iPROCEEDS

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

www.coe.int/cybercrime

Version 18 May 2017

Report

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

27 – 28 March 2017, Sarajevo Bosnia and Herzegovina

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 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 workplan, activity 1.3.2, as a scoping mission aimed to gather specific information regarding online fraud and other types of cybercrime reporting in Bosnia and Herzegovina. The consultants involved met various agencies responsible for or affiliated with cybercrime reporting and drew conclusions and recommendations for the reform of the system, with the aim of improving interagency and, possibly, private-public cooperation in exchanging cybercrime-related information.

A workshop at the end of the study visit served as immediate follow-up to share the preliminary findings and observations and was also used to meet the project team as a whole ad have an interactive discussion.

Participants

The scope of this mission was to visit law enforcement authorities in Bosnia and Herzegovina, the telecommunications regulator and 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 were well organised by the host country and included representatives from the following institutions:

- Ministry of the Interior of Federation of Bosnia and Herzegovina (FBiH) and Ministry of Interior of Republika Srpska)
- Brcko District Police
- Digital Forensics Centre, Ministry of Interior of FBiH
- Federal Prosecutor's Office of FBiH
- Republic Prosecutor's Office of Republika Srpska
- The Agency for Information Society Republika Srpska
- The Ministry of Security of Bosnia and Herzegovina
- The State Investigation and Protection Agency (SIPA)
- Communications Regulatory Agency of Bosnia and Herzegovina (RAK – a state level institution)

- Financial Intelligence Department (part of SIPA).

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 most of the institutions visited.

Visit Summary and factual Findings

DAY 1:27 March 2017

1. Meeting with representatives from the Federal Criminal Police, Cybercrime Unit Ministry of Interior of FBiH

Bosnia and Herzegovina (BiH) is a party to the Council of Europe Convention on Cybercrime. The Convention was transposed in the relevant legislation at the entity level in FBiH and Republika Srpska.

At federal level the Cybercrime Unit that was established in the Organised Crime Service within the Federal Ministry of Interior.

The 24/7 contact point of the Budapest Convention is at the state level within the State Investigations and Protection Agency (SIPA). At the Federation level an investigator is always on standby as a sub-contact. International cooperation with international law enforcement authorities such as INTERPOL and Europol is well established and is frequently used for the rapid exchange of information.

The current cases and initiatives in FBiH highlight recent operational and policy successes. The following cases and initiatives were described, and were selected with an emphasis on cybercrime trends, reporting and prevention:

- Banking crimes - the first successful operation is a case where unauthorised accounts access by malware infections was performed. Three organised crime groups were identified operating under this modus operandi. Law enforcement managed to stop a transfer in the amount of € 200.000 and as a result one of the groups is being put on trial now.
- Zenitsa criminal case – this is a most recent banking fraud case, which was received by a canton, which forwarded the case to the Federal Police. This exemplifies two trends: one is the way the system functions and the other that the Federal unit is considered a cybercrime hub for expertise and regional offices from all cantons are reaching up for support and advice.
- Preventive activities – there is emphasis on the importance of awareness initiatives. To better inform the public the Federal Ministry of Interior issued a press release with details how not to become a victim of unauthorised access. As a result they started to receive calls from the public requiring additional information on how to act. This press release is public and could be retrieved from the website of the Ministry of Interior.
- A mini lab for credit card fraud was detected on the territory of FBiH, located in Sarajevo. Phishing and skimming activities were conducted by foreign nationals who operated this lab. The arrested individuals were sentenced and currently enforcement of the sentence is expected.
- Trainings are organised on a regular basis but they are always looking for new opportunities. Specialised trainings related to forensic investigations, bitcoin investigation and varied advanced topics related to online investigation and networking programing are sought. Training manual on how to deal with digital evidence for first responders is developed and trainings delivered at all cantons.
- Statistics are prepared on monthly and quarterly basis and an annual report is published on the Federal Police website. These reports are submitted towards the analytical unit. The statistics are prepared based on all types of criminal activities including cybercrime. But considering that 30% of

the Cybercrime Unit's time is devoted to assisting other units in solving computer-related crimes, these statistics would not reveal a real picture of the current cybercrime situation.

The Criminal Procedure Code in the Federation prescribes the duties of the separate institutions when it comes to reporting of crime. The options available are to report a crime verbally or in writing. Verbal reporting can be done by telephone or at the police station. Verbal reports are immediately transferred into written form and signed by the reporting person.

