iPROCEEDS

Targeting Crime Proceeds on the Internet in South-Eastern Europe and Turkey

Project workplan

Version 10 June 2016

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Contents

1. PROJECT SUMMARY

Project title / number:	Project iPROCEEDS - Cooperation on Cybercrime under the Instrument of Pre-accession (IPA): Project on targeting crime proceeds on the Internet in South-eastern Europe and Turkey (2015/DGI/JP/3156)
Project area:	Albania, Bosnia and Herzegovina, Montenegro, Serbia, "the former Yugoslav Republic of Macedonia", Turkey and Kosovo*[1]
Duration:	25 months (1 December 2015 – 31 December 2019)
Budget:	EURO 5.56 million
Funding:	European Union and Council of Europe
Implementation:	Cybercrime Programme Office (C-PROC) of the Council of Europe
Project objective	To strengthen the capacity of authorities in the IPA region to search, seize and confiscate cybercrime proceeds and prevent money laundering on the Internet. Indicators include: – 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).
Result 1	Public reporting systems (with preventive functions) on online fraud and other cybercrime improved or established in each beneficiary. Indicators include: – Presence and performance of public reporting mechanisms in terms of receiving and processing reports and publishing analyses in each beneficiary.
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. Indicators include: – Number and quality of relevant draft amendments to laws made available to bring legal frameworks of each beneficiary in line with international standards.
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. Indicators include: – Increase in the number and degree of relevance of cybercrime investigations in each beneficiary accompanied by parallel financial investigations and vice versa.
Result 4	Guidelines on the prevention and control of online fraud and criminal money flows for financial sector entities developed and disseminated, and indicators for

[1]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.

	the prevention of online money laundering reviewed and updated. Indicators include: – Increase in the number of financial sector entities that have published indicators based on these guidelines.
Result 5	Public/private information sharing and intelligence exchange mechanisms on cybercrime established or enhanced at domestic and regional levels. Indicators include: – Number of meetings of financial sector ISACs at domestic and regional levels.
Result 6	Judicial training academies are providing training on cybercrime and electronic evidence and related financial investigations and anti-money laundering measures. Indicators include: – Increase in the number of training courses delivered by judicial training institutions in each beneficiary.
Result 7	International cooperation and information sharing strengthened between cybercrime units, financial investigation units and financial intelligence units (FIUs) as well as between competent authorities for judicial cooperation. Indicators include: – Increase in the effectiveness of international cooperation in terms of timeliness and number of cooperation requests.

CONTACT

Mariana CHICU
Project Manager
Cybercrime Programme Office (C-PROC) of the Council of Europe
mariana.chicu@coe.int

2. CALENDAR OF ACTIVITIES

April – December 2016

PERIOD	PLACE / ACTIVITY	DATE
April 2016	1.1.1/2.1.1/3.1.1/4.1.1/5.1.1/6.1.1/7.1.1 Serbia: Initial country visit to analyse the existing reporting systems on online fraud and other cybercrime, legislation on search, seizure and confiscation of cybercrime proceeds, national interagency cooperation, indicators and redflags used by financial sector to prevent online money laundering, current public/private mechanisms for information sharing and intelligence exchange, training on cybercrime and electronic evidence, as well as financial investigation and anti-money laundering measures, and international cooperation.	14-15 April 2016
	1.1.1/2.1.1/3.1.1/4.1.1/5.1.1/6.1.1/7.1.1 Montenegro: Initial country visit.	18-19 April 2016
	1.1.1/2.1.1/3.1.1/4.1.1/5.1.1/6.1.1/7.1.1 "The former Yugoslav Republic of Macedonia": Initial country visit.	21-22 April 2016
May 2016	1.1.1/2.1.1/3.1.1/4.1.1/5.1.1/6.1.1/7.1.1 Bosnia and Herzegovina: Initial country visit.	5-6 May 2016
	1.1.1/2.1.1/3.1.1/4.1.1/5.1.1/6.1.1/7.1.1 Albania: Initial country visit.	9-10 May 2016
	3.9 Tirana, Albania: Participation in IPA Western Balkans Security Governance Programming Meeting.	10-12 May 2016
	1.1.1/2.1.1/3.1.1/4.1.1/5.1.1/6.1.1/7.1.1 Turkey: Initial country visit.	12-13 May 2016
	1.1.1/2.1.1/3.1.1/4.1.1/5.1.1/6.1.1/7.1.1 Kosovo*: Initial country visit.	19-20 May 2016
	3.9 Strasbourg, France (Council of Europe): Participation in the exchange of views with data protection organisations.	23 May
	3.9 Strasbourg, France (Council of Europe): Participation in the 15th plenary session of the Cybercrime Convention Committee (T-CY).	24-25 May 2016
June 2016	1.7.1 Advice on regulatory framework and enforcing capacities of national CERTs to address reported crime and incidents (upon request).	starting from June 2016
	2.2.1 Advice to public authorities and law reform working groups available to bring legal frameworks of each beneficiary in line with international standards (assessment of draft legislation, desk review).	starting from June 2016
	5.2 Ohrid, "the former Yugoslav Republic of Macedonia": Regional workshop on private/public information sharing and intelligence exchange mechanisms between financial sector institutions, cybercrime units and other stakeholders (combined with the Opening Conference of the iPROCEEDS project).	13-14 June 2016
	7.2 Ohrid, "the former Yugoslav Republic of Macedonia": Regional workshop on international cooperation between cybercrime units, financial investigations units, Financial Intelligence Units, prosecution and competent authorities for judicial cooperation (combined with the Opening	13-14 June 2016

