iPROCEEDS

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

www.coe.int/cybercrime

Version 20 October2016

Report

Advisory mission to Serbia on online fraud and other cybercrime reporting mechanisms

7 and 8 September 2016, Belgrade, Serbia

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, 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 1.3.4, as a scoping mission aimed to gather specific information regarding cybercrime reporting in Serbia. 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 two days 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 scoping mission visited several investigation and police authorities, the CERT and communications regulator, banks - as well as any other players suggested by the host country, such as the ombudsman and a social care centre – to get an overall view of cybercrime reporting situation from the perspective of different players.

The following organisations were part of the mission and the workshop:

- The Cybercrime Unit at the Operational Centre of the Ministry of Interior
- The Financial Investigation Unit at the Ministry of Interior
- The Office of the Special Prosecutor for Cybercrime at the Republic Public Prosecutors Office
- The Administration for the Prevention of Money Laundering (APML)
- The IP crime Sector at the Operational Sector of the Ministry of Interior
- The Ministry of Interior CERT
- The IT Forensics support Unit of the Serbian Police
- The Communications regulator RATEL (to host the national CERT in due course)

- The Ombudsman Office
- The Social Care Centre of the city of Belgrade
- The Association of Serbian Banks
- The Serbian Domain Registry
- ISPs and Banks.

Visit Summary and Findings

DAY 1: Monday 7th September 2016

1. **Meeting at the Ministry of Interior Operational Centre with the Cybercrime Unit, the Financial Investigations Unit, the Ministry of Interior CSIRT and the IP Crimes Sector.**

Institutional setup

The Ministry of Interior has an operational centre that concentrates a number of central police units.

The Service for Combating Organised Crime hosts the Financial Investigations Unit, the Cybercrime Unit and Intellectual Property Rights (IPR) Unit, which attended the meeting in addition to the Computer Security and Incident Response Team (CSIRT) of the Ministry of Interior.

The Financial Investigation Unit has two departments: the financial investigation unit against organised crime (which is partner of the iProceeds project), and a planning and coordination department that deals with investigations and operations across Serbia. The Financial Investigation Unit was established in 2009, when the law on criminal assets was enacted. This unit sits within the police whereas the Administration for the prevention of money laundering (APML) is within Minister of Finance (FIU).

It is noted that in on-going Chapter 24 negotiations[1] there are a lot of obligations on financial investigation, a need is identified to strengthen training and to improve international cooperation. In relation to the latter, the Financial Investigation Unit is a member of the CARIN network and an Asset Recovery Office will be established soon.

The Financial Investigation Unit is looking for new ways to conduct investigations including in cyberspace. This project is timely as they have been dealing with tangible assets and IP, and this project is an opportunity to start work on tackling the issues surrounding virtual property.

The Cybercrime Unit is also relatively new and was established in 2007. There is a very high crime rate in this field, and cybercrime rates are still increasing. The staff of this unit is expected to tripled as part of the Chapter 24 negotiations. This unit has developed international police cooperation that is assessed as very good, in particular with the UK and the FBI office in Belgrade. Police officers are sent to the UK for some trainings, and some have got the MSc in Forensic Computing and Cybercrime Investigation of University College Dublin. The Unit is not only focused on forensics investigations, but for example: in the week of 12th September 2016, it will engage in campaign against sexual crimes against children.

The IPR Unit has been established in 2008 and is unique to Serbia. Protection of copyright and IP remains a relatively new issue and education is still very much needed. This is why the Unit is

[1] European Neighbourhood Policy and Enlargement Negotiations, Chapter 24 on Justice, freedom and security. Serbia has opened negotiations on Chapter 24 in July 2016.

involved in seminars, for instance it will contribute to a seminar on 9 and 10 September 2016 on electronic business operations, mainly for the private sector.

Reporting of online crimes

In Serbia reporting is largely organised around police reports. Information related to cybercrime typically comes from several sources: rumours from media, tabloids and the press, which are often acted upon by the prosecutor and then investigated by the police.

