iPROCEEDS

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

Version 24 April 2017

Report

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

20 - 21 February 2017, Skopje
"The former Yugoslav Republic of Macedonia"

Provided under the iPROCEEDS project

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 Cybecrime@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 was carried out under the iPROCEEDS project Work plan, activity 1.3.7, as a scoping mission aimed to gather specific information regarding online fraud and other types of cybercrime reporting in "the former Yugoslav Republic of Macedonia". 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 and have an interactive discussion.

Participants

The scope of this mission was to visit investigation and police authorities, Prosecutor's Office, Financial Intelligence Office (FIU), the telecommunications regulator and industry players (Internet Service Providers and the Banking Association) – as well as any other player suggested by the host country – to get an overall view of cybercrime reporting. The mission aimed to get the perspective of different players and to recommend best practices based on the findings.

The meetings included representatives from the following institutions:

- The Ministry of Interior
- The Public Prosecutor's Office, Organised Crime and Corruption
- The Agency for Electronic Communications (Telecommunications Authority, AEK) which hosts the national Computer Emergency Response Team (CERT), MKD-CIRT
- The Ombudsperson
- The Financial Intelligence Office (FIU)
- The Banking Association.

The workshop at the end of the mission was used to discuss international best practises and the preliminary findings of the experts and involved representatives from the Cybercrime and Digital Forensics Unit, Ministry of Interior.

Summary and Findings

DAY 1: 20 February 2017

1. **Meeting with a local police station and with the Cybercrime and Digital Forensics Sector of the Ministry of Interior**

The purpose of this meeting was to analyse the existing crime reporting mechanism within the Ministry of Interior. The information in this report was provided by the experts from the Ministry of Interior, the Cybercrime and Digital Forensics Sector. In "the former Yugoslav Republic of Macedonia" criminal complaints are reported to all regional Police Offices in several ways:

At the police station: it is customary to file a written complaint. Both a physical (natural) person and a representative of a legal entity can report as the victim of the crime.

It is also possible to file a complaint to the Cybercrime and Digital Forensics Sector by email. In this case there is no particular form to be filled out and citizens are free to describe the facts in their own logic. The email communication is directed to the Cybercrime and Digital Forensics Unit and is sent in plain text. If the complaint does not constitute a crime within the competence of the Cybercrime and Digital Forensics Unit it is sent to the competent Regional Office. The email at which complaints are received is cybercrime@moi.gov.mk. Research shows that the address does not appear, or is not easy to find on the Ministry of Interior's website. Reportedly, it is often mentioned by the press, however.

Information submitted to the Cybercrime and Digital Forensics Sector by way of email or website (form) is not considered as evidence and can thus not be used in court. The information is merely used for intelligence purposes and serves to form a picture of the situation in the country.

Although most cybercrimes are reported in Skopje, it is possible that crimes are reported at regional stations in the country as well. They will usually report this information to the Cybercrime and Digital Forensics Sector and use their expertise in cases involving cybercrime and/or electronic evidence.

Regional Offices are called Bureau for Public Security (SVR). These are active in eight cities. The SVR Skopje has specialised units for economic and computer crime, and computer crime and electronic evidence (IT forensics).

There is no procedure that dictates that reports are to be always sent to the central Cybercrime and Digital Forensics Sector. It may happen that simple cybercrime cases are not reported to the central level. Although, "the former Yugoslav Republic of Macedonia" is a small country, it is more of an exception when this does not happen.

There is an effort underway on behalf of the Cybercrime and Digital Forensics Sector to create an online reporting system where reports of cybercrime are captured through a Webpage. The system will use a dynamic web form and will allow citizens to report various types of cybercrime. The aim is to differentiate complaints along lines of the categories.

This project, entitled MC3, after the IC3 Internet Criminal Complaints Center of the US, has not yet been finalised. The initiative was partially financed through external support. The financial contribution was used to commission a private company to create a web interface for the reporting system. Although the interface is operational, the programming logic behind it needs more work – and the current budget does not allow for its completion in 2017.

A feature of the system will be that complaints of a certain nature, or that meet certain criteria, can be flagged as high priority cases. An example could be child abuse. In those cases the report will be flagged as high priority (the system has four categories) and a SMS will be sent to an operator (currently the Head of the Cybercrime and Digital Forensics Unit) who will review such complaints immediately.

It will be based on a wizard. The users will be required to tick the box which they consider fits best their scenario. Categories for reporting will be based on the ACORN system from Australia. The administration of the system will require one or two persons responsible for handling the information. It is considered that the reports will be shared with the CERT – if there is an online report about a possible government attack - and with banks – if the reported information is related to bank security or to a particular bank account, for example.

Since the system is not operational at the moment, the Ministry of Interior is in process of seeking additional funding for its further development. There is no estimate available about the cost of finalising the system. Once operational, this system will be run under the auspices of the Ministry of Interior and will be administered by the Cybercrime and Digital Forensics Sector.

The company which developed the web interface have provided the code to the Ministry of Interior, which is the owner of the code. They consider that private experts should further develop the software for the reporting infrastructure.

