iPROCEEDS

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

www.coe.int/cybercrime

Version 1 August 2016

Activity 1.3.5

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

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

Provided under the iPROCEEDS project

Report

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

Funded by the European Union and the Council of Europe
EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Implemented by the Council of Europe

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, as previous efforts under the IPA, and GLACY projects show, 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

This mission is carried out under the iPROCEEDS project workplan, activity 1.2.1, as a scoping mission aimed to gather specific information regarding cybercrime reporting in Kosovo*. The consultants involved met various agencies responsible for or affiliated with cybercrime reporting, financial intelligence and investigation, and the reporting of suspicious transactions. They drew 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 served as immediate follow-up to share the preliminary findings and observations and was also used to meet the project team as a whole ad have an interactive discussion.

Participants

The scoping mission visited several investigation and police authorities, the CERT and communications regulator, banks - as well as any other player, such as the Ombudsperson – to get an overall view of cybercrime reporting situation from the perspective of different players.

The following organisations were visited as part of the mission:

- A Kosovo* Police local unit at Police Main Headquarters in Pristina
- The Integrated Financial Investigation Unit and the Cybercrime Unit of the Kosovo* Police
- The Forensics support Unit of the Kosovo* Police
- The office of the Basic Prosecutor for serious crimes in Pristina
- The Forensic support unit of the Kosovo* Police
- KOS-CERT and the Communications regulator ARKEP (co-located)
- The Ombudsperson
- The Kosovo* Financial Intelligence Unit
- The Kosovo* Banking Association.

Visit Summary and Findings

DAY 1: Monday 4th August 2016

1. Kosovo* Police Local Unit at Police Main Headquarters

As one of the major centres in Kosovo*, the local police station in Pristina (located in police MHQ) receives many complaints, including complaints on cybercrime. Police personnel in the unit have a varied level of training and deal with many different types of cases.

Cybercrime is most commonly reported by "walk-in" complainants. Reporting may also take place via e-mail through a single address (info@kosovopolice.com) that is permanently manned by an officer that routes all messages to the relevant units. Kosovo* Police also have a Facebook presence, although this is not used for formal complaints. Lastly complaints may come by phone.

In the most common scenario complaints are taken at the time of reporting at the station. There are many stations throughout the country, all using a similar process.

Usually the officer on duty takes a statement, and notes the complaint on a form that is made for generic crime reporting. In some cases, the shift commander can also get involved in case the case is important or complicated. No specific operating procedure exists for cybercrime cases. Officers that receive crime reports receive training at the Police Academy, both through the ongoing and initial training they provide. There is no specific training or procedure for first responders to cybercrime complaints.

Although there is a minimum reporting level of €25, in praxis complaints of lower value are also registered. After registration the local station will investigate and decide on the case. If a victim does decide not to press charges, the case (including a statement) is still registered and archived at the station. All complaints are also registered in the central police database that can be accessed by officers throughout the country. A central unit uses this database to generate statistics. Both daily and yearly statistics are available, the latter being published at a yearly event by the Director General of the Kosovo* Police. All cases are categorised based on the article of the Criminal Code (CC) that appears to apply, prima facie.

After receiving the statement, the case is then investigated by an investigator, and in co-operation with the prosecutor, a decision is made as to how to progress the case. In certain cases, central units (such as the economic crimes and cybercrime units) can, or must be involved. Cases over €15000 will always be dealt with by central (national) police units, for instance. In praxis all reports about cybercrime are brought to the attention of the central unit. Financial frauds are usually dealt with by the economic crimes unit.

Financial fraud cases can also be referred through the banks, since they require a police report to be present before disclosing details of a fraud to their customer. Banks appear to have an obligation to report if they are a witness to a crime.

Overall the process of taking a complainant's statement takes between 40 to 60 minutes. As regards preventative action, the Kosovo* Police use the UK's community policing strategy that means that local police will actively reach out to the public and key institutions.