- In police stations, and at the Prosecutor's Office, citizens may report crime. In this case reports are made at the police station or the Public Prosecutor's Office. Police have a duty to take all reports made by individuals. Reports can be made anonymously by phone (192 is the hotline for generic crime reporting). The Cybercrime Unit is required to report information it has received to the Specialised Prosecutorial Office, which means that any information related to cybercrime must be directly reported to this prosecutorial office.
- All reports are recorded in so called minutes. Throughout Serbia there are first responders trained in cybercrime, who are well placed to receive reports on this issue. The Cybercrime Unit may provide support if first responders need this, or if specific expertise is needed.
- Two websites are operational where the public can report crime in general: both at the police and at the Public Prosecutor's website it is possible to report crimes. When a report is made there, the common practice is to ask people to provide a statement in person.
- Businesses can report crime in much the same way.
- In the case of child abuse material and hate speech the police cooperates with the NGO Net Patrola, a member of the INHOPE network, who has a hotline with online reporting for these crimes: reports can be made on the website in Serbian and English.
- Information also comes from the APML and other state and government bodies.

Awareness raising

The Ministry of Interior engages in awareness campaigns in case of new types of crime. The website of the Ministry will be improved, a new version is being developed. Currently it provides information on how to complain. Information on how to report can also be found on the website of the Ministry of Telecommunications.

The Ministry of Interior organise workshops with NGOs on how to report and participates in events and conferences on this subject. For example, it organised a workshop with 250 attendants on the topic of prevention of drug addiction and violence against children, including online abuse.

On financial fraud, there is a forum on prevention of abuse of credit cards and the Ministry of Interior is member of the information security group within the Chamber of Commerce of Belgrade. Ransomware, and man-in-the-middle frauds are on the increase and receive special attention.

Speaking opportunities to the media or in public have to be approved by the cabinet of the Ministry, but in praxis they never refuse – this is a good way to raise awareness.

Processing of reports

All police units have a duty to share their information regarding crimes with the Public Prosecutor. The prosecutor may open an investigation into the crime and may then order the police to conduct further investigations. The investigation is led by the prosecutor.

Within the police, cases are recorded electronically; all units have access to the record of the case.

Where cybercrime is concerned, in praxis, almost all information also reaches the Cybercrime Unit, because of their expertise – although there is no structured process of information sharing. The prosecutor usually orders them to conduct part of the investigation. 30 employees in the Cybercrime Unit deal with child abuse material and juvenile victims and offenders.

All information is fed to a central point, and entered in a database. This central system has a rudimentary intelligence function, so it can detect similar cases based on markers like a telephone number or a name. The police are unaware how the Public Prosecutors' Office deals with criminal complaints information.

The Cybercrime Unit can establish some priorities in handling cases. International cooperation is a priority, for instance. In case a report emanates from the Association of banks or financial institutions, the Unit reacts immediately. There is ongoing discussion with the Association of banks with a focus on IT. The Unit had an urgent case of a Trojan attack of an account, after a similar case in Croatia. The Association knew about it, the Unit convened all banks with people dealing with IT security, with prosecutor, and the Ministry of Interior CSIRT, to manage the case.

Statistics

There is a central office in the Ministry of Interior that produces statistics from all the crime reports. It is noted that the intelligence function is rudimentary, a broader intelligence function would be useful.

There are many issues surrounding statistics, however. For cybercrime it is noted that many statistics are not comparable. The police, for instance, count requests from the prosecutor, as well as complaints in the same case, as separate cases in their statistics.

Statistics on cybercrime are hard to retrieve from this system. They are considered incomplete. Ministry of Interior statistics on cybercrime are not as reliable as the Public Prosecutor's Office statistics: the Public Prosecutor will usually see every complaint or information, and hence has a better overview than the police. Statistics in the police can be kept at station level and the central level, and are not complete: the prosecutor also takes complaints and the police may never hear about these. And although the police report cases to the prosecutor, the reverse is not always true in the Serbian system – also the police sometimes count cases double when the prosecutor asks for assistance in the same case more than once.

Although the information from these statistics is used for awareness and prevention purposes, it's use is rather limited. The Ministry of Interior is building a new site and may improve this function there.

Administration of cases

Complaints information often leads to cases, despite the fact that the system currently has limited possibilities regarding intelligence and enhancing data that is gathered. An example was given of a case where a fraud was reported at various police stations and some reported to the Cybercrime Unit. All information was sent to the Public Prosecutor, who realised the similarities and built a case.

The Cybercrime Unit also often identifies cases, since they usually receive information on cybercrimes through direct cooperation and through the Public Prosecutor.

In the Ministry of Interior all cases are given a unique case number. Their case administration is independent form that of the Prosecutor's Office.