PERIOD	PLACE / ACTIVITY	DATE
	Conference of the iPROCEEDS project).	
July 2016	1.1.2/2.1.2/3.1.2/4.1.2/5.1.2/6.1.2/7.1.2 Initial Situation Report.	15 July 2016
	3.5.1 Design of case simulation exercises on cybercrime and financial investigations.	July 2016 (to be finalised in January 2017)
	3.10 Support participation in long-distance master programmes (course fees for 14 participants; travel and per diems).	from June 2016 (till the end of the project)
August 2016	1.3.4 Serbia: Advisory mission and workshop for the setting up or improvement of reporting mechanisms.	1-2 August 2016
	1.3.5 Kosovo*: Advisory mission and workshop for the setting up or improvement of reporting mechanisms.	4-5 August 2016
September 2016	3.9 Finland: Participation of cybecrime units in the Regional Internet Security Event (RISE) - Finland 2016 (Team Cymru).	13-15 September 2016
	1.2.1 Regional Centre for judicial training on Cybercrime, Zagreb, Croatia: Regional workshop for sharing international good practices on reporting mechanisms (TBC).	19-20 September 2016
	1.3.1 Albania: Advisory mission and workshop for the setting up or improvement of reporting mechanisms.	29-30 September 2016
October 2016	1.3.3 Montenegro: Advisory mission and workshop for the setting up or improvement of reporting mechanisms.	4-5 October 2016
	6.1.3 Regional Centre for judicial training on Cybercrime, Zagreb, Croatia: Regional workshop to review the current state of judicial training curricular on cybercrime, electronic evidence and online crime proceeds. (TBC)	12-13 October
	5.4.1 Regional meeting to discuss existing private/public initiatives or establish such mechanisms at domestic and regional levels.	25-26 October 2016
November 2016	3.7.5 "The former Yugoslav Republic of Macedonia": Advice and workshop on the preparation of interagency cooperation protocols.	1-2 November 2016
	7.3.6 "The former Yugoslav Republic of Macedonia": Workshop on domestic protocols for international sharing of intelligence and evidence.	3 November 2016
	3.9 Strasbourg, France (Council of Europe): Participation in the 16th plenary session of the Cybercrime Convention Committee (T-CY).	14-15 November 2016
	3.9 Strasbourg, France (Council of Europe): Participation in the Octopus Conference 2016.	16-18 November 2016
	3.3.1 Development of an introductory training module on cybercrime and financial investigations for cybercrime, financial investigation units, FIUs and specialised prosecutors.	November 2016 (to be finished in March 2017)
	7.3.1 Elaboration of domestic protocols for international sharing of intelligence and evidence.	November 2016 (to be finalised in September 2017)
	3.7.6 Turkey: Advice and workshop on the preparation of interagency cooperation protocols.	21-22 November 2016
	7.3.7 Turkey: Workshop on domestic protocols for international sharing of intelligence and evidence.	23 November 2016

PERIOD	PLACE / ACTIVITY	DATE
	7.3.8 Kosovo*: Workshop on domestic protocols for international sharing of intelligence and evidence.	29 November 2016
December 2016	3.7.7 Kosovo*: Advice and workshop on the preparation of interagency cooperation protocols.	1-2 December 2016
	2.1.3 Regional workshop on compliance of relevant domestic legislation with EU, FATF and Council of Europe (MONEYVAL) standards.	5-6 December 2016
	3.4.6 Serbia: Workshop for cybercrime units, economic crime units, financial investigators, FIUs and specialised prosecutors on financial fraud and credit card fraud online.	8-9 December 2016

3. WORKPLAN

Project objective	**To strengthen the capacity of authorities in the beneficiaries to search, seize and confiscate cybercrime proceeds and prevent money laundering on the Internet.**	
Result 1	**Public reporting systems (with preventive functions) on online fraud and other cybercrime improved or established in each beneficiary.**	
Activities:		
1.1	Analysis of existing reporting mechanisms.	
	1.1.1 Seven initial country visits.	14-15 April 2016 - Serbia 18-19 April 2016 - Montenegro 21-22 April 2016 – "The former Yugoslav Republic of Macedonia" 5-6 May 2016 - Bosnia and Herzegovina 9-10 May 2016 - Albania 12-13 May 2016 - Turkey 19-20 May 2016 - Kosovo*
	1.1.2 Initial Situation Report.	July 2016
1.2	Organise two regional workshops for sharing international and regional good practices regarding public reporting mechanisms on online fraud and other cybercrime.	
	1.2.1 Regional workshop for sharing international good practices on reporting mechanisms (Regional Centre for judicial training on Cybercrime, Zagreb, Croatia (TBC)).	19-20 September 2016
	1.2.2 Regional workshop for sharing good practices on reporting mechanisms existent in IPA region.	February 2017
1.3	Provide advice in the setting-up or improvement of reporting mechanisms and organise seven in-country workshops.	
	1.3.1 Albania: Advisory mission and workshop for the setting up or improvement of reporting mechanisms.	29-30 September 2016
	1.3.2 Bosnia and Herzegovina: Advisory mission and workshop for the setting up or improvement of reporting mechanisms.	March 2017
	1.3.3 Montenegro: Advisory mission and workshop for the setting up or improvement of reporting mechanisms.	4-5 October 2016
	1.3.4 Serbia: Advisory mission and workshop for the setting up or improvement of reporting mechanisms.	1-2 August 2016
	1.3.5 Kosovo*: Advisory mission and workshop for the setting up or improvement of reporting mechanisms.	4-5 August 2016
	1.3.6 Turkey: Advisory mission and workshop for the setting up or improvement of reporting mechanisms.	April 2017
	1.3.7 "The former Yugoslav Republic of Macedonia": Advisory mission and workshop for the setting up or improvement of reporting mechanisms.	June 2017
1.4	Organise seven in-country workshops in the management and use of the reporting mechanisms.	
	1.4.1 Albania: Training in the management and use of the reporting mechanisms.	March 2018
	1.4.2 Bosnia and Herzegovina: Training in the	March 2018