The system will also be used to collect data about the current threats and will be used for awareness. Complaints will be analysed and advice for users will be based on the threat landscape in "the former Yugoslav Republic of Macedonia". Advice can be given to end users and businesses alike. Europol and INTERPOL monthly reports which are received by the national law enforcement authorities will also be analysed and will be developed into user advisories.

The public reporting system is supposed to receive reports by mail and through a web portal. Everybody can report in the new system, it will be in Macedonian and English languages. There is institutional support for the creation of the system. The Ministry of Interior provides a server, domain and subdomain - all these are actions which aim to support the further development of the public reporting system.

Once information is received from citizens, using one of the above channels, it is examined by an inspector and distributed to the unit which has competence to investigate the case. If it is concluded that the complaint is not a criminal offence no investigation is initiated and the information constitutes only intelligence. All complaints are investigated.

When there is sufficient information that a crime is committed an official report is prepared, which is sent to the Public Prosecution. Only some complaints go to the prosecution as a criminal complaint. According to the Criminal Procedure Code, "the former Yugoslav Republic of Macedonia" has a prosecutor led investigation phase. The Public Prosecutor is involved in the criminal investigation at its early stages.

The role of the police inspector is to gather evidence to support the case.

The Department for Criminal Intelligence Analysis of the Ministry of Interior collates and analyses the statistics on at a central level and publishes them officially. The current methodology for statistic gathering does not provide sufficient data for threat analysis reports or intelligence based policing by the Cybercrime and Digital Forensics Sector, according to the latter.

In order to generate management information and intelligence, there is a Ministry of Interior database of daily activities where all cases are registered – in 95% of the cases SVRs inform the central authorities and usually they join the investigations if the case is under their competence. It is proving difficult to make a clear distinction between pure cybercrime and crime committed with the use of technology. Both are dealt with at regional and central levels, the division is often based more on skillsets.

The central authorities cooperate with the US IC3 to determine how many citizens reported fraud to the US authorities. They use this information as intelligence to initiate an investigation in "the former Yugoslav Republic of Macedonia".

Cooperation with multinational service providers is organised through the central authorities. This process helps them develop direct relations with the multinational companies on the one hand, but also helps them to know the whole picture of cybercrimes happening on the territory of "the former Yugoslav Republic of Macedonia" or from IPs from their territory, on the other.

Several different Reporting Processes and Databases are also in operation in relation to specific subject matters*:*

- There is a National Regional File "Diana "– led by the central authorities where, on a mandatory basis, all law enforcement officers working on a child pornography cases should submit information about the case. The information is a short synopsis of the criminal case. This provides an opportunity for the central authorities to know the whole picture of cyber cases against children on the territory of "the former Yugoslav Republic of Macedonia".

- E-Commerce cases are considered for a similar national file – but this has not yet been established.

- The Safe Net Hotline in "the former Yugoslav Republic of Macedonia" reports everything that happens on the Internet to the central authorities. Some of the information reported by the hotline to the central authorities is used only as intelligence, as it does not constitute a crime.

- The "Red Button" System is a national reporting system which is available under a web portal and a telephone line. When a citizen uses this system the information goes directly to a duty officer who directs the information to the relevant unit.

Although there is an online public reporting system process initiated by the Cybercrime and Forensics Unit Sector, development is frozen because the (public) funding required.

2. Meeting with the IT Forensic Experts from the Cybercrime and Digital Forensics Sector

The digital forensic experts are part of the Cybercrime and Digital Forensics Sector and focus on forensic investigations. The Unit is staffed with nine persons and has two subdivisions/specialisations: computer forensics and mobile forensics.

Data related to digital equipment seized at the crime scene is examined at this unit. Every inspector from the field, together with an order from the public prosecutor or from judge, can bring a digital device. The order contains information about who is the owner of the equipment, what is the evidence associated with it, what needs to be found, passwords, encrypted data.

The reports of the digital forensics experts are brought to court and are accepted as evidence.

The unit also deals with requests for content and/or traffic data. Such orders are sent from the public prosecutor to the service provider and all the data is seized - both content and traffic data by the unit's experts.

When information is requested from a bank the administrator provides the logs to law enforcement – packed and hashed. The hash is kept by the bank and by law enforcement.

To facilitate cybercrime investigations, additional training is needed for First Responders with a focus on how to seize equipment at the crime scene. Currently not all police officers are aware of the nature and requirements of digital evidence. Live data forensics capability is limited and is at the very beginning of being developed. Difficulties that present themselves in Live forensics are the fact that everything must be documented and explained. Also, additional training is needed on crypto currency investigations, as there is not sufficient experience in this field.

3. Meeting with the Public Prosecutor's Office for Organised Crime and Corruption"

"The former Yugoslav Republic of Macedonia" has a prosecutor led investigation. The prosecution service has several prosecutors that have knowledge about cybercrime, but this is not their primary specialisation or field of work.

