iPROCEEDS

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

www.coe.int/cybercrime

Version 27 October 2016

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

29-30 September 2016, Tirana, Albania

Provided under the iPROCEEDS project

Report

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 1.3.1, as a scoping mission aimed to gather specific information regarding online fraud and other types of cybercrime reporting in Albania. The consultants involved met various agencies responsible for or affiliated with cybercrime reporting and 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 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, and other relevant players suggested by the host country, such as the ombudsman – to get an overall view of cybercrime reporting situation from the perspective of different players. Unfortunately the CERT, ALCIRT did not send any representatives to the meetings. Also no representatives of the ISP industry were present.

The following organisations were visited as part of the mission:

- A police station in Tirana, where citizens can report crime in person;
- The Cybercrime Sector in the Ministry of Interior;
- The Albanian Financial Intelligence Unit;
- The IT Forensics Support Unit of the Scientific Police Forensics Directorate (Police, Ministry of Interior);
- The General Prosecutor's Office;
- The Ombudsperson;
- The Albanian Banking Association.

Visit Summary and Findings

DAY 1: Thursday 29th September 2016

1. Albania Police Local Unit of the Tirana Police Directorate

As one of the major centres in Albania, the police station in Tirana, receives many complaints, including complaints on cybercrime. Reporting in person in one of the methods available to victims for the reporting of crime. There are specific desks on the ground floor of the building to allow easy access for members of the public to interact with the police on a wide range of issues. The staffs at these desks are not trained in any specific crime area. They take the report of the crime and contact the operation centre, which allocates a case number and identify an officer to deal with the complaint. This officer is responsible for taking the detailed complaint. He may call on specialists in this process but this is an ad hoc decision.

If a crime is identified, they issue a case number. The case number remains with the case, which is then forwarded to the prosecutor, who has responsibility for the investigation process. The Prosecutor's Office has a separate, manual recording system and they allocate their own case number. There is no interaction between the police recording system and that of the Prosecutor's Office. The Criminal Procedural Code says they should decide in three months and they may dismiss, delay or prosecute the case; the prosecutor may take up to two years to render a final decision on a case or three years in serious cases. The prosecutor may ask the police or the judicial police to investigate on their behalf. Complaints may be made directly to the prosecutor and the police may never know an investigation is being conducted. Businesses may also report cybercrime in the police station and are known to do so.

Reports of crime to the police are recorded on the TIMS system (other information such as border crossings is also registered there). The MEMEX system is used for all information and intelligence received by the police and is able to provide links between reports. 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.

In addition to the ability to report cybercrime personally, victims have options to report via telephone, the Albanian State Police website, email or by using an app that has been created for the purpose and which is available for both iOS and Android devices. Experience of other countries shows there will be an exponential increase in reports once online reporting is widely used, many issues may also not relate to crimes but disputes or intelligence. Filtering these reports will be important as will the ability for crimes reported to be gathered centrally and to be linked. The creation of an online resource for reporting crime may also be a resource for alerting the public of types of crime being committed in a country, and against which the public may be able to adopt prevention measures. In addition this type of resource may also be used to disseminate similar information that may be available from other players such as banks, CERT's and others affected by cybercrime. Having a "one stop" resource is much more likely to be seen as valuable by citizens, rather than having separate sector resources. At present Albania may consider the threat of cybercrime is not so well developed as to merit such a resource, however this is precisely the time to plan for such an eventuality and create the partnerships necessary.

At the moment, accurate statistics across the criminal justice system are not well developed. They could certainly be improved.

2. Meeting with Albanian Cybercrime Sector

The Cybercrime Sector is part of the Albania Police Organised Crime Investigation Directorate.

The biggest source of work for the Cybercrime Sector is reports from citizens or reports from officers who take reports from victims. In terms of statistics, the statistics from the Cybercrime Sector are analysed by the head of Sector. The Analysis Department analyse the overall statistics and make recommendations for changes in internal rules, legislation etc. The Director of police issues statistics on numbers of crime.

It is considered that the impact of cybercrime on the public is great, now being the major crime committed against citizens. As a result the Cybercrime Sector is of the view that the sector should have the status of directorate that also deals with online money laundering, proactive investigations and has some digital forensics capability. The sector is involved in prevention activities through media, meetings at schools and online. Statistics are only available at the sectoral level and the publicly available statistics are rather aggregated. More detailed statistics are only used internally and are not made public.