Formal complaints cannot be anonymous. Citizens can also use email to inform law enforcement of a criminal activity, but these reports cannot be used as evidence. Statements in an electronic format are accepted as intelligence but need to be further investigated in order to be admissible. This task usually falls to police officers, who then meet the victims in person and also advise them about their rights, obligations and procedural matters, all in a format prescribed by law. Law enforcement officers are legally bound to act upon a report that is received, and will always further investigate. They are also bound to immediately inform the prosecutor.

Another option is to report directly to the Prosecutor's Office. Since FBiH has a prosecutor led investigation, the police is only an intermediary receiving the complaint from citizens through different channels. Only the prosecutor is entitled to state what constitutes a crime and or an administrative offence, the police are not to qualify the reported behaviour.

In this regard it needs to be considered that the Prosecution are keeping their own institutional statistics, which may, therefore, differ from those taken by the police.

The prosecutor can be involved in a criminal case in two ways – if the crime is directly reported to the Prosecutors' Office or when law enforcement contacts them. Then they decide whether the reported act constitutes a crime or not.

The complaint, once received by one prosecutor, stays with them to determine the jurisdiction. In some cases jurisdiction could be defined at a later stage. Jurisdiction when multiple jurisdictions are involved is based on the location where the crime is committed. If there is a conflict of jurisdiction, the federal prosecutors deal with the case and reach an agreement also among the different cantonal prosecutors.

The reporting process is also influenced by the location where a crime is reported. Victims may contact either the Federal Cybercrime Unit or a different unit within any of the ten cantons. Each of those cantons have an operations centre with officers on duty.

On the Federal Cybercrime Unit website there is also an email address that can be used to report crime. As soon as an email is received the Unit contacts the reporting person and invites them to present (digital) evidence which is in their possession. The Federal Unit is also contacted by companies if they or their customers become victims of crime. In such cases they take immediate action and, for example, contact the bank to stop a fraudulent transaction, in parallel to other steps. Overall the process, although strictly defined in the law, can be applied "quite flexibly".

Operation centres can be contacted, also outside working hours, and they have the obligation to accept the report. Whether or not they also allow reporting through email is not known at the federal level, this is for the individual cantons to fill in since they are independent administrative structures.

All ten cantons in the FBiH have their own internal Ministries of Interior. The Federal Police Administration has field offices responsible for two or three cantons in Mostar, Sarajevo and Tuzla. In each of these operation centres they have cybercrime officers. There is no direct subordination between the Federal Police and the ten cantons.

As a result of a series of successful investigations which resulted in arrests, the Federal Cybercrime Unit is recognised as the most competent group dealing with cybercrime. This recognition led to strengthening of their cooperation with other units dealing with traditional crime investigations.
As regards public reporting platforms, there is recognition of the importance of automated reporting systems. At the same time, it was stated that there are not enough funds to establish such a system. A public reporting platform will incur not only setup costs, but also maintenance and operational costs as well staff costs. There is no budget for these at this stage. A concern was also raised about the increase of reports, especially about false profiles in different social media, applications and platforms. The concern is that police staff may be overwhelmed by such kinds of reports if public reporting were made possible.

Considering the complex administrative layout of BiH, it is also of importance to determine where to position a potential reporting platform. Options discussed were:

- At the state level - similar to the Financial Intelligence Unit structure (in SIPA).
- Distinct platforms at the entity level.

There was no specific preference expressed for either of the options during this meeting. Other reporting systems that are already active were mentioned, however:

- the Child abuse reporting hotline "Sigurno Dijete"[1] which is a member of the INHOPE network;
- the Crime hunters "Crimolovats" platform, made available by SIPA, which receives and records reports related to all criminal offences and forwards the reports to the relevant services in the entities.

Within the current limits of the institutional framework of BiH, the Federal Cybercrime Unit recognises the need for a public reporting platform. Although they support the idea, a main concern is the cost involved in creating and running the system. Otherwise there are some doubts as to the consequences of the added reports and the strain they may place on the current (largely manual) reporting system. Since they are bound to investigate every report, the Unit is worried that more work may be needed, without resources available to take it on board. As to the placement of the system, there was a preference for a state level platform. It is seen to provide many advantages in scale and in relation to intelligence gathering and linking of cases.