Although the prosecutor is formally in the lead in the Macedonian prosecution system, there are several impediments for the prosecution to co-operate extensively with the Ministry of Interior and/or other entities, when it comes to cybercrime reporting. The main issue is that the prosecutor is held to a relatively strict role, as soon as a formal complaint is lodged. This limits his room to manoeuvre, especially in relation to cases that are reported as intelligence.

According to the Criminal Procedure Code the prosecutor is held to investigate any matter brought to his attention, and is prohibited from sharing details of the on-going investigation with private entities. In practise, therefore, the initiative for the type of operational contacts required for effective cybercrime reporting and investigation, lies with the Ministry of Interior. This is not perceived as a disadvantage by the prosecutor, but rather as an area where a clear choice needs to be made by the Ministry of Interior as the primary party to engage with the industry and the public.

The Criminal Code provides that the Ministry Interior has authority for pre-investigative actions. The Law on Internal Affairs and Police also mandates this.

Overall it is therefore easier for the Ministry of Interior to make a distinction between reports on suspicions (intelligence) and reports that hold grounds for prosecution. This distinction is not formal but is largely for pragmatic reasons: procedures before the prosecutor are confidential. This is not to conceal the process from the public eye, but to protect the rights (and privacy) of potential suspects. It would be preferable for the Ministry to run a reporting system. The role of the prosecutor cannot be significant there.

As all investigations are prosecutor-lead, when the prosecutor requires, all stakeholders are obliged to act on his order. This limits possibilities for voluntary public-private cooperation and makes that the prosecutor is more equipped to deal with the advanced stages of the criminal procedure and with evidence gathering rather than reporting and intelligence gathering. Considering that the Ministry of Interior's Cybercrime and Digital Forensics Sector has more operational and investigative experience, it is also easier to take care of requests for them, since they have all the relevant contacts and are able to operate in a less formal (pre-investigative) role.

Coordination of investigations is a daily task for the prosecution. Prosecutors (especially for organised crime and corruption) are coordinating daily with the relevant Ministry of Interior units. There is no formal structure for this interagency cooperation, but the law requires that both the Ministry and Prosecution ask action from each other.

Another area that relates to cybercrime and reporting is related to consultation, especially for events or incidents that are more of general nature. Communication about general incidents or areas of cybercrime is often informal - the same goes for communications with NGOs. Prosecutors often try to have informal meetings on relevant topics – and this is perceived as very effective as it builds mutual trust.

Cooperation in matters of security breaches, such as incidents reported at the CERT, typically bypass the prosecutor initially, and come to him via police channels (the Ministry of Interior).

The prosecution is currently lacking an appropriate case management system - coordination of cases is mostly informal. The Ministry of Justice is working on a case management system that will be used for data transfer between various authorities to make delivery of case data more efficient in future. The system will be run by the Ministry of Justice and will benefit the Ministry of Interior and the public prosecutor, the Ministry of Finance (the FIU) and the Tax and Customs Administration.

Awareness raising about cyber threats for end users, businesses and public institutions is considered to be a primary task for the Ministry of Interior. The prosecution would consider to support them with such initiatives when necessary, but do not recognise this as a primary function.

Separate statistics on cybercrime are kept at the Ministry of Interior and the public prosecution. Based on the current statistical methodology used it is difficult to compare the statistics collected by the different entities. This is because statistics are collected only for institutional use and not with threat assessment purposes and discovery of trends in mind. There are often differences in statistics since the method of collection influences the data. In order to produce analytical statistics the methodology of data collection should change.

An issue remains that once a prosecutor engages in the procedure it is an official criminal case. The information provided to a reporting platform by the citizen cannot serve as evidence and does not always constitute a crime. It is more an initial informative step that a citizen has suffered a loss or experienced negative experience online. The prosecutor does not need or want to engage in direct assessment of citizen's complaints, but has to base his decision of whether an act represents all elements of a criminal offence based on evidence.

The prosecutor can also act *ex officio* and prosecute a case without a formal complaint. A case involving banks has many aspects that are in play - the prosecutor can sometimes work on prevention as well. Overall the prosecutions role is limited in awareness raising.

Apart from the main task of prosecution of cases, where they are in the lead, the prosecution in "the former Yugoslav Republic of Macedonia" does not envisage a leading role in a (potential) reporting system and associated cooperation platform. They mainly refer to the Ministry of Interior for awareness, online reporting and pre-investigative intelligence gathering and only see a supportive role, for instance in maintaining contacts with independent NGOs.

There is, nonetheless, a need for training and education of prosecutors on topics such as virtual currencies and search, seizure, freezing and confiscation of proceeds of crime. This will benefit the effective search and seizure of criminal proceeds, especially in cybercrime cases. Only few prosecutors are currently capable in this area, and this is largely due to self-learning and interest, rather than formal training or formal specialisation.

4. Meeting with the CERT (MKD-CIRT hosted by AEK, the Electronic Communications Regulator)

MKD-CIRT was recently established as a national CERT and is hosted by AEK, the Electronic Communications regulator. It is set up as a separate department in AEK.

