Result 5: Public/private information sharing and intelligence exchange mechanisms on cybercrime established at domestic and regional levels.	- Number of meetings of financial sector ISACs at domestic and regional levels.	- Performance review workshops carried out under the Action.	Such mechanisms provide intelligence to prevent threats and enhance knowledge of threats and trends.
Result 6: Judicial training academies are providing training on cybercrime and electronic evidence and related financial investigations and anti-money laundering measures.	- Increase in the number of training courses delivered by judicial training institutions in each beneficiary.	- Performance review workshops carried out under the Action. - Websites of judicial training institutions.	Judicial training on cybercrime and electronic evidence is a prerequisite for successful criminal justice action.
Result 7: International cooperation and information sharing strengthened between cybercrime units, financial investigation units and financial intelligence units as well as between competent authorities for judicial cooperation.	- Increase in the effectiveness of international cooperation in terms of timeliness and number of cooperation requests.	- Performance review workshops carried out under the Action. - MONEYVAL and T-CY reports.	More effective international cooperation will help meet the challenge of the transnational nature of cybercrime and related criminal money flows.

ACTIVITIES	MEANS	OVERALL COST	ASSUMPTIONS
	- For all activities: Grant Contract	EUR 5.5 million (EUR 5 million EU financing)	Authorities and other partners are prepared establish and resource mechanism based on advice and other support provided.
Activities to achieve Result 1: - Analysis of existing reporting mechanisms. - Workshops for sharing of good practices. - Advice in the setting up of reporting mechanisms. - Training in the management and use of the mechanisms. - Support to public awareness on the existence of the mechanisms. - Workshops to review performance of the mechanisms.	- Project management unit. - Consultants. - Service contracts and administrative arrangements with public entities for organisational matters.	10%	
Activities to achieve Result 2: - Analysis of legislation against EU, FATF and Council of Europe (MONEYVAL) standards and recommendations. - Advice to public authorities and law reform working groups. - Regional workshops to review effectiveness of legislation. - Online platform for legislation and court rulings.	- Project management unit. - Consultants. - Service contracts and administrative arrangements with public entities for organisational matters.	10%	Governments are committed to support legislative reform process.
Activities to achieve Result 3: - Joint workshops and training for cybercrime units, economic crime units, financial investigators and FIUs. - Advice on the preparation of cooperation protocols. - Workshops to review their practical application.	- Project management unit. - Consultants. - Service contracts and administrative arrangements with public entities for organisational matters.	20%	Different institutions are prepared to cooperate with each other. Leadership of institutions support/promote cooperation.
Activities to achieve Result 4: - Analysis of indicators and red flags used by financial sector entities to prevent online fraud and money laundering. - Regional workshops to share experience. - Creation of domestic and regional working groups to elaborate guidelines. - Dissemination of the guidelines and training in their application. - Workshops to review their practical application.	- Project management unit. - Consultants. - Service contracts and administrative arrangements with public entities for organisational matters.	10%	Financial sector entities are prepared to engage in the process.
Activities to achieve Result 5: - Regional and domestic workshops to promote the concept of Financial Sector Information Sharing and Analysis Centres (FI-ISAC).	- Project management unit. - Consultants. - Service contracts and administrative arrangements with public entities for	10%	Stakeholders are prepared to engage in the process.

- Support to protocols establishing such mechanisms.	organisational matters.		
Activities to achieve Result 6: - Preparation of training modules in cooperation with judicial training institutions. - Training of trainers. - Delivery of pilot training courses in each beneficiary. - Performance review workshops.	- Project management unit. - Consultants. - Service contracts and administrative arrangements with public entities for organisational matters.	20%	Judicial training institutions cooperate in this process and are prepared to mainstream such modules into their curricula.
Activities to achieve Result 7: - Joint workshops at domestic and regional levels. - Elaboration and promotion of protocols for international sharing of intelligence and evidence. - Online platform for international cooperation. - Workshops to review effectiveness of international cooperation.	- Project management unit. - Consultants. - Service contracts and administrative arrangements with public entities for organisational matters.	20%	Cooperation procedures/protocols meet rules of law, including data protection, requirements.