2. Meeting with the Digital Forensics Centre of FBiH

The Digital Forensics Centre is part of the Federal Ministry of Interior. The Centre was created 50 years ago and within it, there are different laboratories. The centre employs around 40 people – mostly doctors of science, engineers, and PhDs. On yearly basis they work on around 3000 cases – mostly complex crimes, and also have around 600 court appearances. They are also responsible for connecting the judiciary to a central network that allows them to work together. This is a requirement from the Association treaties with the EU. The current network however needs further improvement.

For Automated Fingerprint Identification System (AFIS), the fingerprint recognition network, disagreement between institutions at the cantonal and regional and federal level is attributed to most police stations not having access to this vital resource.

Only mobile forensics and not computer forensics are dealt with within the centre at the moment. It is in the process of establishing a fully functional computer forensics lab. They have opened three staff positions, but filling these positions has proven hard since it is not yet clear how the forensics work will be positioned in the future. It has yet to be decided whether these experts will be employed at the Federal Police Administration or at the Centre. At the moment they sometimes

[1] http://www.sigurnodijete.ba/en/

inform the prosecutor or court that expertise can be done by the Electrical Engineering Faculty or by the State Agency of Forensics, which employs two experts.

Mobile device forensics is currently situated in the department dealing with manuscripts and documents. They deal with phone searches. No formal statistics are kept on the number of computer forensics or mobile forensics cases handled by the centre, which creates difficulties to evaluate the workload.

Computer forensics and cybercrime expertise needs to be further developed at federal level and should be following the existing structure off the Federal Investigation Police. The maximum staff members envisaged to be employed is 16, counting staff positions at the federal level as well as in the regional detachments (regional cybercrime investigators) and at the centre. For the development of an efficient computer forensics lab, besides the staff issue, there needs to be consideration for investment in equipment and software and licenses. Emphasis should also be put on the importance of sustainable training programs for the staff and for maintaining adequate equipment levels.

3. Meeting with the Communications Regulatory Agency of Bosnia and Herzegovina (CRA)

The Communications Regulatory Agency for Bosnia and Herzegovina (CRA) is a state level institution that regulates all electronic communications service providers in Bosnia and Herzegovina. The Agency is not competent for the investigation of cybercrime but has competence to deal with security incidents, especially where they involve regulated networks. At this stage there are not many incidents registered and only few examples were provided. The reasons could vary, one could be the lack of formal reporting structure for reporting incidents and another could be the low number of registered incidents.

Security incidents that were reported in recent times included the following cases:

1. A system intrusion was detected and reported by one of the operators. As a result of this incident the loss for the operator was in the amount of approximately 10000 euro.
2. One of the TV station operators was subject to an intrusion that caused heavy traffic and outages. The approximate loss was in the amount of KM 25 000.
3. The Bulgarian CERT informed the regulator about IP addresses being used for illegal activities. This report was a result of informal communication among a representative from the Bulgarian CERT and a representative from the Agency and not due to an established reporting mechanism in place.

It is currently not clear to whom an incident could be reported. If citizens experience an incident they could report it on the website of the Federal Police. On the website additional information about how citizens could report an incident could be found. However, not every incident constitutes a crime and whilst law enforcement investigates a case, it will not provide incident handling or support.

If private entities experience an incident and require incident handling or support there is currently no information regarding a r single point of contact. It is planned to establish a task force and further develop an emergency response team and platform.

The International Telecommunication Unit delegation offered support with the establishment of CERT teams. At the moment there is a functioning, but newly established CERT in BiH, which only covers state level institutions. The National Bank has its own CERT.

A major priority is to develop a cybersecurity strategy. CRA will work jointly with the Ministry of Security at state level to develop a strategy for the benefit of the whole of society. As regards

CERT teams, they would welcome if FBiH could join the state level CERT. The lack of a CERT at the Federation level might pose difficulties in future, especially for incident handling and prevention.

4. Meeting with the Federal Prosecutor's Office of FBiH

Prosecutors' Offices are established in all ten cantons. At the federal level there is the Federal Prosecutors' Office. This is an umbrella office, which monitors and provides guidance to the ten cantonal offices. They also present cases in front of the Federal Supreme Court. The Federal Prosecutors Office is composed of 12 prosecutors – one Chief Prosecutor – two deputies and nine prosecutors. Specialisations within the Federal Prosecutor's Office are not yet established. There is a concept that envisages a special department with ten prosecutors who will deal with organised crime and terrorism cases. This is currently halted due to lack of funding.

