

## **iPROCEEDS:**

# **Capacity building on cybercrime and search, seizure and confiscation of online crime proceeds**

Darko Soldat

7 March 2018, The Hague

# iPROCEEDS

Project on targeting crime proceeds on the Internet in South-eastern Europe and Turkey

Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe

|                                |   |
|--------------------------------|---|
| <b>Project title / number:</b> | <b>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)</b> |
| <b>Project area:</b>           | Albania, Bosnia and Herzegovina, Montenegro, Serbia, "the former Yugoslav Republic of Macedonia", Turkey and Kosovo*.   |
| <b>Duration:</b>               | 42 months (December 2015 – June 2019)   |
| <b>Budget:</b>                 | EURO 5.56 million   |
| <b>Funding:</b>                | European Union and Council of Europe  |
| <b>Implementation:</b>         | Cybercrime Programme Office (C-PROC) of the Council of Europe   |

## 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

## Target groups

- Specialised cybercrime units
- Financial investigations units
- Financial Intelligence Units
- Prosecution services
- Judiciary
- Law enforcement and judicial training institutions
- Financial sector institutions

# iPROCEEDS

Project on targeting crime proceeds on the Internet in South-eastern Europe and Turkey

Funded  
by the European Union  
and the Council of Europe

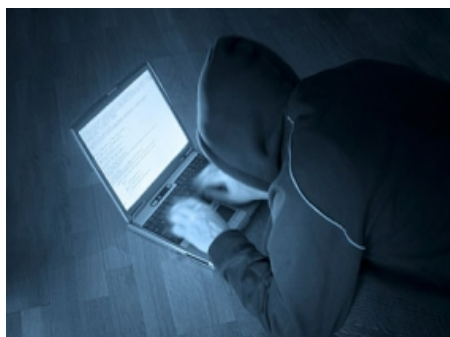


Implemented  
by the Council of Europe

**Standards:** *Budapest Convention, Warsaw Convention, FATF Recommendations*

**Main target groups:**  
*cybercrime and financial investigators, FIUs, prosecutors*

**Cybercrime investigations** are accompanied by **financial investigations**



Search, seizure  
and confiscation  
of cybercrime  
proceeds



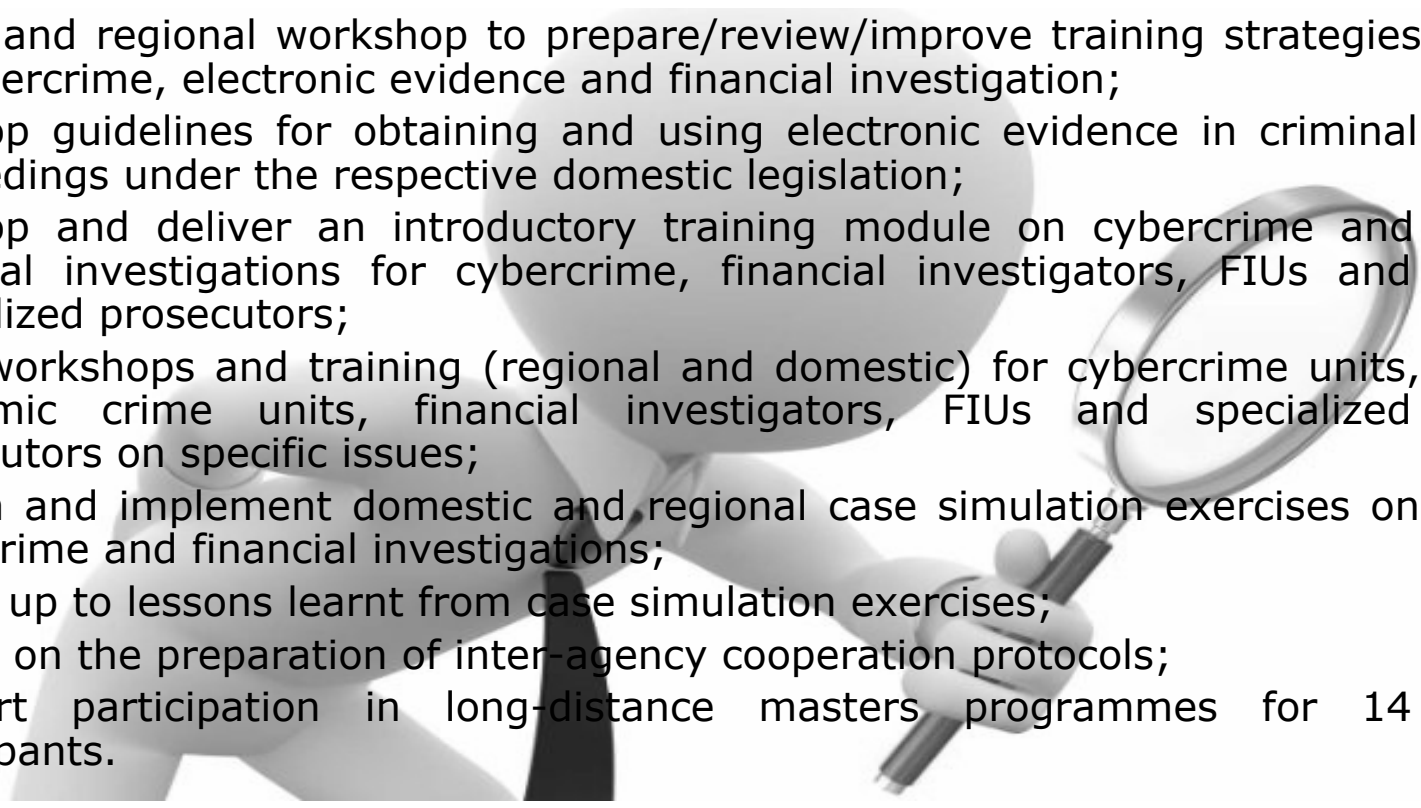
## Result 1: Public reporting systems (with preventive functions) on online fraud and other cybercrime improved or established in each beneficiary

- Advisory missions and workshops to improve/set-up reporting mechanisms;
- Regional workshops for sharing international/regional good practices regarding reporting mechanisms;
- Workshop in the management and use of the reporting mechanisms;
- Workshops to promote the preparation and dissemination of annual reports on the cybercrime situation;
- Regional workshop to review performance of the reporting mechanisms;
- Support to newly established CERTs.