	management and use of the reporting mechanisms.	
	1.4.3 Montenegro: Training in the management and use of the reporting mechanisms.	May 2018
	1.4.4 Serbia: Training in the management and use of the reporting mechanisms.	May 2018
	1.4.5 "The former Yugoslav Republic of Macedonia": Training in the management and use of the reporting mechanisms.	August 2018
	1.4.6 Turkey: Training in the management and use of the reporting mechanisms.	September 2018
	1.4.7 Kosovo*: Training in the management and use of the reporting mechanisms.	October 2018
1.5	Organise seven in-country workshops to promote the preparation and dissemination of annual reports on the cybercrime situation.	
	1.5.1 Albania: Workshop to promote the preparation and dissemination of annual reports.	February 2019
	1.5.2 Bosnia and Herzegovina: Workshop to promote the preparation and dissemination of annual reports.	February 2019
	1.5.3 Montenegro: Workshop to promote the preparation and dissemination of annual reports.	April 2019
	1.5.4 Serbia: Workshop to promote the preparation and dissemination of annual reports.	April 2019
	1.5.6 "The former Yugoslav Republic of Macedonia": Workshop to promote the preparation and dissemination of annual reports.	April 2019
	1.5.6 Turkey: Workshop to promote the preparation and dissemination of annual reports.	May 2019
	1.5.7 Kosovo*: Workshop to promote the preparation and dissemination of annual reports.	May 2019
1.6	Regional workshop to review performance of the mechanisms. (Regional Centre for judicial training on Cybercrime, Zagreb, Croatia (TBC))	June 2019
1.7	Provide support to the newly established national Computer emergency response teams (CERT) in information sharing and cooperation with criminal justice authorities.	
	1.7.1 Advice on regulatory framework and enforcing capacities of national CERTs to address reported crime and incidents.	June 2016 – June 2019
	1.7.2 Study visit of 14 representatives from CERTs to the European Union Agency for Network and Information Security (ENISA).	May 2017
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.**	
Activities:		
2.1	Analysis of legislation against EU, FATF and Council of Europe (MONEYVAL) standards and recommendations and regional workshop.	
	2.1.1 Seven initial country visits.	14-15 April 2016 - Serbia 18-19 April 2016 - Montenegro 21-22 April 2016 – "The former Yugoslav Republic of Macedonia" 5-6 May 2016 - Bosnia and Herzegovina

		9-10 May 2016 - Albania 12-13 May 2016 - Turkey 19-20 May 2016 - Kosovo*
	2.1.2 Initial Situation Report.	July 2016
	2.1.3 Regional workshop on compliance of relevant domestic legislation with EU, FATF and Council of Europe (MONEYVAL) standards.	5-6 December 2016
2.2	Provide advice to public authorities and law reform working groups, including organisation of domestic workshops.	
	2.2.1 Advice to public authorities and law reform working groups available to bring legal frameworks of each beneficiary in line with international standards (assessment of draft legislation, desk review).	June 2016 - June 2019 (need based)
	2.2.2 Albania: Workshop on law reform regarding cybercrime, financial investigation and confiscation of cybercrime proceeds, as well as prevention of money laundering on the Internet. (details and content TBD)	October 2017
	2.2.3 Bosnia and Herzegovina: Workshop on law reform regarding cybercrime, financial investigation and confiscation of cybercrime proceeds, as well as prevention of money laundering on the Internet. (details and content TBD)	October 2017
	2.2.4 Montenegro: Workshop on law reform regarding cybercrime, financial investigation and confiscation of cybercrime proceeds, as well as prevention of money laundering on the Internet. (details and content TBD)	November 2017
	2.2.5 Serbia: Workshop on law reform regarding cybercrime, financial investigation and confiscation of cybercrime proceeds, as well as prevention of money laundering on the Internet. (details and content TBD)	March 2018
	2.2.6 "The former Yugoslav Republic of Macedonia": Workshop on law reform regarding cybercrime, financial investigation and confiscation of cybercrime proceeds, as well as prevention of money laundering on the Internet. (details and content TBD)	March 2018
	2.2.7 Turkey: Workshop on law reform regarding cybercrime, financial investigation and confiscation of cybercrime proceeds, as well as prevention of money laundering on the Internet. (details and content TBD)	April 2018
	2.2.8 Kosovo*: Workshop on law reform regarding cybercrime, financial investigation and confiscation of cybercrime proceeds, as well as prevention of money laundering on the Internet. (details and content TBD)	April 2018
2.3	Organise two regional workshops to review the effectiveness of legislation.	
	2.3.1 Regional workshop to review effectiveness of the relevant legislation.	May 2018
	2.3.2 Regional workshop to review effectiveness of the relevant legislation.	May 2019
2.4	Online platform for legislation and court rulings: Continuous update of the Country Wikis for South-eastern	2016-2019