In terms of reports received from other organisations, the sector reports that they do not normally receive direct complaints from banks although their customers report illegal activity to the banks. On the rare occasion that banks do report, they do report to the police. The Banking Association came into existence because of the cybercrime issue and the police did want to cooperate but reportedly the association did not respond. They will not agree to a meeting with the police to discuss matters of common interest. Reports are sometimes received from other government agencies, such as the tax administration.

It appears that government departments prefer to report criminal matters directly to the prosecutor rather than the police, although the police may of course, may be asked to investigate by the prosecutor. The Albanian CERT (ALCIRT) may also receive reports of cybercrime and the police do receive reports from them, as there is an existing relationship. The CERT try to avoid being involved in the investigation process, as they do not welcome the associated publicity. The Cybercrime Sector state that they need the same level of cooperation with the Internet industry but at the moment they do not cooperate.

There are some concerns in the sector that the knowledge on cybercrime and electronic evidence in the Prosecutors' Office is in need of improvement. They disagree with some decisions the Public Prosecutor Office has taken on cybercrime cases. Although the situation has improved since the early issues in 2009, in that there is a cybercrime prosecutor in Tirana and one in each of the regions, it is considered that the overall knowledge, especially because of the impact of electronic evidence on a wide range of cases is not generally sufficient. A similar situation exists with judges.

In relation to dealing with enquiries from and making request to other countries, the listed person 24/7 Point of Contact (POC) present in the Cybercrime Unit left the police some time ago and has not been replaced at the moment of the visit. Reportedly, after the visit the 24/7 POC was updated accordingly. There are different POC's for Interpol, Europol, G7 and Council of Europe.

The Cybercrime Sector does not have effective relationships with the ISP industry and there are no discussions between the groups to deal with the mechanisms for dealing with lawful requests for preservation or access to data. Data retention legislation is in place and the police are able to obtain lawful access to data through the prosecutor, however they consider that access to data in pre-investigation phase is needed, in order to improve the effectiveness of investigations.

3. Meeting with the Forensic Investigation and Support Unit

The Digital Forensics Unit is part of Scientific Police Forensics Directorate and was created in 2009. Since inception, there have only been four members of staff, however the number has recently been doubled, primarily because the backlog of cases now runs to two years.

They have good cooperation with the International Criminal Investigative Training Assistance Program (ICITAP) who are running a project to enhance the knowledge and skills of the new staff with a seven week training programme in the forensic products Cellebrite and Encase. In addition, the unit uses Winhex (by X-ways) and Internet evidence finder. Their primary tool for examining mobile phones is the Cellebrite UFED and UFED link analyser, which allows up to 100 device extractions to be analysed for links. In addition, they have one licence for XRY. The hardware in the laboratory is out of date and the ICITAP programme is funding a replacement programme that will see the equipment replaced with up to date bespoke digital forensic "FRED" computers. The unit has been working on the preparation of Standard Operating Procedures and these are currently awaiting approval.

The unit holds general statistics for all types of crime submissions and has had five cases involving child abuse in the current year. Drug trafficking makes up the majority of submissions with financial crimes also predominant. When the unit identifies the existence of criminal assets during forensic examinations, they sometimes refer the matter to the Financial Intelligence Unit (FIU). They have only encountered one case involving virtual currency, but no evidence of transactions. In addition to the cases received from the police, the unit also receives cases from the prosecutor and sometimes from the court.

The current backlog of 2 years is concerning and the unit will need to adopt a strategy to deal with this that does not rely entirely on the acquisition of an increased number of staff.

4. Meeting with the General Prosecutor's Office

In Albania the prosecutor can start an investigation by many means, by report from victim, police or by seeing something in the media or any other source of information. Cybercrime is treated in the same way as other crimes. Anyone who is aware of a crime has a legal responsibility to report a crime. The term "hurt person" is used instead of victims except when dead. The banks also are obliged to report but have exemptions.

Most cybercrime reports come from the police. The prosecutor considers that maybe a campaign is needed to inform the public about cybercrime and how to report it. Statistics may vary between the police and the prosecution as the police and prosecutor's data on cybercrime are different.

When the prosecutor starts a case they can ask the police to investigate under the supervision of the prosecutor. They usually use the national police rather than any other branches of the judicial police. Specialised cybercrime prosecutors have been in place since 2014. There is a sector where there are prosecutors who have been chosen on their CVs and interviews in 8 prosecution offices. There are 16 in total with one prosecutor and one judicial police in each region. The general prosecutor deals with all cybercrime cases.