## 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.

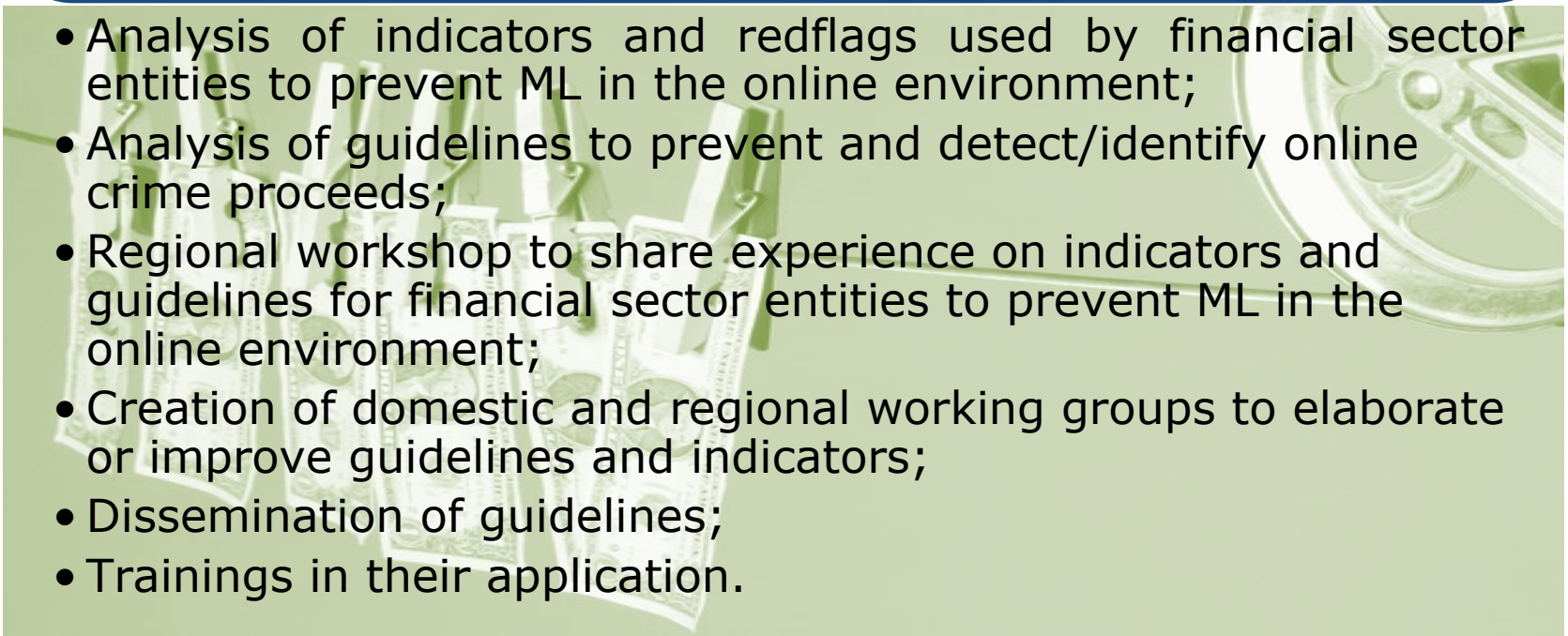
- Analysis of legislation against EU, FATF and MONEYVAL standards and recommendations;
  - Regional workshop on ML risks related to new technologies;
  - Advice to public authorities and law reform working groups available to bring legal frameworks of each beneficiary in line with international standards;
  - Regional workshops to review effectiveness of legislation;
  - Online platform for legislation.
- 
- A decorative graphic of a yellow scroll with a red wax seal, partially unrolled, positioned behind the list of bullet points.

## 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.

- Study and regional workshop to prepare/review/improve training strategies on cybercrime, electronic evidence and financial investigation;
  - Develop guidelines for obtaining and using electronic evidence in criminal proceedings under the respective domestic legislation;
  - Develop and deliver an introductory training module on cybercrime and financial investigations for cybercrime, financial investigators, FIUs and specialized prosecutors;
  - Joint workshops and training (regional and domestic) for cybercrime units, economic crime units, financial investigators, FIUs and specialized prosecutors on specific issues;
  - Design and implement domestic and regional case simulation exercises on cybercrime and financial investigations;
  - Follow up to lessons learnt from case simulation exercises;
  - Advice on the preparation of inter-agency cooperation protocols;
  - Support participation in long-distance masters programmes for 14 participants.
- 
- A 3D rendered figure of a person in a white suit and tie, holding a large magnifying glass over the list of activities.



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.

