iPROCEEDS

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

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

15 -16 March 2017, Ankara, Turkey

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 1.3.6 "Advisory mission and workshop for the setting up or improvement of reporting mechanisms" is intended to support the achievement of the Expected Result 1 **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 Turkey 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.

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 (TBC) one of the government offices of Turkey.

Draft Programme

15 March 2017		
TIME	**AGENCY**	**VENUE**
9h00-10h40	Visit a police unit/station that receives complaints from the public, to follow the path of crime reporting/case processing.	Kavaklıdere Polis Merkezi Amirliği Güvenevler Mah. Hüseyin Onat Sok. No:17 Çankaya/Ankara
11h00-12h00	Visit the cybercrime unit to examine cybercrime complaints/cybercrime reporting mechanism, as well as cybercrime investigation, including collection of electronic evidence.	Ankara Emniyet Müdürlüğü Siber Suçlarla Mücadele Şube Müdürlüğü Öveçler Mah. Çetin Emeç Bulvarı 1328. Sokak No:3 Çankaya/ ANKARA
12h00 13h00	**Lunch**	
13h30-14h30	Visit the digital forensics unit or other agency or service that deals with electronic evidence.	Siber Suçlarla Mücadele Daire Başkanlığı İncek Mah. Boztepe Sok. No:125 Gölbaşı/Ankara
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.	Adalet Bakanlığı Ceza İşleri Genel Müdürlüğü Namık Kemal Mahallesi, Milli Müdafaa Caddesi No:22, 06420 Çankaya/Ankara
16h30-18h00	Visit the communications regulator and CERT to examine how the service providers submit incidents and/or cybercrime.	Bilgi Teknolojileri ve İletişim Kurumu Eskişehir Yolu 10.Km No:276 Çankaya/Ankara
16 March 2017		
TIME	**AGENCY**	**VENUE**
9h00-10h00	Visit social protection services (child protection, Ombudsman, etc.) in charge of receiving reports regarding potential	Aile ve Sosyal Politikalar Bakanlığı Çocuk Hizmetleri Genel Müdürlüğü Eskişehir Yolu Söğütözü Mah.

	violations against children.	2177 Sokak No:10/A Çankaya/ANKARA
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.	Siber Suçlarla Mücadele Daire Başkanlığı İncek Mah. Boztepe Sok. No:125 Gölbaşı/Ankara
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.	Türkiye Vakıflar Bankası T.A.O. Operasyon Merkezi, Anadolu Bulvarı 145 sk. No:3 Macunköy Yenimahalle/ANKARA
13h00-15h00	**Lunch**	
15h00-18h00	**Workshop on online fraud and other cybercrime reporting mechanisms** - initial assessment and corresponding recommendations related to systems of cybercrime reporting in Turkey, 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.	Siber Suçlarla Mücadele Daire Başkanlığı İncek Mah. Boztepe Sok. No:125 Gölbaşı/Ankara