2. Meeting with KP Cybercrime Unit and KP Integrated Financial Investigations Unit

The Cybercrime Unit is part of the Kosovo* Police Organised Crime Investigation Directorate. The Directorate for Investigation of Organised Crime is divided into three Sections:

- Section for Investigation of the Organised Crime
- Section for Integrated Financial Investigations
- Section for Investigation of Cybercrimes

The latter was established in 2011 after the 2010 Criminal Code came into force that held many new cybercrimes, implemented in a way coherent with the Budapest Convention (of which Kosovo* is not a signatory due to its international political situation).

The Integrated Financial Investigations Section (IFIS) is intended to co-operate with the Cybercrime Unit (CCU) and the Organized Crime Unit. The co-operation is described as close and very functional – event though there have only been a very small number of cybercrime cases where the IFIS assisted. Whereas the IFIS will deal with the financial aspects, other units are responsible for the investigation of predicate offences. In the case of money laundering it is often the economic crimes department that investigates, however.

In cases of organised crime and cybercrime, the IFIS will go after the assets of the criminal and investigate their families and business relationships. The IFIS also undertakes international investigations in relation to the financial side, often in close co-operation with banks and the Financial Intelligence Unit (FIU).

The CCU takes most cases from reports filed at police stations. The unit is usually contacted if the case relates to cybercrime. Although they are informed this does not mean they will always open a case themselves. They assess the knowledge available at the local station and, also depending on the nature and complexity of the case, may decide to keep the case at the local unit or take it over themselves. In many cases they merely provide assistance. Prosecutors may also open a case, and will then use the CCU for assistance.

The Directorate for Intelligence and Analysis receives all the complaints that are registered in the central police database system (KPIS). They sometimes provide intelligence accompanied by a 5x5x5 form. Cases are assessed by the CCU who conducts a proactive investigation that is led by the prosecutor, in appropriate cases. They use the same forms for initiating a case as are used by the police who receive complaints.

Although most cases are eventually registered on KPIS, the unit may from time to time, hold back certain information, especially when there are operational security considerations for crucial case-related information on the system. All investigative steps are registered in the system, including search, seizure and confiscation warrants and the use of special measures such as interception or undercover operations.

Kosovo* has a hierarchical prosecution service, Basic prosecutors deal with most crimes, whereas special prosecutors deal with pre-defined functional areas, such as organised crime. There is no special prosecutor in the field of cybercrime and basic prosecutors also do not have special education in that area. The CCU and IFIS consider there is a need for such specialised prosecutors, both in cybercrime and financial crime.

In both cases the police believe they have to tell the prosecutor what is needed, rather than the prosecutor providing guidance and advice on the investigation. In a recent development, the CCU now have a prosecutor working with them, in a dedicated fashion, to improve the situation.

In 2015 there were several cases involving "man in the middle" otherwise known as business email compromise or CEO-fraud (where a payment is made into the wrong account, either using a falsified or misleading email address, or by replacing an invoice or payment request by means of intrusion).

Most cybercrime cases come from crime reported at the police stations:

- 2014 - 24 new cases. 14 from stations 10 opened directly by the CCU.
- 2015 - 34 new cases 33 from police stations, 1 directly.
- 2015 - 118 cases of assistance provided by the CCCU for various other sections.

None of the principal cases were based on STR reporting. Where a case involves money laundering (ML) the case is often referred to the economic crimes department, and do not typically fall under the CCU and IFIS. The CCU and IFIS use the FIU (and STRs) mainly for intelligence purposes, and have a good working relationship with them.

As part of the national strategy on Cyber Security the police plan to have a web platform for the reporting of cybercrime. They are very close to making it operational. It will also provide advice to citizens. Although the public will be able to report crime online, victims will still have to be interviewed by the police. The online reporting is only an initial report to trigger police action. Anonymous reporting is only possible via Facebook and the Kosovo* Police email address. It is believed the platform will need to be advertised to make it successful and known to the public.