	Europe in the Octopus Community regarding legislation and jurisprudence	
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.**	
Activities:		
3.1	Study and regional workshop to prepare/review/improve training strategies on cybercrime, electronic evidence and financial investigations.	
	3.1.1 Seven initial country visits.	14-15 April 2016 - Serbia 18-19 April 2016 - Montenegro 21-22 April 2016 – "The former Yugoslav Republic of Macedonia" 5-6 May 2016 - Bosnia and Herzegovina 9-10 May 2016 - Albania 12-13 May 2016 - Turkey 19-20 May 2016 - Kosovo*
	3.1.2 Initial Situation Report.	July 2016
3.2	Develop guidelines for obtaining and using electronic evidence in criminal proceedings under the respective domestic legislation.	
	3.2.1 Seven country visits to assess the national regulatory framework for obtaining and using electronic evidence in criminal proceedings (Albania, Bosnia and Herzegovina, Montenegro, Serbia, "The former Yugoslav Republic of Macedonia", Turkey, Kosovo*).	January-April 2017
	3.2.2 Study on obtaining and using electronic evidence in criminal proceedings under the respective domestic legislation of the beneficiary countries.	August 2017
	3.2.3 Montenegro: Meeting of the regional working group on developing guidelines for obtaining and using electronic evidence in criminal proceedings.	November 2017
	3.2.4 Albania: Meeting of the regional working group on developing guidelines for obtaining and using electronic evidence in criminal proceedings.	January 2018
	3.2.5 "The former Yugoslav Republic of Macedonia": Meeting of the regional working group on developing guidelines for obtaining and using electronic evidence in criminal proceedings.	March 2018
	3.2.6 Advice on developing guidelines for obtaining and using electronic evidence in criminal proceedings.	November 2017 – March 2018
3.3	Develop and deliver an introductory training module on cybercrime and financial investigations for cybercrime, financial investigation units, FIUs and specialised prosecutors.	
	3.3.1 Development of an introductory training module on cybercrime and financial investigations for cybercrime, financial investigation units, FIUs and specialised prosecutors.	November 2016 – March 2017
	3.3.2 Regional workshop on introductory training module on cybercrime and financial investigations. (Regional Centre for judicial training on Cybercrime, Zagreb, Croatia (TBC))	June 2017
	3.3.3 Training of trainers session on introductory training module on cybercrime and financial investigations.	August 2017

	(Regional Centre for judicial training on Cybercrime, Zagreb, Croatia (TBC))	
	3.3.4 Albania: Introductory training session on cybercrime and financial investigations.	November 2017
	3.3.5 Bosnia and Herzegovina: Introductory training session on cybercrime and financial investigations.	December 2017
	3.3.6 Montenegro: Introductory training session on cybercrime and financial investigations.	February 2018
	3.3.7 Serbia: Introductory training session on cybercrime and financial investigations.	March 2018
	3.3.8 "The former Yugoslav Republic of Macedonia": Introductory training session on cybercrime and financial investigations.	April 2018
	3.3.9 Turkey: Introductory training session on cybercrime and financial investigations.	April 2018
	3.3.10 Kosovo*: Introductory training session on cybercrime and financial investigations.	May 2018
3.4	Organise joint workshop and training (regional and domestic) for cybercrime units, economic crime units, financial investigators, FIUs and specialised prosecutors on specific issues.	
	3.4.1 Regional training for cybercrime units, economic crime units, financial investigators, FIUs and specialised prosecutors on virtual currencies and the dark web.	March 2017
	3.4.2 Regional training for cybercrime units, economic crime units, financial investigators, FIUs and specialised prosecutors on techniques to search, seize and confiscate proceeds from crime online.	July 2017
	3.4.3 Albania: Workshop for cybercrime units, economic crime units, financial investigators, FIUs and specialised prosecutors on specific issues. (details and content TBD)	January 2018
	3.4.4 Bosnia and Herzegovina: Workshop for cybercrime units, economic crime units, financial investigators, FIUs and specialised prosecutors on specific issues. (details and content TBD)	January 2018
	3.4.5 Montenegro: Workshop for cybercrime units, economic crime units, financial investigators, FIUs and specialised prosecutors on specific issues. (details and content TBD)	September 2017
	3.4.6 Serbia: Workshop for cybercrime units, economic crime units, financial investigators, FIUs and specialised prosecutors on financial fraud and credit card fraud online.	8-9 December 2016
	3.4.7 "The former Yugoslav Republic of Macedonia": Workshop for cybercrime units, economic crime units, financial investigators, FIUs and specialised prosecutors on specific issues. (details and content TBD)	December 2017
	3.4.8 Turkey: Workshop for cybercrime units, economic crime units, financial investigators, FIUs and specialised prosecutors on specific issues. (details and content TBD)	March 2018
	3.4.9 Kosovo*: Workshop for cybercrime units, economic crime units, financial investigators, FIUs and specialised prosecutors on specific issues. (details and content TBD)	March 2018
3.5	Design and implement domestic and regional case simulation exercises on cybercrime and	

	financial investigations.	
	3.5.1 Design of case simulation exercises on cybercrime and financial investigations	July 2016-January 2017
	3.5.2 Regional case simulation exercise on cybercrime and financial investigations (possibly in cooperation with Cybercrime@EAPIII project)	April 2017
	3.5.3 Regional case simulation exercise on cybercrime and financial investigations.	January 2018
	3.5.4 Albania: Two case simulation exercises on cybercrime and financial investigations. (details and content TBD)	August 2017 2019
	3.5.5 Bosnia and Herzegovina: Two case simulation exercises on cybercrime and financial investigations. (details and content TBD)	August 2017 2019
	3.5.6 Montenegro: Two case simulation exercises on cybercrime and financial investigations. (details and content TBD)	January 2018 2019
	3.5.7 Serbia: Two case simulation exercises on cybercrime and financial investigations. (details and content TBD)	March 2018 2019
	3.5.8 "The former Yugoslav Republic of Macedonia": Two case simulation exercises on cybercrime and financial investigations. (details and content TBD)	March 2018 2019
	3.5.9 Turkey: Two case simulation exercises on cybercrime and financial investigations. (details and content TBD)	May 2017 2019
	3.5.10 Kosovo*: Two case simulation exercises on cybercrime and financial investigations. (details and content TBD)	June 2017 2019
3.6	Follow up to lessons learnt from case simulation exercises.	
	3.6.1 Albania: Advice and workshop on lessons learnt from case simulation exercises.	2019
	3.6.2 Bosnia and Herzegovina: Advice and workshop on lessons learnt from case simulation exercises.	2019
	3.6.3 Montenegro: Advice and workshop on lessons learnt from case simulation exercises.	2019
	3.6.4 Serbia: Advice and workshop on lessons learnt from case simulation exercises.	2019
	3.6.5 "The former Yugoslav Republic of Macedonia": Advice and workshop on lessons learnt from case simulation exercises.	2019
	3.6.6 Turkey: Advice and workshop on lessons learnt from case simulation exercises.	2019
	3.6.7 Kosovo*: Advice and workshop on lessons learnt from case simulation exercises.	2019
3.7	Advice on the preparation of interagency cooperation protocols.	
	3.7.1 Albania: Advice and workshop on the preparation of interagency cooperation protocols.	March 2017
	3.7.2 Bosnia and Herzegovina: Advice and workshop on the preparation of interagency cooperation protocols.	July 2017
	3.7.3 Montenegro: Advice and workshop on the	August 2017

