**www.coe.int/cybercrime**

## Activity 1.2.2

# Regional workshop
# on sharing good practices on reporting mechanisms
# in South-eastern Europe and Turkey

## (combined with the 4th meeting of the Project Steering Committee)

### Provided under the iPROCEEDS project
### in cooperation with the Ministry of Interior

## 20-21 December 2017

### Holiday INN Skopje
### Filip Vtori Makedonski, 5

# Outline

## Background

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. Proceeds of crime and income from cybercrime are also undergoing major changes in nature. Virtual currencies make relatively anonymous structured payments a reality, for example. These developments create challenges for both cybercrime investigations and financial intelligence and financial investigations alike. There has been a time lag in developing effective countermeasures.

The timely and efficient reporting of cybercrime to the relevant authorities and ensuring meaningful follow-up of the crime reports through the financial intelligence and criminal justice systems, as well as through appropriate financial investigations is perhaps one of the most important countermeasures against offences involving computer systems and data and their proceeds.

However, experience shows that cybercrime reporting remains problematic for a number of reasons, such as fragmented setup of reporting systems across different

institutions, overlapping jurisdictions, lack of clear guidelines and rules for reporting, and lack of transparency in following up an initial crime report.

To assess the situation, the Council of Europe carried out seven visits in Albania, Bosnia and Herzegovina, Montenegro, Serbia, "the former Yugoslav Republic of Macedonia", Turkey and Kosovo*[1] and met various competent authorities responsible for or affiliated with cybercrime reporting. These missions allowed drawing conclusions and putting forward recommendations for the reform of the systems, with the aim of improving interagency and, possibly, public-private cooperation in exchanging cybercrime-related information.

## Expected Outcome

Carried out under Result 1 of the iPROCEEDS project - *Public reporting systems (with preventive functions) on online fraud and other cybercrime improved or established in each beneficiary* – aims to further improve and/or creation or developing of cybercrime reporting systems in South-eastern Europe and Turkey.

Participants will have a better understanding on the functioning and use of the cybercrime reporting mechanism, practical aspects related to the collection of the reports and the use of the information, good practices on sharing the information at the national and regional level and types of threats addressed through the mechanism.

## Participants

The target audience of the regional workshop is made of representatives of the following institutions/organisations from Albania, Bosnia and Herzegovina, Montenegro, Serbia, "the former Yugoslav Republic of Macedonia", Turkey and Kosovo*:
- Prosecutors specialised in supervision/prosecution of cybercrime cases;
- Cybercrime units (Ministry of Interior);
- Ministry of Justice;
- Computer Emergency Response Teams;
- Internet Service Providers;
- Banking Associations.

## Programme

| 20 December 2017 | |
|---|---|
| 9h00 | **Registration** |
| 9h30 | **Opening** <br><br> – Agim NUHIU, Deputy Minister for Internal Affairs <br> – Representative of the EU Delegation (TBC) <br> – Virgil SPIRIDON, Head of Operations, Cybercrime Programme Office (C-PROC) of the Council of Europe. |
| 09h50 | **Session 1:    Macedonian national online reporting mechanism for cybercrime:  example of good practice in the region** |

---

[1] *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.

| | |
|---|---|
| | – Types of threats to be addressed by the online cybercrime reporting mechanism;<br>– Expected benefits of such a mechanism;<br>– Structure and methods to collect reports and the impact of reports on information sharing, investigation of criminal cases and statistical purposes;<br>– Raising awareness of the public on the use of the online reporting system;<br>– Engaging the private sector (ISPs and financial sector).<br><br>*Speaker: Marjan Stoilkovski, Head of the Sector for Computer Crime and Digital Forensics, Ministry of Interior* |
| 10h50 | Coffee break |
| 11h20 | **Session 2:    Online reporting system for cybercrime in Albania and Kosovo***<br><br>Presentations by delegates from Albania and Kosovo* respectively on:<br><br>– The functioning of the online portal of the Albanian State Police (Ministry of Interior)[2];<br>– The creation of the specialised online reporting system for cybercrime of the Kosovo* Police (Ministry of Interior). |
| 12h20 | Lunch |
| 13h40 | **Session 3:    Reporting cybercrime in South-eastern Europe and Turkey.**<br><br>Presentations by delegates from Bosnia and Herzegovina, Montenegro, Serbia and Turkey (20 minutes each) on various aspects related to reporting cybercrime (types of reported cybercrimes; methods to collect cybercrime reports and the impact of reports on criminal cases; information/intelligence sharing; collection of statistics on cybercrime, etc.). |
| 15h00 | Coffee break |
| 15h30 | **Session 4:    Reporting cyber security incidents in South-eastern Europe and Turkey.**<br><br>Presentations by CERTs delegates (10 minutes each) on functioning of cyber security incident reporting and exchanging information with law enforcement agencies. |
| 16h30 | **Session 5:    Assessment of the existing reporting mechanisms of online fraud and other types of cybercrime in South-eastern Europe and Turkey - presentation of findings following seven assessment visits by Council of Europe**<br><br>– Functioning of various reporting mechanisms;<br>– Common challenges;<br>– Conclusions and recommendations for the reform of the reporting systems, with the aim of improving interagency and public-private cooperation in exchanging cybercrime-related information. |

---

[2] https://www.asp.gov.al/denonco_kk/

| | |
|---|---|
| | *Speaker: Hein Dries, Council of Europe expert*<br><br>Discussions |
| 17h30 | **Session 6:** **Exchanging cybercrime-related information from national reporting mechanisms at the regional level – a view on the creation of a regional information sharing mechanism in South-eastern Europe and Turkey**<br><br>*Speaker: Marjan Stoilkovski, Head of the Sector for Computer Crime and Digital Forensics, Ministry of Interior*<br><br>Discussions |
| 18h00 | **Conclusions** |
| 19h30 | Social dinner |
| **21 December 2017**<br>**4th meeting of the Project Steering Committee – only for project team members** ||
| 9h30 | **Opening and introductions** |
| 09h50 | **Review of activities carried out (July – December 2017)**<br><br>– Overview of progress made towards objectives and results (Project Management Unit at C-PROC/Council of Europe)<br>– Comments by Project Team members. |
| 10h50 | **Project management and implementation matters**<br><br>– Overview<br>– Role of iPROCEEDS National Project Teams and effectiveness of implementation of activities.<br>– Comments by Project Team members. |
| 11h20 | **Workplan for the period January – June 2018**<br><br>– Overview by the Project Management Unit (at C-PROC/Council of Europe)<br>– Discussion and approval of the workplan. |
| 12h00 | **Conclusions and Lunch** |

## CONTACT

For any additional information please contact:

Mariana CHICU
Project Manager
Cybercrime Programme Office of the Council of Europe (C-PROC)
Tel: +40-21-201-7840
Email: mariana.chicu@coe.int

Zlatka MITREVA
Senior Project Officer
Cybercrime Programme Office of the Council of Europe (C-PROC)
Tel: +40- 21-201-7880
Email: zlatka.mitreva@coe.int