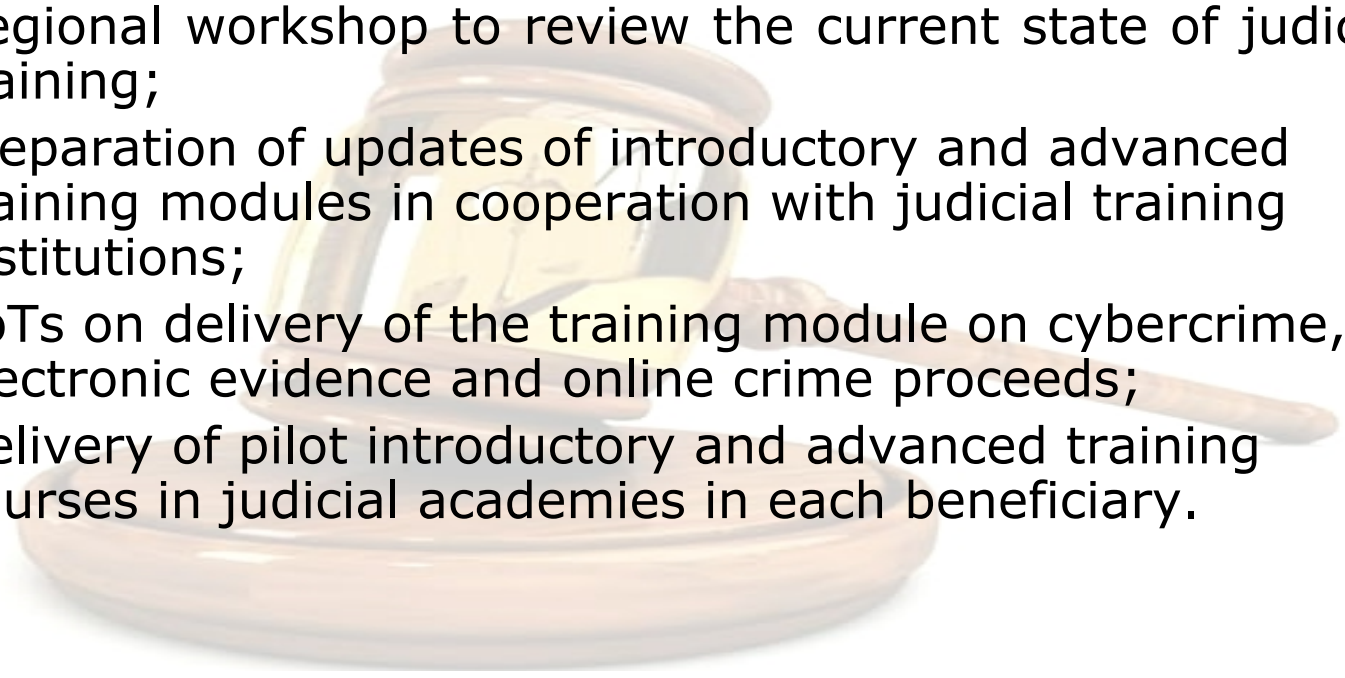
- 
- A background image showing several Euro banknotes (100 and 50 Euro) fanned out, with a large, faint watermark of a person's face visible in the background.
- Analysis of indicators and redflags used by financial sector entities to prevent ML in the online environment;
  - Analysis of guidelines to prevent and detect/identify online crime proceeds;
  - Regional workshop to share experience on indicators and guidelines for financial sector entities to prevent ML in the online environment;
  - Creation of domestic and regional working groups to elaborate or improve guidelines and indicators;
  - Dissemination of guidelines;
  - Trainings in their application.