The team is now active and partly operational. Operations were started up in May 2016. The team is made up of three members. Currently there is no possibility to hire new team members, but the MKD-CIRT is waiting for two new hires. One analysis and one communications specialist are still required.

According to the government approved work program the MKD-CIRT should work with 17 institutions, mostly government agencies and ministries. The National Bank and Telekom MK are also members and links have been established with all of them using membership forms that outline the key contacts in each of the institutions. They have established contacts and assessed the public facing IP address and domains of each of the members and have exchanged PGP keys in order to facilitate co-operation.

The MKD-CIRT website has been published and it offers the possibility to report security related incidents.

Incident reporting and classification are currently the main operational task that is done by the CERT team. They also focus on information exchange. For this the Traffic Light Protocol (TLP) is used, there are some issues in matching official classifications (used state wide and in the host agency) to TLP classifications. The highest level of confidentiality in "the former Yugoslav Republic of Macedonia" is named "confidential" in official terms and it is unclear how this maps to TLP precisely.

Incident reporting can be done in several ways. It is foreseen that the main way is by PGP encrypted email. Another way is through anonymous report submission through the MKD-CIRT website. All reports are sent by email to the MKD-CIRT's ticketing system (the Request Tracker for Incident Response or RTIR, which is almost an industry standard, is used).

All incidents and activities are to be coordinated by MKD-CIRT. They are currently working on more information sharing and threat intelligence. The process of gathering threat intelligence mainly relies on Indicators of Compromise, received from several sources. They use open-source threat intelligence feeds and also have Memoranda of Understanding with Team Cymru and the national CERTs of Italy, The Netherlands and Poland. The information received is filtered and scanned for "the former Yugoslav Republic of Macedonia" IP addresses on the basis of AS number. They hope to expand their threat intelligence service both in scope and coverage. To this end they are cooperating with the Bulgarian CERT and are working on threat-intel with counterpart CERTs in Albania and Kosovo*.[1]

There is a procedure for incident reporting in the MKD-CIRT. It includes informing law enforcement, if the MKD-CIRT believes this is needed. They use the RTIR system for this and, in those cases, give law enforcement access to the incident details through the system. The system can also allow for the details of the case to be anonymised. The legal department in AEK decides if – and what information can and should be shared.

Reporting of incidents and related criminal acts can also be simultaneous. For these cases there is communication on the working level, also to find out if any mutual assistance or sharing of expertise is required.

As regards cooperation, there is a clear divide between the security issues and the criminal matter, in practise, according to both the MKD-CIRT and the Ministry of Interior. The relationship with LEA

[1] All references to Kosovo, whether the territory, institutions or population, in this text shall be understood in full compliance with United Nation's Security Council Resolution 1244 and without prejudice to the status of Kosovo.

could benefit from a Memorandum of Understanding however.

The CERT also works with the Chamber of Commerce, Banking Associations (it was brought to attention that there is more than one banking association) and the ten commercial banks.

The banks that were contacted, are also interested in joining the MKD-CIRT's constituency and are open in exchanging information. They want to use a similar platform between themselves. They are interested in a system to exchange more specific threat intelligence and incidents, but also in sharing fraud cases. The CERT team is currently working to gain the banks' trust. The banking regulator has approved cooperation between the MKD-CIRT and the local banks.

Besides banks, other groups are being considered for the MKD-CIRT's constituency - the telecoms, power/energy and transport sectors will be the primary targets. Information and threat intelligence sharing will be set up per constituency.

The MKD-CIRT team is working on achieving FIRST membership and is a listed team on Trusted Introducer (TI) – and working towards becoming accredited. In order for the FIRST membership to be approved they have to put out a number of tenders to upgrade several facilities to the required level. They contacted ITU for support but were notified that the ITU IMPACT program (that provided assistance in cybersecurity matters) was ended and future activities would be coordinated by the ITU head offices directly.

From a formal point of view the MKD-CIRT has only a limited role to play in the protection of critical infrastructure (CIIP), this policy area is in development however. Currently there is only a Standard Operating Procedure for the case of attacks on CIIP. The approach would involve multiple agencies such as the Ministry of Defence and the National Security Agency.

There have been some workshops with the constituents, but they are *ad hoc* and based on a singular topic, rather than a rolling agenda. The AEK has the obligation to have two public meetings in a year for the MKD-CIRT activity. This cooperation model could be improved with more workshops for a wider range of constituents.

DAY 2: 21 February 2017

5. Meeting with the Ombudsperson

The Ombudsperson of "the former Yugoslav Republic of Macedonia" is appointed by the Parliament and acts as an independent institution. The Ombudsperson has a constitutional role (since 1991) in protecting the rights of citizens. It functions as a Parliamentary body, and works according to the same model as used in Sweden. Protection of children has recently been given special provisions in the law. The Department for Children and Persons with Special Needs deals with children's rights.

The Ombudsperson is a member of international and regional organisations such as the South East Europe Children's Rights Ombudsperson's Network. They hold meetings and discuss children's rights and Internet violence was reviewed a few years ago.