The Ministry of Justice also has a separate administration of cases, which includes the results from prosecution, but also inadmissible cases and other data. It is used for statistical purposes.

The Financial Investigation Unit has a similar working method. Their goal is to find assets related to the ML offence. Since 2009 a reverse burden of proof was introduced so the focus is primarily on finding the assets of a person, who then has to proof their legitimate origin – provided their assets outweigh their legitimate income. They have access to many databases for this purpose. Their work is conducted under the supervision of the prosecutor of the case, and they frequently cooperate with the Cybercrime Unit . Open source intelligence and social media profiles can be very useful in ascertaining information in these cases. Online and virtual property is becoming increasingly important. The CARIN group also stipulated this in recent meetings. Co-operation with cybercrime investigators is therefore crucial. It is useful they are in the same institution.

Reporting of a crime is mandatory in Serbia. Yet it is clear that this is not enforceable in praxis.

National Strategy

Serbia has adopted a Security Strategy and an Information Security Law. In accordance with the law, the Ministry of Telecommunications and Information Society has set up several working groups, and a number of bylaws are in the making. One of these concerns a national CERT that is being set up in the communications regulator, the Republic Agency for Electronic Communications (RATEL).

CSIRT of the Ministry of Interior

According to the law, security incidents should be reported. ISPs however, hardly report any – this is likely due to a lack of sanctions and enforcement capability.

The CSIRT of the Ministry of Interior (commonly named CERT by its representatives, it does appear to be officially affiliated with the CERT division of Carnegie Mellon University. We therefore prefer to use the generic acronym of CSIRT) is in charge of the IT system of the ministry. Until the new CERT is operational, the Ministry of Interior CERT acts as a de facto national CERT for Serbia, cooperating with FIRST and ENISA.

Work is on-going to designate the telecommunications sector and the financial sector as critical infrastructure, and CERT teams are expected to be set up for these sectors as well.

There is Law on protection of IT since January 2016, and per this law one of the duty of the CSIRT is to provide assistance to Cybercrime Unit.

When the CSIRT was set up, information was sent to ISPs, Association of banks and Chamber of Commerce. It had a meeting with leading providers and established communication process with some providers.

The CSIRT is the first in Serbia and considers it has an obligation to intervene for this reason and because they are authorised officers.

2. Meeting with the IT Forensics Support Unit of the Ministry of Interior

The Forensic Unit is a separate service in the Ministry of Interior, Criminal Police. The staff was certified as basic forensic investigator by OLAF, and have taken a two weekly course provided there. Many have extra certifications, depending on their roles.

The Unit usually provides a report in writing to the case team, and the prosecutor may then call them to act as witness in the case. Since they are a police service they do not act as expert witness, but rather as an expert to the police.

On child abuse material, they do not have access to databases of know material, and all material is reviewed manually. In such cases they provide a catalogue of files to the prosecution.

In many cases suspects avail themselves of the "hacking excuse": the unit is often tasked to find specific evidence to show the suspects intent, in these cases, to disprove this scenario.

As an example the unit investigated a classical 419 scam. A victim from Vojvodina, believed in the story of an advanced fee fraudster when shown a picture of a suitcase apparently full of money, but not noticing that all bank notes had the same number. For this case, addresses all over the world were identified.

The unit often works with the Cybercrime Unit. They find devices and make the forensic images. The electronic evidence unit usually writes the charges in child abuse cases. The unit also works with FBI. They have lists of specific files that were (illegally) downloaded and they also have tools to analyse Facebook profiles. In most cases they are sent the computers of victims, to analyse.

There was little work on the financial side of investigations, so far. This is more a part of the Economic Crime Unit. They do cooperate with the tax administration, and they analyse computers of companies involved in tax evasion.

For media analysis (hard drives) they use: FTK (Accessdata), Encase, Xways forensics.

For mobile device analysis they use: Cellebrite (UFED touch 2), XRY (MSAB), The Oxygen suite.

They report issues with ordering tools. Their needs are often misunderstood. For example: they have been waiting for a MacBook, for a very long time, in order to be able to use certain tools for the Apple platform.

For analysis they use i2, this is mainly for understanding telecommunications data.

On an annual basis they analyse about 600 phones, and several hundred PCs (200). The unit comprises 9 staff, with 7-8 people having an operational role. 4 to 5 of this staff do PC analysis. The rest works in other fields. The unit also provide support in traffic data analysis – a task that also takes up a lot of time.