Another directorate in the Prosecutor's Office deals with financial investigations and with the FIU. They have not seen anything to do with cybercrime in financial fraud cases.

Each prosecutor has their own register and each prosecutor reports on the status of their cases every three months. Currently there is no centralised system, however there is a new system to

computerise the case management system. The CAMS system is being developed under an EU project and will have interaction with the police.

The prosecutor identified the main problem as digital forensics, because the delays are unacceptable. They are considering having a capability in the Prosecutor's Office. The police Cybercrime Unit is also considering its own forensic capacity.

International cooperation cases are the problem with no reply being received from many jurisdictions. They use direct access to Facebook etc.

In terms of future activity, the idea is for the Prosecutor's Office to have a small classroom to update staff with information and have training. School of Magistracy does some seminars but there is a need to improve the knowledge by providing in depth trainings and continuing education. There is recognition that training is needed in the subject areas of cybercrime, electronic evidence and online proceeds of crime. They also recognise a need for better liaison with the banks.

DAY 2: Friday 30th September 2016

5. Meeting with the Financial Intelligence Unit (FIU)

The FIU in Albania has an administrative character. Their mandate is covered by the Law on Anti-money Laundering and Counter Terrorism (AMLCT). The FIU is an independent body and cooperates with national and international organisations. Albania is a member of the EGMONT Group. The unit was set up in 2001 and in the beginning it was difficult to impose a culture of reporting on the various entities. It took many years to standardise the methods of reporting. They apply preventative mechanisms and have been commended internationally for this. Recently the Basel Institute published a report on good governance and Albania is listed in the top ten countries that have made progress.

The FIU has 28 staff in four departments. There is the General Directorate and three other, the Operations and Strategic Department, with 14 staff, the Compliance and Analysis Directorate supervising the entities and the Foreign Relations and Legal Department. Staff numbers have gradually increased and further increases are being considered.

In 2012 the law was changed to make the institutes analyse all transactions and not just report everything. The FIU conducted awareness activities, through inspections and reminding institutes if they had not sent any reports. These were asked to send their analysis of transactions even if they were not reportable. The information provided from the previous 3 years from the banks on cybercrime are currently being analysed to see what they can gather. In addition they are looking at all the transactions individually.

Cash transactions over €7,000 have to be reported to the FIU and suspicious transactions which are not dependent on the amount. Since 2012, attempted transactions also have to be reported. The work of the unit is based of the reports received and on databases they have access to, such as criminal convictions registry, passport registry, customs and tax records, real estate register (for Tirana), motor vehicle registrations and other relevant information held by the state.

When the initial investigation is completed and is deemed to require further action, it is submitted to the police and the prosecutor. The submission will be on the basis that they identify the predicate offence or where they have strong suspicion of criminal activity. The unit has freezing powers for transactions.

Until 2014 the FIU used to receive about 500 suspicious reports per year, mainly from the banks. In the last years this has increased to 1300 or 1400 per year. Up to 2104 they used to submit 200 to 250 cases per year to the prosecutor. Since them they have submitted up to 400 per year.

45million euro has been seized in the past year with 80% being sequestered. Sequestration began in 2009 following information received from the US about how it could be used in dealing with these types of crime.

The government is taking the subject this seriously to the extent that specific structures have been set up to deal with this in the directorate of economic crime, with whom the FIU have good relationships. The FIU has seen various typologies of crime and published their opinion on this. In terms of protection of the information held, the FIU system has been certified for its security.

Banks were not really clear if cybercrime cases needed to be reported to the FIU. They left it to the victim to report it to the relevant authorities. Previously they had received sporadic STR's from banks relating to cybercrime. Occasionally they have received requests from the police to access data held by them in relation to cybercrime investigations. In May 2016 the FIU sent a letter to all the banks in Albania to raise their awareness of the threat of cybercrime and requested they immediately report all such cases to them. The banks provided data on the three previous years and now they report all such cases.

The main types of cybercrime they encounter are hacking into email accounts and changing the destination IBAN number. The governor of the Central Bank has also made public statements on this issue. There have been attempts to warn the public about this type of crime and to ensure their vigilance. The FIU is looking at these transactions on an individual basis in conjunction with counterparts in other countries. In many instances money is transferred from its original destination to elsewhere, so tracing the money after the transaction is not often successful in these cases. The measures the FIU took meant that the banks often report cybercrime cases as STR's.