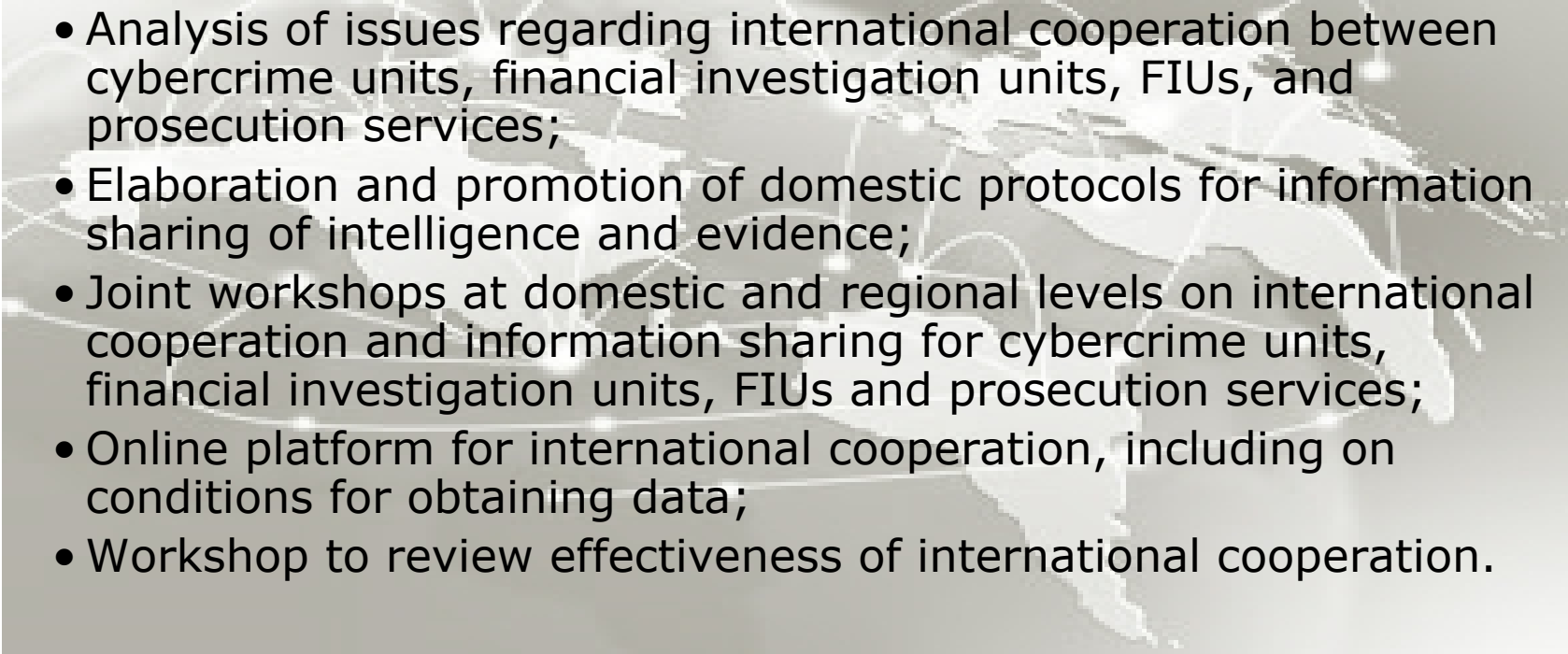
## Result 5: Public/private information sharing and intelligence exchange mechanisms on cybercrime established or enhanced at domestic and regional levels.

- Assessment of the functioning of the current mechanisms for information sharing and intelligence exchange between financial sector institutions, cybercrime units and other stakeholders;
- Develop guidelines for information sharing and intelligence sharing at national, regional and international levels;
- Advice and meetings to support existing initiatives or establish such mechanisms 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.

- 
- Regional workshop to review the current state of judicial training;
  - Preparation of updates of introductory and advanced training modules in cooperation with judicial training institutions;
  - ToTs on delivery of the training module on cybercrime, electronic evidence and online crime proceeds;
  - Delivery of pilot introductory and advanced training courses in judicial academies 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.

- 
- A faint, light-colored map of Europe is visible in the background of the list.
- Analysis of issues regarding international cooperation between cybercrime units, financial investigation units, FIUs, and prosecution services;
  - Elaboration and promotion of domestic protocols for information sharing of intelligence and evidence;
  - Joint workshops at domestic and regional levels on international cooperation and information sharing for cybercrime units, financial investigation units, FIUs and prosecution services;
  - Online platform for international cooperation, including on conditions for obtaining data;
  - Workshop to review effectiveness of international cooperation.



# iPROCEEDS

Project on targeting crime proceeds on the  
Internet in South-eastern Europe and Turkey

Funded  
by the European Union  
and the Council of Europe



Implemented  
by the Council of Europe

[www.coe.int/en/web/cybercrime/iproceeds](http://www.coe.int/en/web/cybercrime/iproceeds)