ADDITIONAL DESCRIPTION

The Action aims at the strengthening of the capacity of the beneficiaries to search and confiscate cybercrime proceeds and prevent money laundering on the Internet. This objective is to be achieved through seven main activities:

1. Public reporting systems: to ensure that criminal justice authorities are provided with information on threats and trends experienced by the public as well as trigger investigations and prosecutions. Such systems would also provide users with alerts, information and tools to prevent cybercrime.

2. Legislation: to support reforms to bring domestic legislation in line with European and other international standards (EU, Council of Europe, Financial Action Task Force) related to cybercrime and crime proceeds.

3. Inter-agency cooperation: to ensure that cybercrime investigations and financial investigations go hand in hand.

4. Financial sector guidelines: to ensure that financial sector entities apply due diligence and risk-based approaches also in the online environment.

5. Public/private information sharing: to provide for a mechanism allowing public and private sector institutions (such as law enforcement, financial intelligence units, banks, regulators etc.) share intelligence on current threats and trends in a trusted environment and thus allow for immediate preventive measures.

6. Judicial training: to ensure that investigations and prosecutions of cybercrime and criminal money flows on the Internet are completed by court rulings, including on the confiscation of crime proceeds.

7. International cooperation: to enhance efficient international cooperation and information sharing. A key challenge will be asymmetrical cooperation (such as a cybercrime unit of one country with a financial investigation unit of another country) as recommended by the FATF as well as respect for data protection regulations.

3. IMPLEMENTATION ARRANGEMENTS

ROLES AND RESPONSIBILITIES

It is proposed that the Action be implemented by the Council of Europe through its Cybercrime Programme Office (C-PROC) in Bucharest, Romania.[15] C-PROC is a thematic external office that is specialised in implementing capacity building projects on cybercrime. Use will also be made of local Council of Europe offices.

The Council of Europe will request the relevant institutions of the beneficiaries to establish a domestic project team (including representatives of cybercrime units, financial investigations/economic crime units, FIUs and judicial training academies) for the purpose of Action implementation and interagency cooperation.[16] One member of each team will function as coordinator.

The EU Commission, the Council of Europe and the coordinators will form the Project Steering Committee.

[15] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/C-PROC/cPROC_about_ENG_v3.pdf

[16] The CyberCrime@IPA project had followed a similar methodology.

IMPLEMENTATION METHOD(S) AND TYPE(S) OF FINANCING

The Action will be implemented following the conclusion of a direct Grant Contract with Council of Europe, based on Article 190 (1)(f) of the rules of application of Regulation (EU, Euratom) No 966/2012 on account of its technical competence and high degree of specialisation on cybercrime legislation.

In fact, with the Budapest Convention on Cybercrime and the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, the Council of Europe has two instruments that are most relevant for the beneficiaries in the cybercrime area. The Action would be backed up by the monitoring mechanisms of the Council of Europe with respect to these instruments.

Moreover, the Council of Europe has the necessary expertise in the subject-matter not only with respect to cybercrime and money laundering but also the specific field of criminal money flows on the Internet. The CoE successfully implemented the CyberCrime@IPA joint project which prepared the ground for the present Action. The CoE will start activities without delay given the ground work already done and tools and the network of counterparts already available.

With the Cybercrime Programme Office (C-PROC) – in addition to external offices in most of the beneficiaries – the Council of Europe now also has the infrastructure for cost-efficient implementation of multi-country actions on cybercrime.

4. PERFORMANCE MEASUREMENT

METHODOLOGY FOR MONITORING (AND EVALUATION)

The Action will be monitored and evaluated at different levels:

- Review of progress by the Project Steering Group (once every six month)
- Council of Europe internal reporting
- Reporting on progress to the European Commission
- Result-Oriented Monitoring
- Mid-term evaluation by Council of Europe
- Assessments carried out by the Cybercrime Convention Committee (T-CY) on the implementation of the Budapest Convention on Cybercrime.[17]
- From the Contracting Authority's side, generally, contract execution is monitored through regular reports (interim, yearly, final – narrative and financial reports), clearly identified milestones linked to each component of the Action, regular meetings with the contractor by the task manager and participation in Steering Committee meetings.
- For payments, the Contracting Authority has established checklists to identify key factors to ensure that contract/project deliverables are adequately verified for the purpose of the visa "certified correct". The invoices are presented to the Contracting Authority accompanied by the necessary detailed reports reflecting the Action developed and the actual cost items accompanied by the necessary justifications and any other supporting documents.