They have no experience in working with virtual currencies, and no operational procedures exist for these. Only 10% of cases concern financial fraud. Child abuse material, drugs and counterfeiting are the most common cases they work on, counterfeiting representing 2 to 3 cases per year. Bitcoin is still being investigated as a phenomenon. They did work on tracing PayPal payments, however.

There is no structured training plan, so training is provided ad hoc and often by international projects or counterparts. There is a need for better certification and training. Currently Serbia has only two certified computer examiners in the force. The certification of one has even expired.

Their budget is perceived as too tight – however so the unit is challenged to provide adequate training levels for all staff.

3. Meeting with the Special Prosecutor Office for Cybercrime, Republic Public Prosecutor's Office (PPO)

The Serbian legal system is closely related to the Austrian-Hungarian system and has similarities with the French system as well. It is a system that is very open to the public, the public is in charge of filing criminal complaints, and is hence at the basis of the prosecution.

Criminal complaints are accepted in many forms, including anonymous complaints that can be made by phone. Based on the information received, and the quality of it, the prosecutor may investigate further or initiate an investigation. In certain cases an official note is made, rather than an investigation conducted.

In the pre-investigation phase and the investigation phase, the prosecutor may investigate himself, or ask the police to cooperate on the investigation. The police have the obligation to report anything relating to a criminal offence. They must notify the prosecutor as soon as reasonable doubt exists. All decisions then are for the prosecutor to make.

Direct reports from citizens are the main source of information for prosecuting cybercrime cases. Recent times have seen a huge increase in the number of the reports in 2014 (+47%, >2000 reports) and 2015 (+46%). 85% of the reports come from the citizens and companies.

The major problem in reporting systems is that citizens and companies are not acquainted with the legal systems and do not use qualified legal assistance. They often report to the police and – separately - to the prosecutor. These results in duplication of reports, sometimes victims report to three different authorities. At the moment, there is no way to prevent such duplication at the time of initial reporting.

The PPO merge cases when they discover duplication: they have a new case management system since 2013. The registry clerk puts the name and surname and social security number, then the clerk will merge cases based on this and he will provide information to the prosecutor. Each new-born gets a unique identification number which he keeps throughout his life. This number is associated with a name, surname, parents, and the places where the person lived.

In terms of intelligence, the complaint is not enriched: the PPO does not have access to other databases like, for instance, the police database. In the Chapter 23 and 24 negotiations, a new unified system for the judiciary is being foreseen and planned. It will probably become active after 2018, and it will lead to more unified case management, as the same case is kept centrally and details are made available according to the requirements and stage of the procedure. There will be a unified number for each case, for instance. The system will be a copy of the Dutch system.

Another change that is foreseen is that the PPO will become fully independent. They will have their own budget and will function as a completely independent part of the judiciary. In the judiciary initially, there was a special part of the court system that had functional judges for cybercrime, next to functional prosecutors for this area. This unit was disbanded, however, leaving only a specialised prosecutor in place. At least two or three specialised judges seem needed to cope with the caseload, and for the court system to gain more experience.

The PPO gets most cybercrime reports. Their Internet page, and good media presence assure them of a steady attention from the public, who have no trouble reaching out to them. There is also word-of-mouth and the fact that many clerks in local governmental bodies are well aware of the special prosecutor. Although there is no designated website for reporting cybercrime, there is an email address and a phone number. The media also regularly invite the Special Public Prosecutor for Cybercrime, and the Head of the Cybercrime Unit.

A major issue is the government wide drive for austerity measures. They are currently unable to hire on the scale that is required. Contrary to the rest of the government the government has granted a request to increase PPO staff with 100% and the Cybercrime Unit with 150% (or 300% according to the Cybercrime Unit), showing commitment to combat cybercrime seriously in Serbia, however.

The increase in cases can likely be explained through the increased use of broadband and mobile usage. The country is reaching 90% Internet penetration, with 75% of homes and nigh 100% of businesses being connected

Overall improvements could be made by making the Cybercrime Unit work more on cybercrime only, by training judges in cybercrime cases to a basic level and by training all regular prosecutors in cybercrime. There is also a threshold amount on prosecutions: this could be removed so all cases go to the cybercrime prosecutor.

