Activity 1.3.5

Advisory mission and workshop on online fraud and other cybercrime reporting mechanisms

3-4 August 2016, Pristina, Kosovo*[1]

Provided under the iPROCEEDS project

Outline

Background

As the use of and reliance on information technology becomes ever more pervasive in society, the targeting and exploitation of computer systems has also become increasingly common. Offences involving computers have grown rapidly both in number and in sophistication, but 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 criminal justice system are perhaps one of the most important countermeasures against offences involving computer systems and data. However, 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.

Objective

Carried out under activity 1.3.5 "Advisory mission and workshop for the setting up or improvement of reporting mechanisms" of the iPROCEEDS project, the scoping mission aims to gather specific information regarding online fraud and other types of cybercrime reporting in Kosovo*. The consultants involved will meet various agencies responsible for or affiliated with cybercrime reporting and will draw conclusions and recommendations for the reform of the system, with the aim of improving interagency and, possibly, private-public cooperation in exchanging cybercrime-related information.

A half day workshop at the end of the study visit will serve as immediate follow-up of the scoping mission to share the preliminary findings and observations with the agencies visited, as well as with project counterparts on the performance of the reporting systems (with preventive functions) on online fraud and other cybercrime, as well as interagency cooperation against cybercrime in the context of cybercrime reporting.

Participants

The scoping mission aims to visit investigation and police authorities, communications regulator and/or one or several of the Internet service providers and banking

[1] *The designation is without prejudice to positions on status, and is in line with the ICJ Opinion on the Kosovo Declaration of Independence.

associations – as well as any other player suggested by the host country – to get an overall view of cybercrime reporting situation from the perspective of different players.

The workshop at the end of the mission will involve representatives of the said agencies and/or companies, and will be also used as an opportunity to talk to the country project team.

Expected results

By the end of the activity, preliminary conclusions and recommendations of experts will be voiced at the workshop.

Draft Programme

3 August 2016	
9h00-10h40	Visit a police unit/station that receives complaints from the public, to follow the path of crime reporting/case processing.
11h00-12h00	Visit the Investigation Unit for Cybercrime to examine cybercrime complaints/cybercrime reporting mechanism, as well as cybercrime investigation, including collection of electronic evidence.
12h00-13h00	Lunch
13h30-14h30	Visit the digital forensics unit or other agency or service that deals with electronic evidence.
15h00-16h00	Visit the Prosecutor for Cybercrime cases to examine crime reporting, the supervision of cybercrime investigation, including collection of electronic evidence and prosecution of cybercrime.
16h30-18h00	Visit the communications regulator and ISPs to examine how the service providers submit incidents and/or cybercrime.
4 August 2016	
9h00-10h00	Visit social protection services (child protection, Ombudsman, etc.) in charge of receiving reports regarding potential violations against children.
10h30-11h30	Visit the Financial Intelligence Unit to examine how required reports from the financial sector are received, analysed and how the results of the analysis is disseminated/shared with the law enforcement.
12h00-13h00	Visit a Banking Association and/or a bank to examine existing mechanisms for submitting complaints regarding online fraud and other cybercrime and how these are processed/handled and forwarded to relevant authorities.
13h00	Break
15h00-18h00	Workshop on reporting mechanism with all the agencies and stakeholders met during the advisory mission and the Council of Europe experts to present an initial assessment of the systems of cybercrime reporting, as well as examples of other practices for cybercrime reporting from various jurisdictions and cooperation between the public agencies in in terms of information sharing and cooperation on cybercrime, and some brief overview of public-private cooperation in cybercrime and electronic evidence.