	preparation of interagency cooperation protocols.	
	3.7.4 Serbia: Advice and workshop on the preparation of interagency cooperation protocols.	September 2017
	3.7.5 "The former Yugoslav Republic of Macedonia": Advice and workshop on the preparation of interagency cooperation protocols.	1-2 November 2016
	3.7.6 Turkey: Advice and workshop on the preparation of interagency cooperation protocols.	21-22 November 2016
	3.7.7 Kosovo*: Advice and workshop on the preparation of interagency cooperation protocols.	1-2 December 2016
3.8	Workshop to assess the functioning of interagency cooperation.	January 2019
3.9	Support participation in training activities and relevant meetings organised by other organisations.	2016-2019
3.10	Support participation in long-distance master programmes (Course fees for 14 participants; travel and per diems).	2016-2019
Result 4	**Guidelines on the prevention and control of online fraud and criminal money flows for financial sector entities developed and disseminated, and indicators for the prevention of online money laundering reviewed and updated.**	
Activities:		
4.1	Analysis of indicators and red flags used by financial sector entities to prevent money laundering in the online environment.	
	4.1.1 Seven initial country visits.	14-15 April 2016 - Serbia 18-19 April 2016 - Montenegro 21-22 April 2016 - "The former Yugoslav Republic of Macedonia" 5-6 May 2016 - Bosnia and Herzegovina 9-10 May 2016 - Albania 12-13 May 2016 - Turkey 19-20 May 2016 - Kosovo*
	4.1.2 Initial Situation Report.	July 2016
4.2	Analysis of guidelines to prevent and detect/identify online crime proceeds.	
	4.2.1 Country visits.	February-April 2017
	4.2.2 Assessment report of guidelines to prevent and detect/identify online crime proceeds.	June 2017
4.3	Regional workshop to share experience on indicators and guidelines for financial sector entities to prevent money laundering in the online environment.	June 2017
4.4	Creation of domestic and regional working groups to elaborate or improve guidelines and indicators.	
	4.4.1 Setting-up working groups to elaborate/improve guidelines and indicators for financial sector entities to prevent money laundering in the online environment.	June-September 2017
	4.4.2 Albania: Two workshops of the working group to elaborate/improve guidelines and indicators for financial sector entities to prevent money laundering in the online environment.	October 2017 2018
	4.4.3 Bosnia and Herzegovina: Two workshops of the working group to elaborate/improve guidelines and	March 2017 2018

	indicators for financial sector entities to prevent money laundering in the online environment.	
	4.4.4 Montenegro: Two workshops of the working group to elaborate/improve guidelines and indicators for financial sector entities to prevent money laundering in the online environment.	October 2017 2018
	4.4.5 Serbia: Two workshops of the working group to elaborate/improve guidelines and indicators for financial sector entities to prevent money laundering in the online environment.	November 2017 2018
	4.4.6 "The former Yugoslav Republic of Macedonia": Two workshops of the working group to elaborate/improve guidelines and indicators for financial sector entities to prevent money laundering in the online environment.	November 2017 2018
	4.4.7 Turkey: Two workshops of the working group to elaborate/improve guidelines and indicators for financial sector entities to prevent money laundering in the online environment.	December 2017 2018
	4.4.8 Kosovo*: Two workshops of the working group to elaborate/improve guidelines and indicators for financial sector entities to prevent money laundering in the online environment.	December 2017 2018
4.5	Dissemination of the guidelines and training in their application.	
	4.5.1 Albania: Training on the application of the guidelines for financial sector entities to prevent money laundering in the online environment.	March 2018
	4.5.2 Bosnia and Herzegovina: Training on the application of the guidelines for financial sector entities to prevent money laundering in the online environment.	March 2018
	4.5.3 Montenegro: Training on the application of the guidelines for financial sector entities to prevent money laundering in the online environment.	May 2018
	4.5.4 Serbia: Training on the application of the guidelines for financial sector entities to prevent money laundering in the online environment.	May 2018
	4.5.5 "The former Yugoslav Republic of Macedonia": Training on the application of the guidelines for financial sector entities to prevent money laundering in the online environment.	June 2018
	4.5.6 Turkey: Training on the application of the guidelines for financial sector entities to prevent money laundering in the online environment.	July 2018
	4.5.7 Kosovo*: Training on the application of the guidelines for financial sector entities to prevent money laundering in the online environment.	August 2018
4.6	Workshop to review the practical application of the guidelines for financial sector entities to prevent money laundering in the online environment.	January 2019
Result 5	**Public/private information sharing and intelligence exchange mechanisms on cybercrime established or enhanced at domestic and regional levels.**	