3. Meeting with the Forensic investigation and support unit

The Forensic Investigation Directorate supports all departments of the Kosovo* Police with a range of forensic services. The Directorate includes the Digital Forensics Unit that has four members of staff. This facility was set up in 2014. There are two civilians and two police staff. The civilian staff has an MSc in computer science. The Finnish Government participated in a project and created a manual for electronic evidence as well as training and certification. The unit also uses the Council of Europe Electronic Evidence Guide for reference. In addition to the typical work the unit undertakes counter terrorist intelligence activity.

The Kosovo* Police funds all hardware and software for the unit, their budget is considered adequate. They use Encase, Winhex and FTK, for media analysis. Internet Evidence Finder to investigate internet artifacts and behavior and CelleBrite and XRY for mobile devices. Although this gives them the capacity to conduct dual tool validation of results, this is not always practiced.

During the visit, however, CoE experts found several issues pertaining to evidence storage and physical security (including the location on the lab on the ground floor: open to attacks) that would be counter to such a certification of the lab under, for instance, ISO 170025 . They notified the unit of their observations regarding the situation.

Regarding financial investigations, the unit indicated they only had limited experience with financial investigations. BitCoin and PayPal transactions were detected on some of the systems they investigated, in combination with the TOR browser. Their main priorities are analytical skills and live forensics.

In 2016 the unit had assisted in 135 cases to date, and capacity is considered adequate.

4. Meeting with the basic prosecutor for serious crime

Kosovo* has a hierarchical prosecution service consisting of Basic prosecutors that prosecute all criminal cases that are not lead by Special prosecutors or Appeals prosecutors. Special prosecutors handle cases that are explicitly mentioned in the law, such as organised crime.

The prosecutor leads the investigation, although police have some ability to conduct investigations independently in the preliminary phase. The Kosovo* Prosecutorial Council has recently deployed the first specialised prosecutors in the field of corruption. It is hoped other functional prosecutors

will soon follow – including cybercrime.

Cases are normally received from the police, especially when it comes to cybercrime. They rarely have any cybercrime case that comes to the prosecutor, unlike other types of crime, which are reported directly. Banks and other organisations often report to the CCU. The prosecutor opens the investigation and the police, under the instruction of the prosecutor, then proceeds to investigate the case.

In cases where the complaint is made directly to the prosecutor, they have full powers in the law to commence proceedings and ask the police for assistance when necessary. When cases are reported to the police they are recorded. All cases are reported to the prosecutor. One officer at each prosecutor's office enters the case data in the database, which is monitored by the prosecutorial council performance unit. This unit will use the information to oversee the quality and quantity of prosecutions delivered per prosecutor in order to assess their performance. Other logs kept by the service include a log of charges, for persons against which charges were pressed and a log with miscellaneous charges.

The prosecutor indicates a preference for using the MoIs independent forensics lab for their cases, although they often have a backlog. This sometimes necessitates the use of the Kosovo* Police forensic unit.

There is a project underway funded by the Norwegian government to be completed in one year to unify databases of all law enforcement and criminal justice systems. Under the new system authorised officers will be able to access the entire new database. At present there would be a difference between statistics provided by police and prosecutors. The difference would be the number of people because the prosecutor can prosecute some but not others.

There is recognition that training is needed in the subject areas of cybercrime, electronic evidence and online proceeds of crime.

5. Meeting with ARKEP and KOS-CERT

Regulatory Authority for Electronic and Postal Communications (ARKEP), the telecommunications regulator of Kosovo*, hosts the National Computer Emergency Response Team (KOS-CERT). The CERT is intended as a national CERT and various sectoral CERTs are envisaged to be established. The CERT is a member of the National Security Council and intends to be TI and FIRST member.

They have just started to offer incident handling services. An online platform was developed recently, where the public can report security incidents. In one case the coordinated with Albania ALCIRT to mitigate 2 Distributed Denial of Service (DDOS) attacks. Communications between them and ISP's is via encrypted channels using PGP. They are following best practice from other CERTS.

ARKEP have drafted a regulation on technical and organisational standards for operations, which is based on the EU Framework Directive (Article 13a).[2] They have defined objectives on security measures, based on ENISA guidelines. These will be subject to a 2-year audit cycle by an external auditor.

