iPROCEEDS

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

Version 12 February 2018

Activity 6.4.5 Introductory training module on cybercrime, electronic evidence and online crime proceeds

15-16 February 2018 – first part

Skopje

Provided under iPROCEEDS project

in cooperation with the Academy for Judges and Public Prosecutors "Pavel Shatev"

Outline

Background and justification

As the use of and reliance on information technology becomes more and more pervasive in society, the targeting and exploitation of computer systems has also become increasingly common. Nowadays, 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. Offences involving new technology products and services have grown rapidly both in number and in sophistication and have created serious challenges for countries in ensuring that these are not misused for money laundering and terrorist financing purposes. Vast amounts of crime proceeds are generated – and often laundered – on the Internet and through the use of new technologies. These provide a range of opportunities to safely cash out, convert or otherwise clean crime proceeds

Lack of adequate training can be a major obstacle in having judges and prosecutors responding to the threat of cybercrime, online crime proceeds and handling electronic evidence in an effective and efficient way. Hand in hand with these measures is the need to equip key actors in the criminal justice system with the skills and the knowledge to apply them. They need to know and understand the nature and evidential implications of cases of cybercrime and search, seizure and confiscation of online crime proceeds, as well as the available legal instruments and approaches to international cooperation.

The Council of Europe approach to protect societies worldwide in the cyberspace is based on the development and implementation of the Budapest Convention on Cybercrime, through a suitable programme of capacity building for criminal justice authorities. Sustainable Judicial Training programmes on cybercrime, electronic evidence and online crime proceeds are the only effective manner of ensuring that judges and prosecutors have sufficient knowledge to fulfil their roles effectively.

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

Expected outcome

Carried out under Result 6 of the iPROCEEDS project – **Judicial training academies are providing training on cybercrime and electronic evidence and related financial investigations and anti-money laundering measures**, the Introductory Cybercrime, Electronic Evidence and Online Crime Proceeds Training Course is expected to provide judges and prosecutors an introductory level of knowledge on cybercrime, electronic evidence and search, seizure and confiscation of online crime proceeds. The course includes legal as well as practical information about the subject matters and concentrates on how these issues impact on the day-to-day work of judges and prosecutors.

The Introductory Module on Cybercrime, Electronic Evidence and Online Crime Proceeds will last for four days. By the end of this course, the participants will have basic knowledge of:

- cybercrime and electronic evidence;
- financial investigations of cybercrime proceeds;
- how judges and prosecutors can deal with them;
- what substantive and procedural laws as well as technologies can be applied, and
- how urgent and efficient measures as well as extensive international co-operation can be taken.

Participants

This course is for Macedonian judges and prosecutors as part of their continuous training.

Location

Academy for Judges and Public Prosecutors "Pavel Shatev", 12 Jane Sandanski blvd, Skopje.

Programme

Thursday, 15 February 2018

09h00	***Registration of participants***
09h30	**1.1.1. Course Opening and Introductions** • Local trainers
10h00	**1.1.2. Introduction to Cybercrime Threats, Trends and Challenges** • Ms Ivana Trajceva, public prosecutor, local trainer
11h15	***Coffee break***
11h30	**1.1.2. Introduction to Cybercrime Threats, Trends and Challenges (continued)** • Ms Ivana Trajceva
12h00	**1.1.3. Introduction to Technology** • Ms Esther George, Council of Europe expert
13h00	***Lunch***
14h00	**1.1.3. Introduction to Technology (continued)** • Ms Esther George, Council of Europe expert

15h30	***Coffee break***
16h00	**1.1.4. Identifying Suspects on the Internet** - Ms Engjelushe Kadriu Leshi, public prosecutor, local trainer
17h00	***End of day 1***

Friday, 16 February 2019

09h30	**Daily Review** - Local trainers
09h45	**1.2.2. Cybercrime Legislation: Substantive Articles of the Budapest Convention on Cybercrime** - Ms Ivana Trajceva
11h00	***Coffee Break***
11h15	**1.2.2. Cybercrime Legislation: Substantive Articles of the Budapest Convention on Cybercrime (continued)** - Ms Ivana Trajceva
12h00	**1.2.3. Cybercrime Legislation: Procedural Articles of the Budapest Convention on Cybercrime** - Ms Engjelushe Kadriu Leshi
13h30	***Lunch***
14h30	**1.2.3. Cybercrime Legislation: Procedural Articles of the Budapest Convention on Cybercrime (continued)** - Ms Engjelushe Kadriu Leshi
15h00	**1.2.4. National Legislation** - Mr Vladimir Milosheski, public prosecutor
16h00	***Coffee break***
16h15	**1.2.4. National Legislation (continued)** - Mr Vladimir Milosheski
17h00	***End of day 2***