Activities:		
5.1	Assess the functioning of current mechanisms for information sharing and intelligence exchange between financial sector institutions (including processing centres), cybercrime units and other stakeholders.	
	5.1.1 Seven initial country visits.	14-15 April 2016 - Serbia 18-19 April 2016 - Montenegro 21-22 April 2016 – "The former Yugoslav Republic of Macedonia" 5-6 May 2016 - Bosnia and Herzegovina 9-10 May 2016 - Albania 12-13 May 2016 - Turkey 19-20 May 2016 - Kosovo*
	5.1.2 Initial Situation Report.	July 2016
5.2	Regional workshop on private/public information sharing and intelligence exchange mechanisms between financial sector institutions, cybercrime units and other stakeholders (combined with the Opening Conference of the iPROCEEDS project).	13-14 June 2016 – Ohrid, "the former Yugoslav Republic of Macedonia"
5.3	Develop guidelines for information and intelligence sharing at national, regional and international levels.	
	5.3.1 Meeting of the regional working group to develop guidelines for information and intelligence sharing at national, regional and international levels.	March 2017
	5.3.2 Meeting of the regional working group to develop guidelines for information and intelligence sharing at national, regional and international levels.	May 2017
	5.3.3 Meeting of the regional working group to develop guidelines for information and intelligence sharing at national, regional and international levels.	September 2017
5.4	Advice and meetings to support existing initiatives or establish such mechanisms at domestic and regional levels.	
	5.4.1 Regional meeting to discuss existing private/public initiatives or establish such mechanisms at domestic and regional levels.	25-26 October 2016
	5.4.2 Albania: Meeting to support existing private/public initiatives or establish such mechanisms at domestic level.	January 2017
	5.4.3 Bosnia and Herzegovina: Meeting to support existing private/public initiatives or establish such mechanisms at domestic level.	January 2017
	5.4.4 Montenegro: Meeting to support existing private/public initiatives or establish such mechanisms at domestic level.	March 2017
	5.4.5 Serbia: Meeting to support existing private/public initiatives or establish such mechanisms at domestic level.	March 2017
	5.4.6 "The former Yugoslav Republic of Macedonia": Meeting to support existing private/public initiatives or establish such mechanisms at domestic level.	April 2017
	5.4.7 Turkey: Meeting to support existing private/public initiatives or establish such mechanisms at domestic level.	April 2017

	5.4.8 Kosovo*: Meeting to support existing private/public initiatives or establish such mechanisms at domestic level.	June 2017
5.5	Establish an online resource in support of such mechanisms as well as on law enforcement / Internet service provider cooperation (research study).	June 2017
5.6	Workshop to review the performance of information sharing and cooperation mechanisms.	March 2019
Result 6	**Judicial training academies are providing training on cybercrime and electronic evidence and related financial investigations and anti-money laundering measures.**	
6.1	Regional workshop for representatives of judicial training academy to review the current state of judicial training and agree on project approach.	
	6.1.1 Seven initial country visits.	14-15 April 2016 - Serbia 18-19 April 2016 - Montenegro 21-22 April 2016 – "The former Yugoslav Republic of Macedonia" 5-6 May 2016 - Bosnia and Herzegovina 9-10 May 2016 - Albania 12-13 May 2016 - Turkey 19-20 May 2016 - Kosovo*
	6.1.2 Initial Situation Report.	July 2016
	6.1.3 Regional workshop to review the current state of judicial training curricular on cybercrime, electronic evidence and online crime proceeds. (Regional Centre for judicial training on Cybercrime, Zagreb, Croatia (TBC))	12-13 October 2016
6.2	Training of trainers on delivery of the training module on cybercrime, electronic evidence and online crime proceeds.	April 2017
6.3	Preparation of updates of introductory and advanced training modules in cooperation with judicial training institutions and trained trainers.	
	6.3.1 Advice on developing introductory and advanced training modules on cybercrime, electronic evidence and online crime proceeds.	January-June 2017
	6.3.2 Translation.	March 2017
6.4	Delivery of pilot introductory and advanced training courses in judicial academies in each beneficiary.	
	6.41. Albania: Two pilot training sessions on introductory and advanced training courses on cybercrime, electronic evidence and online crime proceeds.	May 2017 2018
	6.4.2 Bosnia and Herzegovina: Two pilot training sessions on introductory and advanced training courses on cybercrime, electronic evidence and online crime proceeds.	May 2017 2018
	6.4.3 Montenegro: Two pilot training sessions on introductory and advanced training courses on cybercrime, electronic evidence and online crime proceeds.	June 2017 2018
	6.4.4 Serbia: Two pilot training sessions on introductory and advanced training courses on cybercrime, electronic evidence and online crime proceeds.	July 2017 2018
	6.4.5 "The former Yugoslav Republic of Macedonia": Two pilot training sessions on introductory and advanced	August 2017 2018

	training courses on cybercrime, electronic evidence and online crime proceeds.	
	6.4.6 Turkey: Two pilot training sessions on introductory and advanced training courses on cybercrime, electronic evidence and online crime proceeds.	September 2017 2018
	6.4.7 Kosovo*: Two pilot training sessions on introductory and advanced training courses on cybercrime, electronic evidence and online crime proceeds.	September 2017 2018
Result 7	**International cooperation and information sharing strengthened between cybercrime units, financial investigation units and financial intelligence units (FIUs) as well as between competent authorities for judicial cooperation.**	
7.1	Carry out analysis of issues regarding international cooperation between cybercrime units, financial investigation units, FIUs, and prosecution services.	
	7.1.1 Seven initial country visits.	14-15 April 2016 - Serbia 18-19 April 2016 - Montenegro 21-22 April 2016 – "The former Yugoslav Republic of Macedonia" 5-6 May 2016 - Bosnia and Herzegovina 9-10 May 2016 - Albania 12-13 May 2016 - Turkey 19-20 May 2016 - Kosovo*
	7.1.2 Initial Situation Report.	July 2016
7.2	Regional workshop on international cooperation between cybercrime units, financial investigations units, Financial Intelligence Units, prosecution and competent authorities for judicial cooperation (combined with the Opening Conference of the iPROCEEDS project).	13-14 June 2016 – Ohrid, "the former Yugoslav Republic of Macedonia"
7.3	Elaboration and promotion of domestic protocols for international sharing of intelligence and evidence.	
	7.3.1 Elaboration of domestic protocols for international sharing of intelligence and evidence.	November 2016 – September 2017
	7.3.2 Albania: Workshop on domestic protocols for international sharing of intelligence and evidence.	April 2017
	7.3.3 Bosnia and Herzegovina: Workshop on domestic protocols for international sharing of intelligence and evidence.	April 2017
	7.3.4 Montenegro: Workshop on domestic protocols for international sharing of intelligence and evidence.	September 2017
	7.3.5 Serbia: Workshop on domestic protocols for international sharing of intelligence and evidence.	October 2017
	7.3.6 "The former Yugoslav Republic of Macedonia": Workshop on domestic protocols for international sharing of intelligence and evidence.	3 November 2016
	7.3.7 Turkey: Workshop on domestic protocols for international sharing of intelligence and evidence.	23 November 2016
	7.3.8 Kosovo*: Workshop on domestic protocols for international sharing of intelligence and evidence.	29 November 2016
7.4	Joint workshops at domestic and regional levels on international cooperation and information sharing for cybercrime units, financial investigation units, FIUs and prosecutors.	
	7.4.1 Albania: Workshop on international cooperation and	June 2018