They are awaiting publicity on the web site when they will expect more complaints. They will have a link between regulator and the Kosovo* Police service for these complaints. They envisage that

[2] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009.

most consumers will typically complain at their ISPs in first instance, in the case of security incidents, however.

In terms of legislation, lawful interception legislation and data retention are covered in the telecommunications law. No regulation has been issued at the moment.

DAY 2: Thursday 4th August 2016

6. Meeting with the Kosovo Ombudsman office

The first local Ombudsperson was appointed in 2009. In 2015, the responsibility was broadened to cover other subjects such as gender equality. There are five units, children's rights, disability, gender equality and human rights as the overarching subject. There is good cooperation with the police. Recently the police sent a memo asking all stations to cooperate with the Ombudsmperon's office. The institution in relation to Child Abuse Online (CAO) has received no complaints. Previously there had been 2 complaints received but not under the current regime.

Various complaints reporting systems are in operation at the Ombudsperson's office, including one for inmates, that can report anonymously and in writing via special complaint boxes.

The overall process is that the target of the complaint is identified and a legal officer then begins to write official letter to institutions. Letters are signed by the Ombudsperson. The institution is asked on their knowledge and corrective action on the case. Letters are addressed to the head of the institution. Legal officer sometimes has direct interviews. There is a legal obligation to provide answer. In some cases they chose to intervene more informally and this was very effective.

Online reporting and child protection is a new field and limited activity has taken place in this field, so far. It is a priority area for the Ombudsperson, however.

7. Meeting with the FIU

The FIU provided a demonstration of the goAML software which is rapidly gaining popularity in many related (foreign) units. It is easier to co-operate with similar software. Visualisation is done using i2 and iBase as backend. In an example case a number of (cybercrime related) STRs were received and the FIU opened an investigation once they realised that the names suspects were aliases for the same person.

The FIU has access to multiple databases. Requests regarding a named suspect can be sent automatically to all 10 Kosovo* banks and all money transfer agencies, also using the software and the FIU's website. Cooperation with tax authorities and law enforcement (requests inbound and outbound) is also, often, done through the software.

Issues raised by the FIU include: they were not satisfied with the quality of STR's. They gave feedback to the banks and it has improved; they also tell the banks what has happened to the STR. Tax and customs departments are joining together, so the cooperation levels may see an improvement. They do not receive feedback from the police when they send STR's to them.

The FIU consider that prosecutors and judges are a problem, as they do not understand cybercrime. For example, they do not understand that criminals use PayPal as a conduit. In terms of the police, the FIU went to the economic crime unit who did not understand; they then referred the matter to the CCU then to special prosecutor. The FIU prepare intelligence reports using 5x5 with details of all information.

Although the FIU is almost ready to become an EGMONT group member, the latest meeting (to be held in Turkey) was cancelled following an attempted coup d'état. This caused delay to the application process, which is in the final stages after recent amendments to the AML legislation.

The Kosovo* FIU and their staff is extremely knowledgeable and proactive in the area of cybercrime.

8. Meeting with the Bankers Association (BA)

The Bankers Association has 9 of the 10 banks in Kosovo* as members and has 10 committees, including fraud and security. There is an interbank agreement for sharing information about fraud. Where there is a customer complaint, the customer fills out a dispute form and the bank starts an investigation. The customer usually goes to the bank, not the authorities in case of fraud.

Occasionally the police will come to the BA and ask for information. There is no system to report crimes to police. Cases usually involve criminals or aspects of the case that are outside Kosovo*. If the crime is in Kosovo*, and the bank is a victim, they report to the police. Skimming cases are an example. They have meetings with the Cybercrime Unit and they have exchanged contact numbers.

Cybercrime is now more of a concern to the banks than the traditional crimes. They inform customers to be vigilant, to have recent have antivirus software, and not to answer email directly but to check validity by other means.

The individual banks set security policies. For safeguarding credit card transactions, they rely mostly on Visa and MasterCard, for instance for detecting compromised BINs. Four banks are using 3D secure. The BA has seen a huge increase in malware, against both customers and the bank.