As regards online crime the institution has limited experience with online reporting. There has been only a small number of Internet related complaints in the country. The main complaints come from parents and are related to publication of photos of children online. The rules regarding age limits are not always observed by social networks. In practice children of very young age have a Facebook profile.

Many children approach the Ombudsperson in person. For children requesting help, the

Ombudsperson also takes complaints via the website, email and phone. Complaints and requests on the website are anonymous. Few complaints were received regarding children online, some reports refer to online bullying.

Violence is often reported by children via Internet, but mostly through personal contact in schools or via NGOs when parents and teachers are not present. It was reported that children do not want to address issues as "I" but talk about "friends", when they have questions or complaints about abuse.

There is SOS helpline maintained by the Children's Embassy, an international NGO for reporting violence and abuse of children's rights. Children and citizens can report there. Some other NGOs have also hotlines in the area of domestic violence too. The Ombudsperson has been seeking funds for a special hotline for children to report violence. There is a general complaints line. However, a special hotline for children is needed.

Most staff at the Ombudsperson's Office are trained lawyers, the Children's Department also has social workers pedagogues and psychiatrists. In some cases they are also requesting the opinion of other institutions, as is allowed by law.

The main issue related to children is violence, especially amongst peers (in school, mainly). In the last two years, together with the Ministry of Interior there have been activities to raise awareness and point out the sanctions against such violence. Recommendations were issued to schools in order for staff to recognise the signs of abuse and (emotional and physical) violence. Also, to increase awareness, in 2016 a brochure on children rights and violence, harassment and emotional abuse was created. It is being printed and is written in a language suitable for children. In cooperation with UNICEF the Ombudsman has also prepared a translation of the Convention on the Protection of Children, also suitable for children.

At the same time, the Ombudsperson acknowledged that awareness is needed for parents and children in the area of Internet.

More awareness is needed and the general preventive functions of the Ombudsperson seem to be somewhat underdeveloped. A children-specific hotline, and more child-specific content would be a good start to raise parents and children's stance against online threats.

Violence is criminalised and as prescribed in the Criminal Code. The Law on Family Values, points to bodies that are responsible to deal with these issues. A national body was foreseen, with representatives from various institutions, but is not yet functional. Due to its monitoring role, the Ombudsperson is not a party to this body.

As regards children families and institutions usually accept the Ombudsperson's recommendations. In 90% of cases the issues are resolved. In other areas this number is much less. All aspects of children's rights are covered: street kids, kids residing in institutions, in daily centers, foster care families etc. If needed, complaints are sent to competent state organs. Although the Ombudsperson can indicate and inform, the institution cannot implement sanctions or measures. They monitor authorities' performance also in the area of children's rights. They verify that cases are dealt with effectively by authorities. The law also gives them opportunity to act on their own initiative. The Ombudsman is often opening cases of their own initiative for children housed in state institutions.

Statistics are available in the annual report, published on the website of the institution. In total they resolve about 2000 citizens' complaints at the Ombudsperson Office in Skopje on average, each year. For the entire country, the number of complaints is not provided, but it must be much higher since there are six branches each headed by a deputy Ombudsperson. They all have own staff, and are in permanent contact with the Skopje office. All applications are treated in Skopje, regional units can receive requests and can meet the citizens involved. Annually 150 complaints are received, related to children.

6. Meeting with the Financial Intelligence Office

The FIU in "the former Yugoslav Republic of Macedonia" is administrative. It cooperates with the Ministry of Interior on cybercrime cases. This cooperation is perceived to be good and of a high level. As an administrative FIU, the unit acts on request of several institutions. They act proactively when it comes to computer fraud. The main type of fraud they see at the moment is Business Email Compromise (BEC) or CEO-fraud.

The FIU has an analytics unit. Using financial investigations and the available data they analyse a person's financial status and then provide the requesting agency or institution, including the Ministry of Interior, with relevant intelligence, explanations and possible suspicions. The intelligence received from the FIU is not used as evidence. In order for it to be admissible in court, the prosecutor needs to request the same information again using his investigative mandate.

Lately cybercrime is a trend. Mostly the FIU comes across cybercrime cases through requests from the Ministry of Interior. There have been cybercrime cases that were detected by the FIU, in first instance, but this is more of an exception. In cases of suspected online fraud, they call the associated banks and tell them to monitor the account involved.

The FIU cooperates internationally on a daily basis. As a member of the Egmont Group, the FIU is in a position to call on foreign counterparts and send a request for suspending suspicious transactions.

There have been successful cases so far, the prosecution is working on several cases where they were returning funds to owners. A main issue of such cases is that banks should react instantly and call a correspondent bank to suspend transactions – especially if a suspicion arises that a transaction is the result of computer fraud or cybercrime.

The FIU has been asked to suspend cybercrime related transactions by foreign counterparts as well.

The Ministry of Interior and banks both send cases to the FIU for further analysis - and in certain cases they contact each other directly. The FIU will then start a case. Usually, the first step is to work on suspending the transactions and identifying any funds and proceeds that belong to the suspect or case. In practise it often happens that the institutions act immediately and do not wait on the official request (or STR) to come in – transactions are postponed and information is shared spontaneously.

