



iPROCEEDS

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

5.4.6 Activity outline

Meeting on Public-private cooperation for fighting cybercrime and online crime proceeds

23 June 2017, Skopje

BACKGROUND

Cooperation between criminal justice authorities and private sector entities, including Internet service providers (ISPs) and financial sector, is essential to protect society against crime. Such cooperation concerns primarily prevention, detection of crime, ensuring necessary evidence for criminal justice purposes, financial investigations and confiscation of proceeds of crime, but also the sharing of information and experience, as well as training.

There are several entities at the national level that have a significant role in the cybercrime area. According to the legislation and their mission, each of them should work in their own areas but, in any case, should be prepared to react in cooperation with the other institutions. The cooperation among the institutions can be impossible or complicated if no appropriate laws and procedures are in place, or if there is no proper understanding of the exact role of the relevant institutions.

The efficient cooperation between the public sector (LEA) and the private sector and appropriate coordination is maybe one of the most important challenges in prevention, investigation and prosecution of offences involving computer systems, computer data and their proceeds.

EXPECTED OUTCOME

The expected outcome of this meeting is to raise awareness on cyber threats, potentials risks, vulnerability and consequences, to provide information on new trends and cyber-criminal activity in the country, present best practices of cooperation and discuss recommendations for improving cooperation. By presenting the capacities and capabilities of each entity involved in the cybercrime and cyber security improved cooperation between the public and private sector is expected to follow.

PARTICIPANTS

Public sector: Representatives of the Cybercrime and Digital Forensics Department of the Ministry of Interior (MoI), Financial Investigation Unit MOI, Financial Police, Financial Intelligence Unit, Ministry of Justice, and the National Bank.

Private sector: – National CIRT, Internet Service Providers, Bank Association, Processing center CASYS.

Funded
by the European Union
and the Council of Europe



Implemented
by the Council of Europe

LOCATION: Hotel Solun, 10 Nikola Vapcarov Street, 1000 Skopje.

Programme

23 June 2017	
08h30 – 9h00	Registration
09h00 – 9h30	Opening <i>Director for Public Security Ministry of Interior, TBC (Cybercrime and Digital Forensics Department)</i>
09h30 – 10h30	Session 1: Financial crime challenges and internet abuse - Presentations/Panel discussion <i>Cybercrime and Digital Forensics Department and Bank fraud forum</i>
10h30 – 11h00	Coffee break
11h00 – 12h00	Session 2: Banking sector - challenges of modern business and cybercrime - Presentations/Panel discussion <i>National Bank and Bank Association</i>
12h00 – 13h00	Session 3: Cooperation between law enforcement agencies and private sector, LEA perspective and challenges - Presentations/Panel discussion <i>Cybercrime and Digital Forensics Department, Ministry of Interior</i>
13h00 – 14h00	Lunch break
14h00 – 15h00	Session 4: Cyber security challenges, ISPs' experience in cooperation with the state authorities - Presentations/Panel discussion <i>Cybercrime and Digital Forensics Department, ISPs, National bank, Bank Association</i>
15h00 – 15h30	Conclusions and way forward
15h30 – 16h00	Networking coffee break