The understanding of the PPO is that the Cybercrime@IPA was supposed to set up a judicial training centre in Serbia. Serbia is currently working to provide the envisaged training though its own means and materials. The level of interaction between the Judicial Academy in Serbia and the Regional Centre for judicial training on Cybercrime that was established under the auspices of Judicial Academy of Croatia (for all IPA region) was not discussed by the PPO.

4. Meeting with the Republic Agency for Electronic Communications (RATEL), the Serbian Telecommunications Regulator

RATEL is currently involved in making policies on the new Law on Information Security passed in January 2016.

The law itself was adopted, but four more bylaws are needed for it to become fully operational. These bylaws were expected to be adopted in the next six months, but delays occurred due to the replacement of the government. After the recent elections a technical government was appointed and the work on the bylaws could resume.

The Ministry of Telecommunications and Information Society is currently in the process of drafting these bylaws, and it is expected that the first bylaws will be adopted soon. The Ministry of Interior and the Ministry of Defence have both commented in the inter-sector consultation round, while RATEL considered the drafts to be acceptable.

The bylaws are about ICT security, protective measures for information and communication services, the content of the security act, the list of businesses providing critical information services and procedures of cooperation (including reports by industry to RATEL). The law identifies public institutions, energy, transport, telecom operators, banks and financial services as critical infrastructures. One bylaw will cover registration of other CERT teams.

The bylaws will make mandatory for telecoms operators to report incidents to the national CERT operated by RATEL, banks and financial institutions to report to the national bank, and the other industries to report to the Ministry of Information Society. For organisations which are not of public importance, they can report to the national CERT, but this will not be an obligation.

RATEL will be in charge of the national CERT. It will have to follow cyber incidents at national level, issue warnings and announcements, produce report on threats and incidents, respond to incidents (incident handling), do analysis of risks. It will also have a role in awareness raising. The national CERT will register the CERT units operating in other organisations and sectors.

All organisations are covered by the bylaws, and are required to have measures of protection in place. They will need to publish a security policy and will report incidents to the national CERT.

RATEL is currently preparing to set up the CERT operation. Once it will be in operation, procedures will be in place on how to get reports from the public. RATEL will also aim to work with some other institutions and it will organise which incidents should be sent to some other institutions. In these situations, generally, agreements on cooperation may be concluded, also with some guidelines and procedures. This instrument was used also on frequency licensing, to make sure that only licensed operators get frequency license. Similar agreements in police are foreseen. So far they have had few contacts however.

ISPs have frequent contact with the police mainly through requests in individual cases. Helpdesks do not get much cybercrime related information. Fraud is not reported at providers. Where fraud affects telecommunications operators directly, they report to the police.

DDoS attacks are a notable issue. They will be covered in the bylaws, such that if loss of service takes place it needs to be reported to CERT. In terms of regulation, ISO 27001 is required as a baseline. Specific controls also need to be there.

About reporting, they foresee that incidents are needed to be reported there based on severity, such as more than 1000 users that are confronted with a loss of service for more than 4 hours.

RATEL requires extra staff to man the CERT. They are still waiting for an answer. A recent study will indicate the ideal composition of the CERT team. RATEL is already in contact with foreign CERT counterparts. First cooperation will be with Lithuania. Also an analysis study was commissioned to recommend the number of staff and their qualifications (engineers, lawyers etc.), in an independent manner. This study is on-going, it will be ready in one month from the day of the meeting.

DAY 2: Tuesday 8th September 2016

5. Meeting with the Social Care Centre of city of Belgrade

The Social Care Centre of the City of Belgrade is taking 100.000 beneficiaries, including 4.500 who are victims of violence and neglect, and 29.000 children. It has 580 employees, half of them being social care workers.

The Centre sporadically deals with cases which are of interest to this mission.

An example was given of a 17 years old boy who has been found as being part of a chain of gay prostitution. This boy has had a difficult past (parents divorced, mother left home when he was very young) and had some hyperactivity. This activity was identified by the fact the boy had bought a 1000€ smartphone and his father found porn content on it. The phone was given to the police for analysis. Identified proceeds are a payment of 1000€ made to the bank account of an aunt (she was told the money was coming from the step mother of the boy) and the smartphone. Investigation concluded that the boy was contacted initially on social networks. The boy refused to provide more details and refused any form of psychological assistance, denied being homosexual. The case was identified by the police, who contacted the Centre. The situation has not been solved yet, and the Centre does not have the experience required for handling such difficult case.