The FIU, and the Governor of the Central Bank have raised the awareness of many entities about 419 type frauds and in one case prevented a transfer of €7,000 to protect the victim. They have also taken a strategic look at money transfer services that send money to suspicious countries. They want to identify the extent that money transfer services are used for money laundering purposes and those of trafficking of humans. The main crime typologies are "man in the middle" and 419 frauds. Three days before the visit, a bank reported that a client account had been hacked into, they saw an unusual transaction request and on checking the customer it was established it was an illegal transaction and stopped. It was valued at about €90,000. In another case a bank informed the FIU of a foreign citizen they issued a card to. There were transactions but he had not entered Albania. The FIU suspected that something was wrong but it turned out he was a fisherman and entered the country at various times. He was not on the TIMS system and should not have been entering the country without registering and they thought he was there to commit fraud. He came under another regime and his entry was not entered in the TIMS system. The FIU is aware of card cloning activity but the police deal this with.

The FIU consider there is room for improvement in the reporting system. They have had cases that have been reported but not quickly enough. In one case €800,000 was lost from an experienced businessman because the bank reported late and they could not freeze the transactions. A measure that could still be taken is to improve the system of contact persons in each bank.

Banks have a responsibility to conduct due diligence on all their activities to protect customers. In the May 2016 letter, the FIU explained to the banks their obligations under the law to vet all

transaction even if authorised by the customer. One of the main issues was the amount of analysis required on the part of the banks. In particular they should examine any transactions not matching the business of the client or where they is an unusual nature of the transaction or the destination. They should ask the client questions to ensure the validity of the transaction. The immediate reporting of the transactions to the FIU is essential. The FIU has also reported to the police AML Department the details of all cases with a view to identifying organised crime groups.

The FIU has seen some cases involving virtual currency, this has not yet been a major problem. At the moment they are examining precisely such a case. It is not considered yet to be widespread but they have discussed this with the banking industry and are preparing their policies on the issue.

The workload of the FIU has increased significantly, and the budget has not kept up. This situation is not desirable and could be improved.

In terms of enforcement, the FIU has fined a number of entities and also has a constant programme of training for the banks compliance officers and also for the cashiers and other bank staff including legal staff, in Tirana and other regions. All public notaries have been trained (they were prone to underreporting). They meet every three months to share information. They have also been meeting with car dealers, construction companies, money transfer companies and others. Some individual bank staff have been reported to the prosecutor for non compliance. The banks now allow the FIU a role in their training programmes.

6. Meeting with the Albanian Ombudsperson

The Ombudsman deals with complaints from citizens and also undertakes self-initiated activity. Their remit is to deal with issues that are not being effectively dealt with by state institutes. They normally receive complaints when something has not worked in state bodies. When they find something wrong with legislation they can submit recommendations to departments to improve their legal or regulatory frameworks. In the area of cybercrime they have received no complaints.

According to the Ombudsman, it is a new area and Albania lacks the public awareness of the risks of cybercrime, especially in relation to children and their parents or caretakers. There is a cybercrime unit at the Prosecutor's office and in the police. They have not had the chance to look at their functioning because they have not received complaints. There have been fake Facebook accounts in the Ombudsman name. They reported the case to the prosecutors and police but have had no response.

The Section for the Protection of the Right of the Child is planning some activity to monitor the use of the Internet. It is considered that there are many problems with this with the media, ethics and parental guidance in the area of cybercrime. It is new to Albania so there is much to do to understand the challenges. They are aware that 13 to 18 year olds use smart phones with access to the Internet. 85% have access to Internet in Albania according to the World Forum Study.

7. Meeting with the Albanian Banking Association

The Association has existed since 2000 and has in the region of 17 members. There are different committees including anti money laundering. They see continuous threats from cybercriminals on a daily basis. They are seeing phishing and ransomware cases. Companies have suffered from phishing and man in the middle attacks, together with customer's information being captured while they are on Chinese websites. The banks do not refund losses to customers in this type of case. The banks have dual verification by email and phone. There is a regulation that the person must

be present for a transaction made by the customer. In reality, what happens is that the customer does not want to go to bank so they agree to take liability and conduct the transaction by phone. It is considered that the banks are well protected but customers are not. The Banking Association is preparing new advisories for the public.

In terms of cooperation with government agencies, the association is not complimentary about the authorities and would be willing, for example to have conversations with the police if the police would exchange information. In the view of the Association ALCIRT do not have the ability and knowledge to be able to deal with cybercrime or protect their customers. ALCIRT has been in existence for five years, have six members of staff and yet have limited capabilities for security.

