# iPROCEEDS

**Project targeting proceeds from online crime in South-eastern Europe and Turkey (IPA region)**

## Project proposal

Version 26 November 2015

| | |
|---|---|
| Project title / number: | iPROCEEDS (3156) – Cooperation on Cybercrime under the Instrument of Pre-accession (IPA): Project on targeting crime proceeds on the Internet in South-eastern Europe and Turkey |
| Project area: | Albania, Bosnia and Herzegovina, Montenegro, Serbia, "the former Yugoslav Republic of Macedonia", Turkey and Kosovo* |
| Duration: | 42 months (1 January 2016 – 30 June 2019) |
| Budget: | EURO 5.56 million |
| Funding: | Joint project of the European Union (IPA II Multi-country action programme 2014) and Council of Europe |
| Implementation: | Cybercrime Programme Office (C-PROC) of the Council of Europe |

### BACKGROUND AND JUSTIFICATION

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 information and communication technologies (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". 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) and the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS 198) 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 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.

The issue of criminal money flows was furthermore one of the components of the joint EU/CoE project CyberCrime@IPA from 2010 to 2013.

*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.

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

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. With some exceptions, public reporting mechanisms are not yet in place. In most beneficiaries, criminal justice statistics are not available on cybercrime and related fraud.
- 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 public/private information sharing and 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 to update indicators regarding money laundering and additional guidelines to assess risks, and prevent and control criminal money flows online.
- 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 present project will address these issues.

## OBJECTIVE AND EXPECTED RESULTS

| | |
|---|---|
| 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.<br><br>Indicators include:<br>– Extent of financial investigations and prosecutions related to cybercrime and proceeds from online crime<br>– 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.<br><br>Indicators include:<br>– 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.<br><br>Indicators include:<br>– 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.<br><br>Indicators include:<br>– 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 the prevention of online money laundering reviewed and updated.<br><br>Indicators include:<br>– 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.<br><br>Indicators include:<br>– 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.<br><br>Indicators include:<br>– 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.<br><br>Indicators include:<br>– Increase in the effectiveness of international cooperation in terms of timeliness and number of cooperation requests. |

**CONTACT**
Alexander Seger
Head of Cybercrime Division, Council of Europe
alexander.seger@coe.int