After the ratification of the Council of Europe Convention on Cybercrime the Federal Prosecutors' Office needed adequate training in order to prosecute cybercrime cases. The Centre for judicial and prosecutorial training provides at least one training on this topic per year for the last decade. As part of their capacity building efforts they also publicised a manual covering cybercrime and money laundering investigations. In addition there is also a manual regarding forensics, aimed at judges.

From the statistics from last year it is obvious that there are not many cases on cybercrime as compared to other subjects. There is more computer related crime. Case numbers were as follows:

3 – Intercepting computer data
3 – Illegal fraud
11 – Online fraud within the banking transaction system
2 – Disrupting networks
5 – Unauthorised access
19 – Unauthorised recordings
9 – Child pornography
2 - Providing minors access to pornography
6 - Credit card fraud
16 – Reports of hate crimes.

In one computer fraud case – a bank account of a company was hacked. An organised group of four hackers set up a shell company, hacked the target company and transferred the money to their account and cashed it. When the case reached the authorities the money was gone. The company reported within 3 – 4 days after the crime happened. Money mules were used to hide the path of the funds.

In these types of cases, the biggest issues are related to establishing the location where the crime was committed, gathering all the necessary data from the different providers and the use of money mules. For the successful case resolution everyone needs to work together and share information on time.

It was reported that in terms of location at the federal level of an online reporting system, such system should be based at the Federal Police Administration. Another option is to place the system at state level. This system should allow representatives from all entities to have access to it and search for information. With such system the international cooperation with multinational service providers would be facilitated but it will raise the issue of ownership. If such a model is developed at state level the logical placement should be at SIPA because they have competence at the state level.

DAY 2: 28 March 2017

5. Meeting with the Financial Intelligence Department (FID) at SIPA

The State Investigation and Protection Agency of Bosnia and Herzegovina, SIPA, is the home of the Financial Intelligence Department (FID), the Financial Intelligence Unit of Bosnia and Herzegovina. They function at the state level and cooperate with all relevant entity level authorities. The FID has police and investigative powers. Investigations conducted by the FID take place under the direct supervision of the State Level Prosecutor. The State Level Prosecutor is attached to the Court of Bosnia and Herzegovina, which is responsible for organised crime, economic crime and corruption.

The reporting process in the FID is handled by the two main departments. The Investigations Department handles investigative aspects, whereas the Analysis Department is more involved with reporting and analysis in/on individual cases/reports. Next to these departments there is the International Cooperation Department that is responsible for international cooperation, for example, with foreign counterparts in the EGMONT Group.

The Anti-Money Laundering and Counter Financing of Terrorism Law requires reporting of all transactions that (individually or structured) exceed 30.000 Convertible Marks (equivalent of € 15.000). On top of that, suspicious transactions are always to be reported. Cash transactions are also reported with the same threshold. The law clearly stipulates the obligors. Apart from banks, they include casinos, pawn brokers, currency exchanges, pension funds, insurance companies and real estate agencies, amongst others.

The law sets guidelines and minimal standards for reporting. They provide guidance for each type of obligor to help it decide what to report. The main reporting entities are banks. Most have software based AML reporting systems. Since 2006 AMLS (a software) was implemented in the FID, which is used by banks to report transactions. Over the years many other types of obligors have been brought on board. Some obligors that have a low volume of reports still report in writing (post offices, notaries, for example).

The FID uses police authority and powers under the AML and CFT legislation, in combination with typical powers of an administrative FIU. Their most important power, in the latter category, is the ability to suspend a transaction for five days. They can also order the monitoring of transactions for six months. In urgent cases information is often exchanged by phone, especially when time is of the essence.

In practice, the use of this power has not always proven easy. FID has significant experience with Business Email Compromise (BEC)/ CEO frauds. An example that illustrates this is a recent case that is still on-going. FID received a report of a company from abroad that was supposed to pay 1 Million KM to an account in BiH. The company received a (spoofed) email from the supposed supplier saying that there was a bank account change, and subsequently paid into an account operated by fraudsters. In this case the transaction was not stopped (postponed or suspended) by any of the banks involved.