STR's go to the compliance departments of the banks and then to FIU. Banks are not receiving regular feedback from the FIU or the police on the results, however. The issue appears that the compliance departments of the banks are not communicating information to their security and fraud staff.

BA gave some feedback on the Cyber Security Strategy. The national CERT has taken several years to set up and no information has been given to the BA about the CERT. They would also prefer a more formal method of communication of complaints to the police.

Workshop

The workshop began with a summary of the activities under the iPROCEEDS project by the CoE representative, followed by two short presentations on existing cybercrime reporting systems and practical issues related to their operation, by the CoE experts.

The Kosovo* Police provided information about their planned web portal and online reporting system. It will be hosted on the Kosovo* Police web site and will have the possibility to report various cybercrimes. There will be some compulsory fields such as the name address and contact details so that they may be contacted; the type of crime and a description of the actions will be included.

The CERT has its own platform for reporting cyber incidents. They say the police initiative is a good idea as the CERT platform can have a link to report directly to the police in appropriate circumstances. The statistics can be collected and analysed for identifying future threats.

The police facility will be secure and only certain people can access the information in the report. The system will use encrypted channels to maintain the confidentially of the reports. The types of crime reported will follow the criminal code which sets out various crimes.

There was an interactive discussion among the participants, primarily looking at how they may cooperate in the future.

Conclusions and Proposals

Conclusions

There is encouraging progress in the provision of updated reporting systems for cybercrime, through the online portals of the Kosovo* Police and the CERT. Once these are active, experience of other countries shows there will be an exponential increase in reports, many of which may not be crimes but disputes. Filtering the reports will be important, as will the ability for crimes reported to more than one portal e.g. to both CERT and police, to be linked.

There is room for improvement in the cooperation between the various players in the criminal justice system. There is no group that looks holistically at the issue of cybercrime and cybercrime proceeds. They are treated as separate issues and although the FIU is extremely proactive in its investigations, the link between cybercrime and online proceeds of crime is not well developed from the investigative perspective. There is a recognition that additional training is needed in the police as well as in the judiciary. Financial investigations into cybercrime are still few and the ML angle to cybercrime needs to be developed in praxis, by paying more attention to these aspects of the cases.

The workshop showed that there is a willingness among the various players to discuss these issues; however, at this time, there is no mechanism for them to meet in the future to continue the discussion and to provide recommendations and a structure for future activity to combat the illegal use of the Internet to counter money laundering and related seizure and confiscation of assets and material gain.

While it is not directly linked to the project, the visit to the Digital Forensics Unit of the Kosovo* Police revealed some areas that may be improved, particularly in relation to the security of the facility and the storage of evidence. In addition, there are no offsite backups of the data recovered from the seized devices. On the day of the visit, the windows were open, and the door to the office was not secure. It would have been possible for someone to have set fire to the office from the outside and potentially destroy the evidence in a large number of cases.

Proposals

Consider creating a working group of the relevant players to engage and discuss future collaboration in the issue of online proceeds of crime, in particular and wider issues such as training, identifying crime patterns, laundering typologies, STR indicators and other relevant subjects.

Consider further integration of the reporting mechanisms of the CERT, the Kosovo* Police and possibly engage the Ombudsperson in relation to children and abuse material. Engage all stakeholders and manage the information flow to create benefits for all stakeholders.

Consider a cybercrime proceeds desktop case exercise with all relevant players in order to identify the challenges of this type of investigation, the responsibilities and opportunities for future collaboration and possible training needs.

Consider improving security and evidence storage within the Digital Forensics Unit.

Consider improving the co-operation of the government agencies involved in cybercrime and financial investigations, with the financial sector and the ISP industry. Awareness and reporting are

shared interests and there is a marked willingness in the financial sector to engage on several topics such as STR feedback and fraud trends.

Consider expediting the creation of the CERT. Not only does it play a crucial role in safeguarding critical infrastructure, it is a good place for co-operation between sectors and public bodies.

Consider specialised prosecutors for cybercrime and advanced financial crimes/money laundering.