



iPROCEEDS

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

Activity 1.3.2

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

27-28 March 2017, Bosnia and Herzegovina

Provided under the iPROCEEDS project

Outline

Background and Justification

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.

Activity 1.3.2 "Advisory mission and workshop for the setting up or improvement of reporting mechanisms" is intended to support the achievement of the expected result number one **"Public reporting systems (with preventive functions) on online fraud and other cybercrime improved or established in each beneficiary."**

Expected Outcome and Outputs

Specific information regarding online fraud and other types of cybercrime reporting in Bosnia and Herzegovina is expected to be gathered during the various visits undertaken under the scoping mission. The consultants involved, who will have met various agencies responsible for or affiliated with cybercrime reporting, 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.

Funded
by the European Union
and the Council of Europe



COUNCIL OF EUROPE



Implemented
by the Council of Europe

EUROPEAN UNION

CONSEIL DE L'EUROPE

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 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.

Location

The workshop will take place at Ministry of Security of Bosnia and Herzegovina, TRG BiH 1.

Programme

27 March 2017		
Time	Agencies	Contact person and venue
9h00-10h00	Visit a police unit/station that receives complaints from the public, to follow the path of crime reporting/case processing.	Ministry of the Interior of the Federation of Bosnia and Herzegovina, Mehmeda Spahe 7
10h10-11h10	Meeting with the Department for the fight against cybercrime Ministry of the Interior of the Federation of Bosnia and Herzegovina to examine cybercrime complaints/cybercrime reporting mechanism, as well as cybercrime investigation, including collection of electronic evidence in the Federation of Bosnia and Herzegovina.	Ministry of the Interior of the Federation of Bosnia and Herzegovina, Mehmeda Spahe 7
11h10-12h10	Visit the digital forensics unit or other agency or service that deals with electronic evidence.	Ministry of the Interior of the Federation of Bosnia and Herzegovina, Mehmeda Spahe 7
12h10-13h30	Lunch	
14h00-15h00	Visit the Communications Regulatory Agency of Bosnia and Herzegovina to examine how the service providers submit incidents and/or cybercrime reports.	Communications Regulatory Agency of Bosnia and Herzegovina, Mehmeda Spahe 1
15h30-16h30	Meeting with the Federal Prosecutor's Office of Federation of Bosnia and Herzegovina to examine cybercrime complaints/cybercrime	Federal Prosecutor's Office of Federation of Bosnia and Herzegovina, Valtera Perića 15/II

	reporting mechanism, as well as cybercrime investigation, including collection of electronic evidence in the Federation of Bosnia and Herzegovina.	
28 March 2017		
Time	Agencies	Contact person and venue
9h00-10h00	Meeting with the Financial Intelligence Department to examine how required reports from the financial sector are received, analysed and how the results of the analysis are disseminated/shared with the law enforcement.	Financial Intelligence Department, State Investigation and Protection Agency, Nikole Tesle 59
10h30-11h30	Meeting with the Ministry of Security of Bosnia and Herzegovina to discuss the setting-up of the CERT for the institutions of Bosnia and Herzegovina	Ministry of Security of Bosnia and Herzegovina, TRG BiH 1
11h30-12h30	Meeting Republic Prosecutor's Office of Republika Srpska and Section for high-tech crime Ministry of the Interior of the Republika Srpska to examine cybercrime complaints/ cybercrime reporting mechanism, as well as cybercrime investigation, including collection of electronic evidence in Republika Srpska	Ministry of Security of Bosnia and Herzegovina, TRG BiH 1
12h30-13h15	Meeting with Police of the District Brčko	Ministry of Security of Bosnia and Herzegovina, TRG BiH 1
13h30-15h30	<p>Workshop on online fraud and other cybercrime reporting mechanisms</p> <ul style="list-style-type: none"> - initial assessment and corresponding recommendations related to systems of cybercrime reporting in Bosnia and Herzegovina, as well as cooperation between public agencies in terms of information sharing and cooperation on cybercrime, and some brief overview of public-private cooperation in cybercrime and electronic evidence; - examples of practices for cybercrime reporting from various jurisdictions. 	Ministry of Security of Bosnia and Herzegovina, TRG BiH 1