Whilst FID has the ability to suspend the transaction on the request of the Ministry of Interior or the Tax Authority, the system faces some issues in these types of cases. Due to their division of competences, the FID cannot usually act *ex officio* and needs the information on the underlying case first. The main problem is that if a company is defrauded, they are likely to go to the police (the Ministry of Interior). In turn, not all police units are well aware of the FID and their powers. This causes delays that prevent them from effectively suspending suspicious transactions.

Many cases are also brought to them by banks. In case of very concrete suspicions banks notify and postpone the transaction. There are many cases where banks let potentially suspicious

transactions go through, however. The overall picture is very mixed. There are penalties up to 200K KM for missing clearly suspicious transactions. There are rules and standards on what constitutes grounds for suspicions. Even though the penalties are significant, FID stipulates this system is currently far from functioning well.

The process could perhaps be further automated to speed up reporting times, but in some cases this would not lead to an improvement: it is often human interaction and analysis that detects the suspicion, therefore a human analyst must be involved either at FID or the bank. Since the majority of STRs come from banks and they already report into AMLS directly, a major issue appears to be the internal process in the banks themselves and the involvement of human analysis which delays the process significantly. Mandatory indicators also imply the intervention of a human fraud analyst. The full automation of the reporting process is hence problematic, if not impossible. In some cases however (such as STRs based on the threshold and CTRs – structured or not) analysis is not needed and automatic reporting is done to FID directly.

It was concluded that SIPA has strong investigative skills. They have powers to suspend a transaction. This could be useful to counter BEC yet delays in processing STRs and CTRs – either at banks or at the FID often lead to the impossibility to suspend a fraudulent transaction in time to protect the victim. Awareness of FID and its powers could be improved with the entity police forces, and some processes could be reviewed (such as the analysis of automated reports, and further automation of the STR reporting process) within FID to optimise the speed of reporting.

6. Meeting with the Republic Prosecutor's Office and Ministry of Interior (High Tech Crime Unit) of Republika Srpska

The Republika Srpska has a High Tech Crime Unit that is part of the Ministry of Interior. The investigation phase is led by the prosecutor but the High Tech Crime Unit works closely with the prosecutor due to their specific expertise. Several prosecutors received specialised training for cybercrime.

In practice most victims come directly to the police station and report crimes, including cybercrimes. Reporting may also take place via phone and email. For the reporting of cybercrime there is no dedicated or specialised system in place, but the High Tech Crime Unit has a website and email open to citizens, where they can report crime. The website just has a generic form and does not ask any specific questions. Any complaints will be referred to both the prosecution and the High Tech Crime Unit, who may forward complaints to other police units.

The unit is responsible for all high tech crime investigations in Republika Srpska. For this purpose there is a High Tech Crime inspector in each of the public security centres that are present on the territory of Republika Srpska. When a high tech crime is reported, this inspector is informed and he will, in turn, inform the central unit. Information about the case can then be disseminated to other centres – if the operational need arises.

A recent investigation that is exemplary of the high standard set by the Republika Srpska High Tech Crime Unit was the DDoS for Bitcoin, or DD4BC investigation. This investigation focused on an organised gang that was offering DDoS services on the Darknet, in exchange for payment in bitcoin. Several countries and police units took part internationally including the FBI and Europol (EC3). The unit was involved in the arrest of suspects involved in the DDoS gang that offered services in return for a bitcoin payment.

Another example is the Darkode (FBI codename: Shrouded Horizon) investigation. In this case the High Tech Crime Unit assisted in the takedown of a criminal forum and the arrest of several suspects/administrators. This investigation, also, was led by EC3 and the FBI and involved 20 countries.

Due to the international nature of the threat of cybercrime, the High Tech Crime Unit often works internationally and has many and various international cases where international cooperation is needed, such as exemplified above. They try to exchange information as rapidly as possible, also internationally.

In terms of threats they encounter, the biggest issue at the moment is ransomware. The unit is also involved in other criminal cases that have "digital" aspects, so called "cyber enabled crimes". In fact most cases, nowadays, involve some form of digital evidence. In a country as ethnically diverse and divided as BiH, hate speech may be seen as a major issue, but in practice - the prosecutor reports – no – or only very few - cases were ever prosecuted.