A second case involved a mother who fell victim to a "419 scam": she left home for two years to go to the US, as she was led to believe that she had inherited. The daughter ran away from home.

Other cases involved the use of social networks but without financial motives, such as a 14 years old girl who met a 20 years old boy online, or a case of peer abuse involving the posting of images of an ex-girlfriend.

The primary role of the Centre is to cure, not to deal with prevention, but it does work with two NGOs who have facilities open daily with computers, where some training on computer literacy is provided. The Centre is not in contact with Net Patrola. For preventive measures, the relevant authority is the Serbian Institute for the advancement of education, under the umbrella of the Ministry of Education.

What the Centre considers most useful is cross-agencies trainings, with police and judiciary, but they do not happen every year due to the cost and for logistical reasons. There was such a meeting hosted by the Social Care Centre for the Rights of Children on the topic of a new Law on juvenile protection and a new protocol for protection. It was paid by the municipality.

Overall, the relationship with law enforcement agencies appears to be established and working, and juveniles identified as living in the area covered by the Centre are duly reported. This relationship does not however appear to enable the management of complex cases, when the juvenile is also an offender and requires a combination of expertise in social care and police.

6. Meeting with the Ombudsman

The role of the Ombudsman is to supervise how state institutions - with the exception of the judiciary – protect the public. This being said, it has built over the years an authority which expands beyond the scope of its mandate: it cooperates with the judiciary and the private sector pays attention to their recommendations.

While the Ombudsman does not have information specifically on proceeds of crime, violence on children enabled by the Internet is a recognised problem. Also complaints are received from parents for children whose pictures have been exposed online, and who did not know how to deal with it.

700 complaints have been received in one year in relation to children, with 1/3 of the complaints related to peer violence at school, via social networks and by SMS, a volume which is underestimate the actual size of the problem given that the result of a tour performed by the Ombudsman of the schools across the country revealed that children would only talk to peers and friends about such issues, not teachers and parents. Almost all cases include internet, social networks, SMS and MMS.

Less than 10 cases are related to sexual violence, but again it is estimated that this type of cases is underreported.

The statistics are considered very worrying by the Ombudsman as children are exposed to predators, do not know how to stop communication and how to protect their privacy. The sexual predators are Serbian.

A regional meeting with other Ombudsman took place in 2014, which issued a series of recommendations aiming at a closer attention to be paid by authorities.

A protocol on violence against children has been released by the government and supervised by the Ombudsman, but still children do not know how to deal with these incidents, and there are no trainings or awareness sessions in schools.

7. Meeting with the Administration for the Prevention of the Money Laundering (APML)

The AMPL is an administrative department, which is separate from the Financial Investigations Unit within the Ministry of Interior.

The APML receives reports from citizens by email, the motivation typically being jealousy (for instance a neighbour reporting a young man as suspicious as he drives a SUV). AMPL does checks

if the report looks comprehensive but they do not have a duty to examine the complaint. In any case, reporting by individuals happens rarely. APML calls reports from individuals "anonymous" as usually they are not signed. The authors of the reports tend to confuse money laundering with tax evasion. Individuals do not know which authorities oversee such cases, thus they report to various authorities at the same time. All this makes that reports by individuals are overrated and are negligible in volume compared to STRs reported by banks (maybe 0,1% of the cases).

Cybercrime cases are reported by banks to law enforcement rather than APML. APML cooperates with the Cybercrime Unit of the Ministry of Interior when they have requests related to some transactions, but such requests or reports are rare.

Overall, the small number of STRs related to cybercrime can be explained by the fact that a bank, accountant or an exchange office would not easily know how an offense has been committed over the Internet.

Reports are received electronically and on paper, everything is scanned and put in the electronic system, and the AMPL does its own integration for case management.

APML publishes annual reports[2], which include detailed statistics on the number of suspicious transactions received. The latest annual report has been published in 2016 and covers 2015, for instance:

Obliged entities	No of reported suspicious transactions/activities
Banks	737
Money remitters	4,881
Notaries public	2
Accountants	3
Auditors	11
Bureaux de change	4
Entities engaged in postal communication	17
Insurance companies	18
Leasing	1
Factoring	1

Also in 2015, AMPL has received 26 requests from prosecutors and APML forwarded information to the prosecution in 58 cases. According to the 2015 report, there is no specific case related to cybercrime: "Description of a ML suspicion is most commonly related to the crimes: abuse of office, fraudulent practice, abuse in the process of privatisation of companies, spending of funds for unintended purposes, embezzlement, human trafficking, drug trafficking, forgery and all sorts of organised crime, etc."