The Association does report to the police if there is an ATM or card fraud. This is reported to the Economic Crime Directorate with mixed results as far as subsequent investigations are concerned. The Association would consider it useful if threat intelligence about the dark web (identities and bin lists) could be made available by the authorities to the banks, as this activity is expensive for the banks.

Workshop

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

The workshop showed that there is a willingness among the various players to discuss these issues; ISPs however were absent from the meeting. Also, 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. The demand for such an exchange was not only mentioned in relation to the national level, but was discussed also as a regional issue. There is recognition that there is a need to cooperate in the region too.

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

Conclusions and Proposals

Conclusions

The mission identified an encouraging status quo regarding the provision of reporting systems for cybercrime. The use of a mobile reporting app is a best practice that is not always found in the region. Reporting is possible through the online portal of the police (Ministry of Interior), where citizens may denounce cybercrime.[1] Issues exist in public-private cooperation and especially, cooperation with ISPs and banks.

The CERT, ALCIRT currently is set up to have the government as constituency. They appear to have a reporting form on their website, this process could not be studied however, as no representative was met. Since it is the only CERT in the country, "de facto" functions as a national CERT until a national CERT is created.

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

Reporting is still largely done in person, however, at the police station. Experience of other countries shows there will be an exponential increase in reports once online reporting is widely used, many issues may also not relate to crimes but disputes or intelligence. Filtering these reports will be important as will the ability for crimes reported to be gathered centrally and to be linked. For this Memex is used as an intelligence tool in Albania. Statistics are not very developed. They could certainly be improved.

There are also opportunities to improve in the cooperation between the various players in the criminal justice system. There is currently no active group that looks holistically at the issue of cybercrime and proceeds from crime online. They are treated as separate issues and although the FIU was successful at engaging with the banking sector to improve cybercrime reporting (it is a very good example in the region and it is worthwhile to examine further), the link between cybercrime and online proceeds of crime is not well developed from the investigative perspective. The Cybercrime Sector has not received cases from the FIU for instance, but instead these are reported to the Economic Crime Sector as money laundering cases.

There is recognition that training is needed in the police as well as in the judiciary. Financial investigations into cybercrime are still few and the money laundering angle to cybercrime needs to be developed in praxis, by paying more attention to these aspects.

The meetings with various players demonstrated a commitment of the country to engage in the iPROCEEDS project. Some key players did not respond to the invitation, however. Especially the lack of ISP cooperation was a noticeable issue.

As regards reporting systems, the Albanian system has the makings of an effective reporting system, although online reporting volumes seem low. Speaking to each complainant in some cybercrime cases (mass frauds) seems impossible in the long run.

The FIU has a good track record in engaging the banks in STR reporting for cybercrime related cases. They have been engaging actively with the banks, and developed an effective culture of reporting that is based on pro-active investigation. Further examination of their practices, for instance through presentations at regional events in the project, is advisory.

One area, not specifically subject of the activity was highlighted during the visit to the Digital Forensics Unit, and commented on by others, is the delay in dealing with the forensic examination of devices and evidence obtained from them. At present the 2 year delay in processing evidence has a significant negative impact on the administration of justice in Albania and requires urgent attention. The current response is to increase the number of staff, train them and benefit from donor supplied equipment. While this is welcome, on its own, it will not solve the issue. There is a requirement to introduce clear management processes and have clear targets to reduce the backlog to acceptable levels.

Proposals

There follow details of the proposals, which are to be conducted by the Albanian authorities, albeit, they will likely need external support, most probably from the iProceeds project, to a greater or lesser extent:

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

- Engage all stakeholders and manage the information flow that comes from the reporting mechanism to create benefits for all stakeholders.
- Conduct a targeting proceeds from crime online desktop case exercise with all relevant players in order to identify the challenges of this type of investigation, also in relation to reporting, and assess the distribution of responsibilities and opportunities for future collaboration and possible training needs.
- Improve the co-operation of the government agencies involved in cybercrime and financial investigations, with the ISP industry and the CERT. 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. Such cooperation may also assist in the development of an online preventative resource to share information with citizens that may allow them to adopt prevention measures.
- Further the role 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. The current CERT plays only a limited role (only government constituency) so a national CSIRT is advisory.
- Consider joint awareness action with banks and possibly ISPs.
- Consider training needs of prosecutors in the area of cybercrime and advanced financial crimes/money laundering.
- Consider the introduction of specific management processes to reduce the 2 year backlog of examinations in the Digital Forensics Unit. These should include but not be limited to: case acceptance policies, prioritisation, risk assessment, triage and an effective case management system.