The FIU indicates that some obligors' reports are not of an adequate level and these reporting entities would benefit from more training in computer fraud cases, in order to both report and detect these cases more efficiently. The main challenge in these cases is to stop transactions before the money has left the jurisdiction, or was disbursed from a neighbouring one.

The challenge is to stop such transactions in good time and be able to retrieve the funds. Although, as Egmont Group member they can ask for this relatively efficiently, requests still may take a while. Therefore, not in all cases can they suspend transactions successfully. Sometimes an account is only used for committing a crime and as soon as the money is on the account it is withdrawn or disbursed elsewhere. Even though cooperation with other countries is at a high level, success depends on speed. Although success is not achieved in all cases, other countries have provided feedback and have provided the requested information or acted on a request for freezing.

The FIU can suspend a transaction for 72 hours. The prosecutor then has time to establish cause for further actions such as executing a freezing order. In practise it is the policy of the receiving bank and the working hours of that bank, that are affecting the outcome a lot. Time differences are often used to the criminals advantage and transactions are usually requested (and cleared) near the end of working hours or just before bank holidays. This is in fact, almost an indicator of fraudulent intent.

The law requires that banks implement anti-money laundering detection, and every bank has special software for this purpose. According to several typologies and indicators (many of which were published by the FIU) banks analyse client transactions. Once a year the FIU reviews the effectiveness of these indicators.

STRs are reported in XML format via the FIU website. They use a system called AskMK. The XML format for the reporting is prescribed by law. XML reporting formats are available for STR, CTRs and loan/credit application reports where there is a suspicion regarding a transaction. There are numerous cases where a bank called immediately, in cases of fraud, even before the actual STR was submitted. The FIU will then provide a report to the prosecutor and notify the Ministry of Interior and begin the investigation. Often, intermediary banks report frauds, as well. In a clear-cut case they will then suspend the transaction – but this is not always the case. Banks are generally reluctant to stop any, but the clearest of fraudulent transactions.

Although time is of the essence, AskMK users were recently asked to put more manual labour (analysis) into STR reporting rather than merely passing on the STR. This was done to achieve better and more usable reports. It is not immediately obvious that a fully automated reporting system would give better results and they had reverted from that – requiring banks to now input manually generated STRs only. The FIU receive 170 STRs yearly from 14 banks. Overall, 90% of the total STR volume originates at banks.

The statistics also indicate that other obligors are (most likely) underreporting. Training of these obligors needs to be initiated, also, and perhaps especially, for them to understand cybercrime. The statistics for 2015 are on the FIU website, contained in the annual report. The annual report is also available in the English language.

Cooperation with banks is *ad hoc* – for example when a new typology emerged (through STRs) the FIU notifies all banks. When new trends emerge, the FIU contacts all banks to explain the situation. In some cases, indicators and typologies are shared, so banks can recognize a pattern, for example money from a certain country (or combination of countries), a suspect person’s name, age and country taken together.

There is also a regular AML meeting where recent typologies are discussed and banks are stating issues where their cooperation is concerned. The forum for this meeting is the AML Committee of the Banking Association. Regular meetings are also held.

The FIU is performing it is typical reporting and intelligence functions well, but needs more skills and understanding in relation to cybercrime and related frauds, in order to be effective in this demanding area. The FIU indicates it would like to hear more from other counterparts on these topics and would welcome to hear how they handle suspicious transactions. Recently training needs have been identified.

7. Meeting with the Association of Banks

The Association of Banks has all banks as their member, as well as other financial sector companies. When it comes to cybercrime and online financial fraud the most relevant committees in the Association are the Information Security and the Anti-Fraud Committee. The AML and Compliance Committee also has good cooperation with the FIU and Central Bank. They have a memorandum on sharing information, which is limited to sharing the typologies of any attacks and not personal details.

Online money laundering and electronic banking are increasingly important for the banking sector in "the former Yugoslav Republic of Macedonia". Commercial banks are affected by cybercrime, a common fraud, for example, is the CEO, or BEC fraud. In many of these cases banks receive emails for money orders, in order to transfer to a foreign (often Polish) bank. After the transaction, the receiving account is often closed out in hours. All the same, clients are often adamant to go ahead and authorise the fraudulent transaction, since the fraudsters are very effective in persuading their targets through social engineering. The total of fraudulent transactions prevented is 100.000 EUR in one bank.

More and more cases like this are reported. Banks report these cases to the Ministry of Interior. They also exchange such data amongst themselves. Currently they exchange the typologies and trends in the banking sector internally. More work is clearly needed to prevent such cases and help to better prevent cases for the future. As a first step Know your customer (KYC) requirements could be amended.

Banks are aware of the risks posed by the personal data processing and money laundering aspects of their retail banking services (especially current accounts and credit cards are prone to fraud). They also use the special fraud departments in Visa and Mastercard and have limits on certain types of transactions and country based limits on transactions in place. Information and anti-fraud practises are shared within the Banking Association.