	information sharing for cybercrime units, financial investigation units, FIUs and prosecutors (details and content TBD)	
	7.4.2 Bosnia and Herzegovina: Workshop on international cooperation and information sharing for cybercrime units, financial investigation units, FIUs and prosecutors. (details and content TBD)	July 2018
	7.4.3 Montenegro: Workshop on international cooperation and information sharing for cybercrime units, financial investigation units, FIUs and prosecutors. (details and content TBD)	July 2018
	7.4.4 Serbia: Workshop on international cooperation and information sharing for cybercrime units, financial investigation units, FIUs and prosecutors. (details and content TBD)	February 2019
	7.4.5 "The former Yugoslav Republic of Macedonia": Workshop on international cooperation and information sharing for cybercrime units, financial investigation units, FIUs and prosecutors. (details and content TBD)	February 2019
	7.4.6 Turkey: Workshop on international cooperation and information sharing for cybercrime units, financial investigation units, FIUs and prosecutors. (details and content TBD)	March 2019
	7.4.7 Kosovo*: Workshop on international cooperation and information sharing for cybercrime units, financial investigation units, FIUs and prosecutors. (details and content TBD)	March 2019
	7.4.8 Regional workshop on international cooperation and information sharing for cybercrime units, financial investigation units, FIUs and prosecutors. (details and content TBD)	July 2017
	7.4.9 Regional workshop on international cooperation and information sharing for cybercrime units, financial investigation units, FIUs and prosecutors. (details and content TBD)	March 2018
7.5	Online platform for international cooperation, including on conditions for obtaining data.	June 2017
7.6	Regional workshop to review effectiveness of international cooperation.	April 2019

4. PROJECT LOGFRAME

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.[2]			
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: – By month 32, measureable increase in domestic, regional and international financial investigations in relation to cybercrime. – Upon completion of the project, cybercrime investigations are more systematically accompanied by domestic and international financial investigations to search, seize and confiscate 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): – By month 32, reforms are underway in terms of legislation, institutions and practices and in line with international standards and recommendations. – Upon completion of the project, beneficiaries are compliant with provisions of ETS 185 and 198 that are relevant for cybercrime proceeds.	– 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.

[2] 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)

RESULTS	**OBJECTIVELY VERIFIABLE INDICATORS (OVI)**	**SOURCES OF VERIFICATION**	**ASSUMPTIONS**
Result 1: **Public reporting systems (with preventive functions) on online fraud and other cybercrime improved or established in each beneficiary.**	Presence and performance of public reporting mechanisms in terms of receiving and processing reports and publishing analyses in each beneficiary: – By month 32, public reporting mechanisms have been established or improved in each beneficiary. – Upon completion of the project, public reporting mechanisms receive and process reports and publish 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.
ACTIVITIES			
1.1 Analysis of existing reporting mechanisms.	Research study including country-visits		
1.2 Regional workshops for sharing of good practices.	2 workshops x 30 participants		
1.3 Advice and domestic workshops for the setting up or improvement of reporting mechanisms.	7 in-country workshops Advice		
1.4 Training in the management and use of the mechanisms.	7 in-country workshops		
1.5 Workshops to promote the preparation and dissemination of annual reports.	7 in-country workshops		
1.6 Workshop to review performance of the mechanisms.	1 regional workshop (30 participants)		
1.7 Support to the newly established national Computer emergency response teams (CERT) in information sharing and cooperation with criminal justice authorities.	Advice 1 study visit (14 participants)		
Result 2: **Legislation strengthened regarding the search, seizure**	Number and quality of relevant draft amendments to laws made available to bring legal frameworks of	– Performance review workshops	Draft amendments are adopted by

and confiscation of cybercrime proceeds and the prevention of money laundering on the Internet in line with data protection requirements.	each beneficiary in line with international standards: – By month 32, draft legal amendments available in most beneficiaries – Upon completion of the project, amendments adopted by Governments or working groups and in some instances by Parliaments.	carried out under the Action. – Reports by MONEYVAL and Cybercrime Convention Committee (T-CY).	Parliaments. A clear legal basis will allow for criminal justice action that meets rule of law requirements.
ACTIVITIES			
2.1 Analysis of legislation against EU, FATF and Council of Europe (MONEYVAL) standards and recommendations and regional workshop.	Research study, including country visits 1 regional workshop (30 participants)		
2.2 Advice to public authorities and law reform working groups, including domestic workshops.	7 domestic workshops Advice and desk reviews		
2.3 Regional workshops to review effectiveness of legislation.	2 workshops (30 participants)		
2.4 Online platform for legislation and court rulings.	Consultant services		
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 and vice versa: – By month 34, protocols and procedures established for interagency cooperation in each beneficiary and measureable increase in financial investigations. – Upon completion of the project, increased number and relevance of cybercrime investigations accompanied by parallel financial investigations and vice versa.	– 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.
ACTIVITIES			
3.1 Study and regional workshop to prepare/review/improve training strategies on cybercrime, electronic evidence and financial investigations.	1 study, including country visits		