A problem that stands in the way of deploying an online reporting solution is that complaints filed at such a platform would not have evidence value. A victim would still need to give a statement in order for the prosecution to be able to start an investigation. A victim can report online, but would then be asked to make a formal statement. This is no different in ordinary cases as there are no special provisions for cybercrimes and related (electronic) evidence.

The law sets out the procedure for gathering evidence. It consists of a classical evidence gathering procedure. The origin of the evidence will be especially important for the court, and IT forensic evidence can therefore not be taken in any format. They will usually need a forensic copy for evidence to be admitted.

All officers in the Republika Srpska High Tech Crime Unit are AccessData (ACE) certified. For cases where they have physical access to the computer this provides them with credible references, but where physical access is impossible, there is a high risk that evidence cannot be gathered or is refuted in court.

Although it could not be used for evidence directly, both Prosecutor and High Tech Crime Unit see the added value of an online reporting platform for cybercrime. If such a reporting platform would be available, incidents could be reported. The prosecutor indicates that only the High Tech Crime Unit appears to be skilled enough to deal with these issues in Republika Srpska. Prosecutors cannot keep up with developments. At the same time the management has little understanding of the threat, and has yet to form a strategic view. The prosecutor believes it would be best to set up an entity level reporting mechanism, as only limited cybercrime offences exist in state law. Most illegal behaviours are described in the entities' criminal codes, so reporting should follow this layout too. In practice, the laws in both entities do not differ much and only small differences exist in their provisions so the systems can be largely similar.

Republika Srpska seems well on track as regards the investigation and prosecution of cybercrime. There is a willingness to engage in establishing a reporting platform, although a preference for solutions at the entity level seems to exist, regarding its placement. Both recognize the importance of cooperation.

7. Meeting with the Agency for Information Society of Republika Srpska and the Ministry of Security of Bosnia and Herzegovina

The Agency for Information Society of Republika Srpska (AISRS) is the host organisation for CERT-RS, a CERT that covers the territory and all potential constituents in RS. The agency for Information Society of RS established a CERT in 2011. Its operations are governed by the Law on Information Security. CERT operations started in 2015. The CERT team consists of five staff members. The CERT provides intelligence sharing, and assists organisations in taking proactive and reactive measures (incident handling). They act as the national CERT for the entire entity, meaning that all companies and networks in Republika Srpska are part of their constituency.

The CERT in Republika Srpska makes use of email for reporting (and receiving reports) both in PGP encrypted and plaintext formats. They also host a secure website where reports can be made. Ransomware is the main threat that is currently being reported. As a CERT team they take reactive action to these reports, although sometimes they also do initial incident screening of their own initiative. They perform the basic incident handling steps, such as looking for indicators of compromise in order to enhance security and solve the issue for the future. If, during this process, indicators of criminal activity are found (as defined in the Criminal Code of Republika Srpska) they also report the incident to the High Tech Crime Unit at the Ministry of Interior of the Republika Srpska. After the criminal investigation, mitigation becomes a priority and measures to prevent further incidents are taken. Overall only few cases go to law enforcement this way.

In BiH, security awareness is low, as is the willingness to report. Better hygiene and a security culture are needed.

The CERT-RS also shares intelligence with international partners. They are working to become a member of First and to be listed and accredited at Trusted Introducer. The Croatian CERT will be their sponsor in these activities. CERT-RS has the duty to report yearly on its activities. Some of the statistics they gather are not public (related to incidents at the government) but the remainder are published on their website.

As regards the placement of a reporting platform, representatives from Republika Srpska indicate that they take a strict legal perspective on the placement of any (security related) institutions: there is a basic legal establishment of the state – and amending its tasks is not an easy process as these are defined in the Constitution. This point of view dictates that the state structure needs to perform only constitutional tasks - so placing a reporting platform at that level may lead to an unconstitutional practise as this task is not currently mentioned.