[17] See www.coe.int/tcy. For the first round of assessments see:
http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/T-CY(2012)10_Assess_report_v31_public.pdf
The second round (assessment of international cooperation provisions) is underway in 2013/2014.

INDICATOR MEASUREMENT

Objectives / Results	Indicator	Baseline (2014)	Last available (year)	Milestone 2017	Target 2020	Source of information
Specific objective To strengthen the capacity of authorities in the beneficiaries to search, seize and confiscate cybercrime proceeds and prevent money laundering on the Internet.	Extent of financial investigations and prosecutions related to cybercrime and proceeds from online crime. Level of compliance with international standards on cybercrime, money laundering and the search, seizure and confiscation of proceeds from crime (Council of Europe Conventions ETS 185 and 198).	With few exceptions, proceeds from cybercrime are not searched, seized and confiscated. With exceptions, beneficiaries are only partially in compliance with ETS 185 and 198.		Measureable increase in domestic, regional and international financial investigations in relation to cybercrime. Reforms are underway in terms of legislation, institutions and practices and in line with international standards and recommendations.	Cybercrime investigations are systematically accompanied by domestic and international financial investigations to search, seize and confiscate proceeds from online crime. Beneficiaries are compliant with provisions of ETS 185 and 198 that are relevant for cybercrime proceeds.	- For baseline: analyses during inception phase - Performance review workshops carried out - Initial situation report at the outset of the Action to establish baseline data - Assessment report towards the end of the Action to determine progress made. - MONEYVAL and T-CY reports.
Result 1: Public reporting systems (with preventive functions) on online fraud and other cybercrime established in each beneficiary.	Presence and performance of public reporting mechanisms in terms of receiving and processing reports and publishing analyses in each beneficiary.	With exceptions, public reporting mechanisms are not in place.		Public reporting mechanisms have been established in each beneficiary.	Public reporting mechanisms receive and process reports and publish analyses in each beneficiary.	- For baseline: analyses during inception phase - Performance review workshops carried out under the Action. - Reports published by reporting mechanism
Result 2:	Number and quality of relevant	All beneficiaries		Draft legal	Amendments	- For baseline: analyses

Legislation strengthened regarding the search, seizure and confiscation of cybercrime proceeds and the prevention of money laundering on the Internet in line with data protection requirements.	draft amendments to laws made available to bring legal frameworks of each beneficiary in line with international standards.	have cybercrime legislation largely compliant with the Budapest Convention on Cybercrime, however, with gaps regarding procedural law and concerns regarding data protection and privacy. Specific measures regarding crime proceeds on the Internet and international data sharing are yet to be addressed in most beneficiaries.		amendments available in most beneficiaries	adopted by Governments or working groups and in some instances by Parliaments.	during inception phase - Performance review workshops carried out under the Action. - Reports by MONEYVAL and Cybercrime Convention Committee (T-CY).
Result 3: Cybercrime units, financial investigators and financial intelligence units cooperate with each other at the domestic level in the search, seizure and confiscation of online crime proceeds.	Increase in the number and degree of relevance of cybercrime investigations in each beneficiary accompanied by parallel financial investigations.	Limited interagency cooperation and thus limited financial investigations related to cybercrime.		Protocols and procedures established for interagency cooperation in each beneficiary and measureable increase in financial investigations.	Increased number and relevance of cybercrime investigations accompanied by parallel financial investigations.	- For baseline: analyses during inception phase - Performance review workshops carried out under the Action. - Reports by cybercrime units, FIUs, financial investigation/economic crime units.
Result 4: Guidelines on the prevention and control of online fraud and criminal	Increase in the number of financial sector entities that have published indicators based on these guidelines.	With exceptions, specific guidelines are not available.		Guidelines have been developed and adopted.	Financial sector entities have published and apply indicators based on these	- For baseline: analyses during inception phase - Performance review workshops carried out under the Action.