A major issue is that analysis of transactions and STRs takes a lot of time. One bank is currently holding 300.000 EUR due to several freezing orders.

Since 2009 there is a special regulation on information security. Under this policy banks have to report cyber-attacks. Macedonian banks seem vulnerable, especially in relation to their retail operations and current accounts. Up to eight banks have predominantly foreign capital, meaning they often adopt policies, and use technology acquired at group level.

Since 2016 the Central Bank created a cybercrime risk assessment tool, which can be used to self-assess cyber risk. All banks have taken the self-test and sent the results to the Central Bank.

All banks have action plans on information security and coordinators keep track of their implementation. The regulator requires that a basic level of protection should be reached by now. A "medium level" needs to be achieved by 2019. Implementing such measures comes at a significant cost to banks; it is estimated to cost an average of 500.000 EUR per bank.

The cost issue is mostly related to AML systems, which are already used to do scoring. By 2019 the systems will be expanded and have an online fraud detection system, which will also be connected to credit card issuers and to their own audit system in order to audit bank internal data for anomalies. This correlation technology to detect patterns using artificial intelligence is not widely deployed, so it is hard for banks to acquire suitable solutions. The policy that mandates these measures is transposed from a US banking policy.

The Information Security Committee is in the process of signing a Memorandum of Understanding with the CERT. They established a link with the AEK, the telecommunications regulator, regarding information security. They already exchange information with the CERT and are currently working on incident management as foreseen at the CERT.

ISO 27001 has been required since 2005 and penetration tests are also mandatory. In practice both black and grey box testing are used and two to three yearly penetration tests. Especially new products are tested on implementation. The exposure is measured by the cybercrime measurement tool of the Central Bank. Branches and eBanking operations are the biggest risk factors according to that model.

The developments in "the former Yugoslav Republic of Macedonia" are in line with the EU NIS Directive. More central reporting is mandated there too. Banks are mainly looking to free or cheap tools, and are currently looking to implement better information exchange. Typology and threat intelligence will be exchanged, where the focus is first on threat intelligence. For board level executives more data is needed to assess the risks as to be able to tackle the issues more comprehensively. A major risk is also the reputational risk. For the same reason banks are very careful in sharing information. Clients' reputation needs to be protected also.

At the same time, attacks on information systems in the bank are registered at the Central Bank and major issues are always reported. Any issue that leads to an outage of the core banking system of more than one hour is to be reported. The new system requires medium to high risk incidents to be reported.

Major types of frauds detected are postal terminal and credit card related frauds. Many Bulgarian skimmers are active in this area. Banks get occasional spikes of these cases and then put additional controls in place.

Other fraud is related to POS terminals. Bank clients in "the former Yugoslav Republic of Macedonia" use credit cards extensively, also contactless. Email interception, also internationally – as in committed from abroad – is also on the rise, leading to CEO fraud to spike. Due to the increase of (mobile) Internet usages eBanking is also on the rise. Last year there was 50% increase of t

The usage of eBanking. Both mobile and regular online banking are used. All banks have OTP verification in place. Also a SMS warning system can be employed. Two factor verification is mandated by the Central Bank. Clients are to change password on three monthly basis. The system is not currently subject to much cybercrime or abuse.

Customer complaints are often lodged at the bank. The investigation is then started inside the bank. The banks advice the costumers to also file the case at the police.

The Data Protection Act obliges banks to keep only 30 days the video logs. There can be issues with data no longer being available that way – since the billing cycle for many products is longer and customers may not notice a fraudulent transaction before then. Biometrics is not very well regulated, and therefore difficult to use in banking at the moment due to permission required from DPA.

The banking sector does not act very proactively when it comes to fraud risks related to customers. Awareness raising is not very developed on the banking side, in line with the limited efforts at the institutional level. This could perhaps be a good area for the MKD-CIRT team to start cooperating on, with the sector, as cooperation with the CERT is developing well, and security has a high priority in the sector (both on the side of banks as at the regulators). Cooperation on improving end-user security awareness seems like a logical next step.

Conclusions and Proposals

Conclusions

The mission identified a good status quo and encouraging developments in the area of reporting cybercrime. The Ministry of Interior's specialised Cybercrime and Digital Forensics Sector is working on setting up an online reporting system (MC3). It is held up due to funding issues. The system looks promising and the front-end is well developed (part is copied from the ACORN system). The backend logic (database, analysis, statistics and reporting of priority cases, etc.) is not finished yet, however, and this is a significant step in the development of any reporting system.

The newly established CERT handles security related reports online.

Informal cooperation is working well, but may lead to issues when cybercrime reporting is scaled up. The current systems seems to be based on informal contacts and direct communication, but if and when smaller crimes are reported, this type of cooperation needs to be replaced with more automation and reporting as a complaint-by-complaint system will no longer by adequate.

The meetings demonstrated a commitment of the country to engage in the project. However some key players were missing at the workshop and a lack of ISP presence was a noticeable issue.