The Ministry of Security is responsible for many aspects of the security of the state of Bosnia and Herzegovina. It is, for example, responsible for data collection, international cooperation, border crossings and border protection and coordination with the entities in relation to security. They also provide forensic examination and expertise. The Ministry has very recently taken the decision to set up a CERT for the institutions that operate at the state level of Bosnia and Herzegovina. The CERT will be placed in a department of the Ministry. At the Ministry it will benefit from pre-existing connections with academia and banks. The CERT only just came into existence and is not yet operational. In the mid-term they aim for FIRST membership and Trusted Introducer accreditation. They also established relations with many regional and international CERTs and started looking at the first incidents such as the governments email servers that crashed recently. First contacts with industry have been established at a recent kic-koff meeting. Discussions on information security are starting in BiH. Since BiH intends to join EU they also work on acquiring the *Acquis Communautaire.* including the NIS (Network and Information Security) Directive. It is required to have a cybersecurity strategy and a central authority according to this directive. The legislation to achieve this can be harmonised and will then probably be implemented at the entity level. The legal framework will have to address and recognise all business and government run infrastructures that are deemed to be critical for BiH. For the moment they are working on bringing the energy and banking sector on board, but eventually all critical sectors need to be included.

Although an entity level implementation of this legislation is likely to be favoured, it will still require a central board or management body. Common goals still need to be set. In this area there are no objections to cooperation, however, so the definitive approach will mature over the next months. From the perspective of the NIS Directive there is some flexibility regarding implementation and discussions are ongoing. The NIS directive also imposes mandatory breach reporting, which will likely increase the need for reporting mechanisms to be strengthened. Prevention and detection are needed as well, on all levels.

Republika Srpska has a professional CERT, FBiH is not covered by any CERT and at the state level the Ministry of Security is setting up a CERT. This fragmented setup may cause problems, but these can be overcome by close cooperation. A nationwide cybersecurity strategy is needed, also in view of the NIS directive. Republika Srpska representatives are unanimously supporting entity level reporting systems and question the subsidiarity and constitutionality of a central (state level) reporting system. Reporting will also, likely, be needed as a requirement following the NIS Directive, which is part of the EU *acquis*. The Ministry of Security is working on such a strategy.

8. Meeting with the Brcko District Police

The police of Brcko District are an independent organisation (not part of a larger Ministry of Interior) and answers to the Chief of Police in the Brcko District. Their work is regulated by the Law on Police of the Brcko District of BiH. Due to the different police agencies and jurisdictions, crime reporting is not seen as very efficient by the Brcko District police, who – as a small force – often rely on cases brought from other police forces. The complaints mechanism for cybercrime is the same as for all types of crimes. Complaints are taken at the station and by telephone. The website of the Brcko District Police has a section about cybercrime and also lists an email address for the police, which citizens can use to report cybercrime.

The related cybercrime content on the police website was developed as part of the latest internet safety day. Although this is a good start, the reporting system lacks a form for complaints where the upload of photos and other material would be welcome too. A problem is that complaints, in terms of evidence, seem like a rather weak as evidence in a court case. Also – as a general rule - a chain of evidence is to be respected – and it is not always clear where these complaints come from. Hence they are mainly treated as intelligence.

Brcko District Police are also considering online reporting for all crime. They recently spoke to a provider of a platform for this. That company also works in Republika Srpska. They have developed a system which would be very useful for cybercrime reporting too. They have, for example, a reporting application for mobile phones, which allows for uploading video and photo material and also sends and stores GPS coordinates from reports. Uploaded photos and videos have digital signatures (hashes) making them more useable as evidence. The entire report could then also be forwarded more easily to the appropriate departments in digital form. At the same time, it is sometimes feared that having more reports will lead to lower crime resolution rates – and this may hamper development of online reporting.

According to the Brcko District Police representative, in the ideal situation, all entities would have their own online reporting system, also at the state level.

At the state level SIPA used to have a hotline called Crimehunters where people could call in. It was advertised state-wide and all manner of crimes were reported. Based on where the report was from and where a crime took place, the information would then be forwarded to entities. Feedback on the complaint was provided by the receiving institution. This system functioned well, while advertising was going on. When advertising stopped, however, awareness became less, and the system was less effective. The key is to make people aware.

In 2005 there was a project to establish a joined database for criminal intelligence at SIPA. All police agencies would be able to see the data and enter data. This initiative faced a crucial problem. The issue was that there was no clarity over data ownership and little supervision. All the proposals about ownership of data, usage and supervision were rejected and this eventually leads to failure of the partnership. Today all agencies have their own database and decide whom they share with at the entity level. It is feared that a central reporting platform could well suffer the same fate.

