Capacity building on

Targeting crime proceeds on the Internet

iPROCEEDS

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

Cybercrime economy…in numbers

- $1.5 trillion in revenues every year, if cybercrime were a country it would have the 13th highest GDP in the world (2018)

- $600 billion or 0.8% of global GDP (2018)

- Social media-enabled cybercrimes are generating at least $3.25 billion in global revenue annually (2019)

- England and Wales: 4.5 million cybercrimes (3.24 million online frauds and about 1.23 million were related to computer misuse) with around £130 billion being stolen (2018)

- 10% of the estimated $1.6-$2 trillion of laundered money in circulation can be attributed to cybercrime – totalling up to $200 billion

Most lucrative varieties of revenue-generating cybercrimes:

- Ransomware
- Illicit online markets
- Data trading
- Crimeware
- Payment frauds
- Online frauds
- BEC/CEO fraud

- A wide range of methods and mechanisms for generating revenues, often at industrial scales
- Digitally specific currencies and currency exchange tools
- Data as a commodity and object of value for illicit trading
- A range of specialised economic agents, such as producers, suppliers, service providers and consumers
- Specialised tool supply, technical support and provision of skills and expertise
- Dedicated marketplaces (drugs, firearms, stolen data, fake goods, fake services, fake identity, crime-as-a-service, etc.)

Proceeds of crime/follow the money approach

- Low sanctions for cybercrime (usually suspended sentence, 6 months, 2 years)
- Confiscation of proceeds undermines the financial motive of the cybercrimes
- Attacking assets of cybercriminals undermines their investment in crime/illicit funds
- Re-use confiscated proceeds for crime prevention and social purposes
- Compensate society and businesses
- Raising public confidence in the financial and criminal justice system

iPROCEEDS
EU/COE Joint Project on targeting crime proceeds on the internet in South Eastern Europe and Turkey

► **To strengthen the capacity of authorities in the IPA region to search, seize and confiscate cybercrime proceeds and prevent money laundering on the Internet.**

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

Duration	48 months (Jan 2016 – December 2019)
Budget	EUR 5,56 million
Funding	European Union (IPA II Multi-country action programme 2014) and Council of Europe
	- Albania - Bosnia and Herzegovina - Montenegro - Serbia - North Macedonia - Turkey - Kosovo*

*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.

Public reporting systems (with preventive functions) on online fraud and other cybercrime improved or established

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

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

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

Public/private information sharing and intelligence exchange mechanisms on cybercrime established or enhanced at domestic and regional levels

Judicial training academies are providing training on cybercrime and electronic evidence and related financial investigations and anti-money laundering measures

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

iPROCEEDS: results and impact

Increased number and relevance of cybercrime investigations accompanied by parallel financial investigations

Protocols and procedures established for interagency cooperation in the search, seizure and confiscation of online crime proceeds

Increased technical and practical skills of LEA to search, seize and confiscate online crime proceeds

New cybercrime indicators for the financial sector

Public/private information sharing and intelligence exchange mechanisms on cybercrime with financial sector established at domestic level

Training on cybercrime and electronic evidence and related financial investigations and anti-money laundering measures is part of the regular curriculum of judicial training academies

Enhanced partnerships between IPA national authorities with counterparts from other countries and international organisations

Structured and documented procedures (domestic protocols) for inter-agency cooperation in the search, seizure and confiscation of online crime proceeds

Workshops on inter-agency cooperation and General guide on Protocols on inter-agency and international cooperation for investigations involving proceeds from crime online

Pristina, Kosovo*, December 2016

► **Institutionalised interagency cooperation in the search, seizure and confiscation of online crime proceeds**

Working together to investigate cybercrime and its financial gain

Regional and national case simulation exercises on cybercrime and financial investigations

Bucharest, Romania, November 2018

► **Efficient cross-sector information and evidence sharing between cybercrime units, financial investigation units, FIUs and prosecution services**

iPROCEEDS: activities and results


Dublin, Ireland, December 2018

"Little did I know that UCD could have such a profound impact on me".
İbrahim ÖZDEMİR, Cybercrime Department, Turkish National Police

Master Programme in Forensics Computing and Cybercrime
Investigations, University College of Dublin

► **Equipped with increased knowledge and improved investigatory skills**

iPROCEEDS: activities and results

Responding to the needs and current challenges related to investigation of cybercrime and online crime proceeds
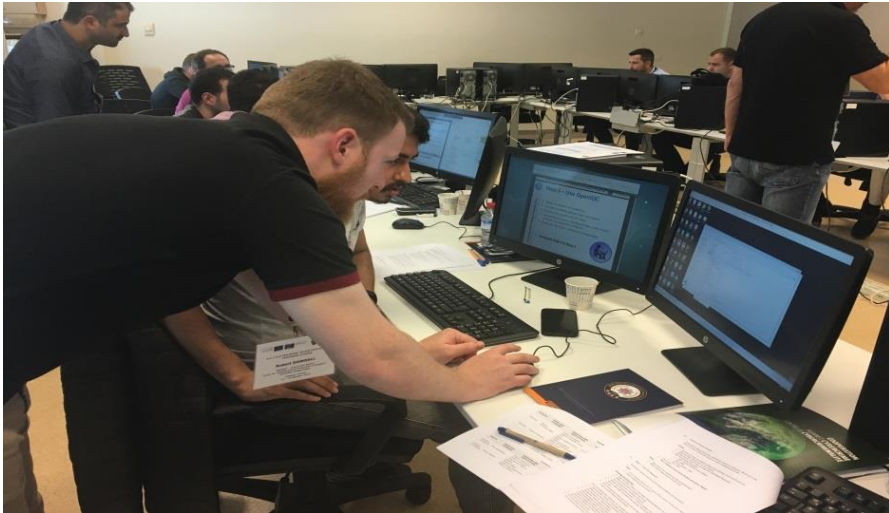
Ankara, Turkey, October 2018

More than 20 specialised trainings and workshops for law enforcement authorities

► **New investigative techniques to search, seize and confiscate online crime proceeds**

iPROCEEDS: activities and results

Support in improving and developing indicators for the prevention and control of online fraud and criminal money flows on the Internet for financial sector entities

Assessment missions to all project countries/areas and reports on indicators, regional workshop on guidelines and indicators, working groups for the review/update of indicators

Ljubljana, Slovenia, October 2017

► **New cybercrime indicators for the financial sector**

Working with the financial sector

Public/private meetings for fighting cybercrime and online crime proceeds in all project countries/areas

Belgrade, Serbia, April 2017

► **Public-private information sharing and intelligence exchange mechanisms on cybercrime established**

iPROCEEDS: activities and results

Improving the knowledge and skills of judges and prosecutors

Review of the current state of judicial training curricula on cybercrime in all project countries/areas; development/update of introductory and advanced training modules; training of trainers; national delivery of training courses in all project countries/areas.

Budva, Montenegro, June 2017

► **Cybercrime training integrated in the curriculum of judicial training institutions. A pool of national trainers available in each project country/area. More than 350 judges and prosecutors trained.**

Thank you!