AMPL expressed a need for training and exchange of information with representatives from Financial Investigations Units from developed countries with experience on STRs related to cybercrime.

8. Meeting with the Association of Serbian Banks

The self-assessment of the Association is that the banks operate in a very complex environment and the country was facing a lot of banking incidents (fraud, including governmental fraud), so there is trust issue with banks.

The Association of Serbian Banks started to develop a security community 2 years ago, to address new regulation and the increase in incidents. A portal platform has been developed for all banks, covering IT security, security and in a more limited fashion fraud, to share information and trends.

[2] http://www.apml.gov.rs/eng35/tdoc/Annual-Reports.html

This community also deals with physical security, and believes to be the only one to propose to take additional measures, in line with the strategy of the companies. The most active CISOs in the Security Committee represent more than 60% of the market.

The Chamber of Commerce developed a similar platform on security but more focused on physical security.

E-banking has developed a lot since 2003, when commercial banks started. Today more 50% transactions are electronic.

The Association express interest in developing similar coordination with CISOs of ISPs in Serbia, and in being more connected with authorities. Some meetings already took place but until now only related to 3 cases, resulting in arrest of mules.

Regarding attacks and intrusions against IT systems, the participants are not aware of such incidents.

The situation is very different with "Man in the mail" attacks, or fraud involving fake invoices with different IBAN numbers, which are known phenomenon. The Association tries to develop awareness among customers and engage with authorities to develop such awareness campaigns, but it is not easy. There is no coordinated action on prevention.

Victims are invited to file complaint/inform the authorities.

Banks in Serbia do not protect client's infrastructure and do not refund money lost, differently from Croatia.

The Association expressed clear interest in inviting ISPs to collaborate on major attacks. ISPs current position is to say that they do not see any crime on their network.

The upcoming national CERT may be an opportunity to develop exchange of information, and the Bank Association would be open to interact with ISPs.

There is no measurement at national level on the impact of various attacks and their impact on victims.

No bank in Serbia is a member of the European Banking Association (EBA). The Association reached out to EBA regarding the topic of cooperation on security, but with no success.

Workshop

The workshop consisted of two short presentations on existing cybercrime reporting systems and practical issues related to their operation, delivered by the Council of Europe experts.

The workshop held at the end of the mission showed that there is willingness among the various players to discuss these issues and improve the collection of reports on crimes which have a financial impact on citizens and businesses in Serbia. "CEO fraud" or "man in the email" has been specifically identified as a current and important issue for the country. However, at this time, there is no mechanism for the stakeholders to meet in the future to continue the discussion and to provide recommendations and a structure 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 clearly there, but follow up was not directly organised.

Conclusions and Proposals

Conclusions

The mission enabled to identify key areas of cooperation and improvement, where the support of the Council of Europe is timely and welcome.

As regards reporting systems, there may be a need to establish a precedent as to the evidence value of online complaints. Conducting individual interviews with each complainant in some cybercrime cases (mass frauds) seems impossible, and in any case is not recommended, but remains the standard practice today within the Ministry of Interior with no immediate plans to develop online reporting.

There is scope for more work on so called "CEO fraud" (also known as "man in the email" fraud). This seems to affect many businesses in Serbia and is likely to be a thankful subject to start cooperation in the area of iProceeds.

Proposals

There follow details of the proposals, which are to be conducted by the Serbian authorities, albeit, they will likely need external support.

- Create a working group of the relevant players to engage and discuss future collaboration in the issue of online crime proceeds. It can work on CEO fraud and wider issues such as training, identifying crime patterns, laundering typologies, STR indicators and other relevant subjects.
- Further integrate the reporting mechanisms of the Prosecutor's Office, the police and possibly the national CERT. Engage the Ombudsperson in relation to children and abuse material.
- Engage all stakeholders and manage the information flow to create benefits for all stakeholders.
- Conduct a desktop case exercise related to online crime proceeds with all relevant players to identify the challenges of this type of investigation, the 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 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.
- Expedite 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.