Overall the situation as regards reporting is showing good progress. The Cybercrime and Digital Forensics Sector are professional and have a good understanding of the issues at hand. At the same time, statistical analysis and intelligence functions seem somewhat underdeveloped when it comes to cybercrime. The responsible department does not seem to deliver statistics and intelligence in a usable format, forcing the Sector to take this up instead. This is not due to unwillingness or inefficient cooperation but is the result of the current reporting system methodology. Statistics are gathered for institutional purposes and thus do not provide sufficient intelligence for in depth threat analysis. The same goes for awareness – the new system will foresee in some awareness raising content, but so far limited efforts were done and the focus is universally on the Ministry of Interior. The banks could perhaps explore cooperation with the MKD-CIRT on this topic, too, for example, and the Ombudsperson and some NGOs could step up their efforts on online content in this area too. A cross-sector and coordinated approach would likely lead to the best result.

Reports generated by online reporting mechanisms are not directly admissible as evidence. This may be problematic if a case relies on online reports for a factual basis. The process for obtaining statements as evidence is still manual and time consuming, mass frauds will not be easy to detect and deal with in this fashion. But this will require a major change in the criminal procedure process.

The online reporting system under development at the Ministry of Interior is of crucial importance. It should be funded but no budget appears to exist for its completion in 2017. A needs assessment for further development of the website was discussed as a possible activity to be supported by the iPROCEEDS project. Given the limited budget available, progress on the system is good. The alerting function it implements (alerting case officers of cases that require immediate attention), is a best practice in the region and was not seen anywhere else.

The preventive activities are playing important role in public awareness when dealing with cybercrime. There are partial efforts on behalf of the Ministry of Interior to translate and adapt preventive content developed by Europol and other law enforcement agencies and publish it for public use. It would be advisable to further develop country's preventive capabilities by participating in pan European preventive initiatives or develop country specific ones. It would be advisable when developing the public reporting system to develop content and campaign which will explain to the public not only the benefits from such a reporting system, but also will make them aware how to protect themselves and not become victims of crime. Such initiatives could be developed with NGOs or private entities on a case by case basis.

Proposals

In this part of the report are included concrete proposals, which could be conducted by "the former Yugoslav Republic of Macedonia" authorities:

- Form an interagency working group to jointly brainstorm and develop the concept of the public reporting system. This will assist Ministry of Interior to better understand the needs of other agencies like the CERT, the FIU and the Public Prosecution and will foster interagency cooperation.
- Assess the needs (at all other agencies) that exist in terms of the reporting-system back end (where collection, collation, prioritisation and reporting takes place) before commissioning further work.
- The process of gathering statistics should be improved and become a priority in cybercrime prevention activities at the Ministry of Interior. The current statistics are used only for institutional purposes and not useful with relation to threats assessment. Thus, the methodology for statistics gathering should be improved and provide additional capabilities.
- Cooperate with NGOs – national and international in order to jointly develop preventive material and public awareness content and campaigns. This activity is recommended to be conducted during and after the establishment of the public reporting system. It will also serve as a mechanism to promote among citizens, businesses and public entities the newly developed reporting system.
- When the public reporting system is developed to consider analysis of the reporting cases and prepare threat assessment with the purpose to inform the public about the latest attacks and mechanism for protection. This activity will also serve the small and medium enterprises when developing their security strategies and will facilitate the investment in the right tools and initiatives.
- Strengthen institutional capacity. The institution within "the former Yugoslav Republic of Macedonia" that has most competence to combat cybercrime is the Ministry of Interior. Other institutions support them in the investigation of cybercrime cases but do not possess their own skills, in most cases. In order to further develop a strong approach against cybercrime it is needed to develop such cyber skills among the other institutions. This could be achieved by organising joint trainings, methodology development and participation in joint task forces on subject matters.
- Engage all stakeholders and manage the information flow that comes from the reporting mechanisms (CERT, Ministry of Interior) to create benefits for all stakeholders.
- Conduct a topical, proceeds of cybercrime oriented 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 and formalise the (mostly informal) co-operation of the government agencies involved in cybercrime and financial investigations, especially with the ISP industry and the

CERT. Awareness and reporting are shared interests and there is already good cooperation on information security between the banks and the CERT and fraud trends are shared proactively at the FIU. This could be the start of a more coordinated approach.

- Further strengthen the role of the CERT, not only should it play a crucial role in safeguarding critical infrastructure, it is a good place for co-operation between sectors and public bodies.
- Consider more joint awareness actions with banks and possibly ISPs.
- The role of the Ombudsperson is crucial when it comes to children and parents awareness of the risks online. Their role should be expanded without compromising their valuable work on violence against children. More attention for prevention and awareness is needed, in this area. The current efforts mainly focus on reporting.
- Consider training needs of the FIU and other actors in the area of cybercrime and advanced online financial crimes/money laundering.
- Automate STR reporting with banks or improve response times and success rates in freezing funds in cases of "man in the middle" or "CEO" fraud. It is crucial to detect such cases very early on.