3.2 Develop guidelines for obtaining and using electronic evidence in criminal proceedings under the respective domestic legislation.	1 Study including country visits 3 meetings of a regional working group Advice		
3.3 Develop and deliver an introductory training module on cybercrime and financial investigations for cybercrime, financial investigation units, FIUs and specialised prosecutors.	Consultant services 1 regional workshop x 30 participants 1 training of trainers session for 21 trainers 7 domestic training sessions		
3.4 Joint workshops and training (regional and domestic) for cybercrime units, economic crime units, financial investigators, FIUs and specialised prosecutors on specific issues (e.g. virtual currencies, terrorist financing, smuggling of persons).	2 regional workshops 7 domestic workshops		
3.5 Design and implement domestic and regional case simulation exercises on cybercrime and financial investigations (e.g. on cases of smuggling of persons).	Consultant services for design of exercise 2 regional workshops 14 domestic workshops		
3.6 Follow up to lessons learnt from case simulation exercises.	7 domestic workshops Advice		
3.7 Advice on the preparation of interagency cooperation protocols.	7 domestic workshops Advice		
3.8 Workshop to assess the functioning of interagency cooperation.	1 study, including country visits 1 regional workshop x 50 participants		
3.9 Support participation in training activities and relevant meetings organised by other organisations.	Travel and per diems		
3.10 Support participation in long-distance master programmes.	Course fees for 14 participants Travel and per diems		
Result 4: **Guidelines on the prevention and control of online fraud**	Increase in the number of financial sector entities that have published indicators based on these	– Performance review workshops	Such guidelines and indicators will

and criminal money flows for financial sector entities developed and disseminated, and indicators for the prevention of online money laundering reviewed and updated.	guidelines: – By month 32, guidelines have been developed and adopted and AML indicators have been updated – Upon completion of the project, financial sector entities have published and apply indicators and guidelines.	carried out under the Action. – Websites of financial sector entities, financial intelligence units and regulators.	help prevent criminal money flows but also improve reporting of suspicious transactions to FIUs.
ACTIVITIES			
4.1 Analysis of indicators and red flags used by financial sector entities to prevent money laundering in the online environment.	1 research study including country visits		
4.2 Analysis of guidelines to prevent and detect/identify online crime proceeds.	1 research study including country visits		
4.3 Regional workshop to share experience on indicators and guidelines.	1 workshop x 50 participants		
4.4 Creation of domestic and regional working groups to elaborate or improve guidelines and indicators.	2 x 7 in-country workshops		
4.5 Dissemination of the guidelines and training in their application.	7 in-country workshops		
4.6 Workshop to review their practical application.	1 regional workshop x 50 participants		
Result 5: **Public/private information sharing and intelligence exchange mechanisms on cybercrime established or enhanced at domestic and regional levels.**	Number of meetings of financial sector ISACs at domestic and regional levels: – By month 32, financial sector ISACs or similar mechanisms established in each beneficiary. – Upon completion of the project, financial sector ISACs will have met at least two times in each beneficiary and three times at regional level.	– Performance review workshops carried out under the Action.	Such mechanisms provide intelligence to prevent threats and enhance knowledge of threats and trends.
ACTIVITIES			

5.1 Assess the functioning of current mechanisms for information sharing and intelligence exchange between financial sector institutions (including processing centres), cybercrime units and other stakeholders.	1 research study including country-visits		
5.2 Organise a regional meeting exchange between financial sector institutions, cybercrime units and other stakeholders to share experience and good practices on such mechanisms.	1 regional meeting (50 participants)		
5.3 Develop guidelines for information and intelligence sharing at national, regional and international levels.	3 meetings of a regional working group		
5.4 Advice and meetings to support existing initiatives or establish such mechanisms at domestic and regional levels.	7 domestic and 1 regional meeting		
5.5 Establish an online resource in support of such mechanisms as well as on law enforcement / Internet service provider cooperation.	1 research contract		
5.6 Workshop to review the performance of information sharing and cooperation mechanisms.	1 regional workshop x 50 participants		
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: – By month 24, specific modules on cybercrime proceeds have been developed. – By month 34, at least two training courses have been delivered by judicial training academies in each beneficiary. – Upon completion of the project, training on cybercrime and electronic evidence is part of the regular curriculum of judicial training academies.	– 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.
ACTIVITIES			

6.1 Regional workshop for representatives of judicial training academy to review the current state of judicial training and agree on project approach.	1 research contract including country visits 1 regional workshop x 30 participants		
6.2 Training of trainers.	1 regional training workshop x 28 trainers		
6.3 Preparation of updates of introductory and advanced training modules in cooperation with judicial training institutions and trained trainers.	Advice Translations		
6.4 Delivery of pilot introductory and advanced training courses in judicial academies in each beneficiary.	2 x 7 training sessions		
Result 7: **International cooperation and information sharing strengthened between cybercrime units, financial investigation units and financial intelligence units (FIUs) 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: – 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.	– 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			
7.1 Carry out analysis of issues regarding international cooperation between cybercrime units, financial investigation units, FIUs, and prosecution services.	1 research contract including country visits		
7.2 Organise a regional workshop on this matter, including mechanisms such as the Egmont Group (for Financial Intelligence Units), the Camden Asset Recovery Interagency Network (CARIN) and the Budapest Convention network of 24/7 points of contact.	1 regional workshop (75 participants)		
7.3 Elaboration and promotion of domestic protocols for	7 x domestic workshops		

international sharing of intelligence and evidence.	Advice
7.4 Joint workshops at domestic and regional levels on international cooperation and information sharing for cybercrime units, financial investigation units, FIUs and prosecutors.	7 x domestic workshops 2 x regional workshops (50 participants)
7.5 Online platform for international cooperation, including on conditions for obtaining data.	1 service contract
7.6 Workshops to review effectiveness of international cooperation.	1 regional workshop (75 participants)