It was proposed that perhaps the CERTs would be appropriate an appropriate place for a reporting platform. Reports could then be referred according to territorial jurisdictions. Integration would be crucial however. Whether this is feasible is hard to assess, but from the perspective of Brcko District it is clear that they need more and better intelligence, and stand to benefit from better intelligence on cybercrime.
Brcko District Police are small but effective when it comes to cybercrime. Whilst they currently do not have an online reporting system, their size makes this less of an issue. A well-integrated reporting system at the entities level will likely provide them with better intelligence.

Conclusions and Proposals

Conclusions

Bosnia and Herzegovina has a complex institutional layout that makes it harder to deal with a national, if not an international threat like cybercrime. Especially at the federal level administrative structures are fragmented. At the same time, a lot is achieved within the limits of the current system, and no major flaws in the framework exist that would make the implementation of a centralised reporting system problematic.

Two options were discussed during the mission:

- a central system ran by a state body,
- distinct entity level systems.

There are advantages and disadvantages to consider with these two major alternatives. If a platform would be based on a state level then there might be issues related to ownership of cases and data especially due to the multitude of non-hierarchical jurisdictions. Since cybercrime is transnational, such cases might be the norm, rather than the exception. An advantage of the creation of such a platform is the volume of data which will be gathered. It will provide more intelligence and it would be easier to prepare accurate threat analysis and form a full intelligence picture. It will likely also have the advantage of available budget for state initiatives related to prevention and other campaigns. Institutions that were mentioned as possible candidates for hosting such a system were SIPA or CERT at the state level.

If reporting platforms were placed on the entity level it will be clear who is the owner of the data, and there would not be only limited jurisdictional issues, but on the other hand the information will not draw the entire picture of the country and will be segmented in two (possibly three or four) entities.

The choice for either option should be made at the state level. A decision could perhaps be taken by the strategic forum as it brings together the relevant bodies. The body could, for this case, perhaps also include representatives from Communications Regulatory Agency (CAR). A decision by the forum will create a clear line of command for all entities, and this is especially important if a shared resource or reporting system is considered, but also to coordinate the operation (especially on data sharing and intelligence gathering) between possible entity level systems, if these are considered).

Form a task-force could then be created to determine the proper lay out of such a public reporting system, considering the administrative technicalities and aiming at creation of an efficient public reporting system.

As a compromise solution, a central system – perhaps with distributed direct access for various entities institutions could be considered. Such a system could either be placed at the state level and could have entity-specific (and perhaps even state level) front-ends.

The situation as regarding CERT coverage is particular since FBiH has no active CERT on its territory.

Statistics are not unified, although the federal prosecutor and the CERT-RS appear to have a good practice in that area. Overall a better overview of statistics is needed, also in relation to the upcoming security strategy for BiH that will require a good overview of the threats and challenges that the country is facing.

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 deal with in this fashion.

Proposals

Following the mission, and given the outcomes of various meetings and discussions, the following proposals are put forward:

- Given the lack of a reporting system, and the lack of any initiative to create a cybercrime-specific public reporting system, it is first and foremost propose to decide on the nature and the placement of such a system in BiH. It is recommended to take that decision at the state level before proceeding with implementation or requests for support from external actors.
- Form an interagency working group with the relevant agencies and institutions to jointly brainstorm and develop the concept of the public reporting system. Apart from the respective entity level cybercrime units, it is necessary to better understand the needs of other agencies like the CERT, Forensics Centre, Prosecution offices and to commission the development of a public reporting system with joint specifications.
- Cooperate with NGOs and industry in order to jointly develop preventive material and public awareness 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 reported cases and prepare a national 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.
- Engage all stakeholders and manage the information flow that comes from the reporting mechanisms (CERT, MoIs) to create benefits for all stakeholders.
- Conduct an oriented desktop case exercise with all relevant players in order to identify the challenges of this type of cybercrime 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, with the ISP industry and the CERT. Awareness and reporting are shared interests.
- Further the role of CERTs and make sure FBiH has an entity level CERT. Not only should they play a crucial role in safeguarding critical infrastructure, it is a good place for co-operation between sectors and public bodies. A single national contact for foreign CERTs is preferable and coordination is needed.
- Consider more joint awareness actions with banks and possibly ISPs in both entities.
- Consider training needs of the Forensics Centre and other actors in the area of cybercrime and advanced financial crimes/money laundering.
- Automate Suspicious Transaction reporting with banks and improve response times and success rates in suspending transactions in cases of BEC, “man in the middle” or “CEO” fraud.