money flows for financial sector entities developed and disseminated.					guidelines.	- Websites of financial sector entities, financial intelligence units and regulators
Result 5: Public/private information sharing and intelligence exchange mechanisms on cybercrime established at domestic and regional levels.	Number of meetings of financial sector ISACs at domestic and regional levels.	Initial efforts have been made in some beneficiaries to facilitate public/private information sharing.		Financial sector ISACs established in each beneficiary.	Financial sector ISACs have met at least two times in each beneficiary and three times at regional level.	- For baseline: analyses during inception phase - Performance review workshops carried out under the Action.
Result 6: Judicial training academies are providing training on cybercrime and electronic evidence and related financial investigations and anti-money laundering measures.	Increase in the number of training courses delivered by judicial training institutions in each beneficiary.	Judicial training academies in all beneficiaries dispose of basic capacities to deliver training on cybercrime. These capacities are not yet sustainable. Specific modules related to cybercrime proceeds are not yet available.		Specific modules on cybercrime proceeds have been developed. At least two training courses have been delivered by judicial training academies in each beneficiary.	Training on cybercrime and electronic evidence is part of the regular curriculum of judicial training academies. At least four training courses have been delivered in each beneficiary.	- For baseline: analyses during inception phase - Performance review workshops carried out under the Action. - Websites of judicial training institutions.
Result 7: International cooperation and information sharing strengthened at all levels (cybercrime units, financial investigation units and financial intelligence units,	Increase in the effectiveness of international cooperation in terms of timeliness and number of cooperation requests.	Regional and international cooperation on cybercrime and electronic evidence by most beneficiaries. All beneficiaries encounter problems regarding the		Protocols, guidelines and online tools available to facilitate international cooperation.	Increased number, quality and timeliness of international cooperation requests related to cybercrime and related proceeds.	- For baseline: analyses during inception phase - Performance review workshops carried out under the Action. - MONEYVAL and T-CY reports.

competent authorities for judicial cooperation, private sector entities).		efficiency of cooperation, cooperation with private sector entities, and cooperation involving multiple types of institutions.				

5. CROSS-CUTTING ISSUES

ENVIRONMENT AND CLIMATE CHANGE
Not applicable.

ENGAGEMENT WITH CIVIL SOCIETY
Non-state actors to be involved in the Action include in particular Internet Service Providers and financial sector institutions.

EQUAL OPPORTUNITIES AND GENDER MAINSTREAMING
Women and children are often victims of cybercrime, cyber bullying and cyber harassment. Actions should therefore consider and address the gender dimension when designed and implemented. Efforts will also therefore be required to promote the participation of women in Action activities, for example in the composition of domestic project teams and the nomination of participants in Action activities such as workshops and trainings.

MINORITIES AND VULNERABLE GROUPS
Not applicable.

6. SUSTAINABILITY
Activities are designed to be sustainable. Legislation (Result 1), once adopted, is difficult to reverse. The judicial training component (result 6) is to mainstream training on cybercrime (and related fraud) and electronic evidence into the curricular of training institutions. This is more sustainable than ad-hoc training. With regard to the remaining components, the Action is aimed at formalising cooperation arrangements through protocols and other means to enhance sustainability.

Governments are increasingly prepared to make resources available to enhance the security, trust and confidence in information technologies. This should further enhance the chances of sustainability of Action results.

7. COMMUNICATION AND VISIBILITY
Communication and visibility will be given high importance during the implementation of the Action. All necessary measures will be taken to make public the fact that the Action has received funding from the EU in line with the Communication and Visibility Manual for EU External Actions.

The implementation of the communication activities shall be the responsibility of the contractor and shall be funded from the amounts allocated to the Action.

Visibility and communication actions shall demonstrate how the intervention contributes to the agreed programme objectives and the accession process. Actions shall be undertaken to strengthen general public awareness and promote transparency and accountability on the use of funds.

The Commission shall be fully informed of the planning and implementation of the specific visibility and communication activities.

The Action will be publicised at the Council of Europe cybercrime website (www.coe.int/cybercrime). A specific page will be established for the Action. Moreover, the activities and results will be widely disseminated at international fora (as was the case with the CyberCrime@IPA joint project).

A communication plan will be prepared during the inception phase of the Action.