iPROCEEDS

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

www.coe.int/cybercrime

22 November 2016

Report

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

3 – 4 October 2016
Podgorica, Montenegro

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 is carried out under the iProceeds project work plan, section 1.3.3, as a scoping mission aimed to gather specific information regarding cybercrime reporting in Montenegro. The consultants involved met various agencies responsible for or affiliated with cybercrime reporting, financial intelligence and investigation, and the reporting of suspicious transactions. They drew conclusions and recommendations for the reform of the system, with the aim of improving interagency and, possibly, private-public cooperation in exchanging cybercrime-related information.

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

Participants

The scoping mission visited several investigation and police authorities, the ombudsperson, the prosecution service, banks - as well as any other player suggested by the host country, to get an overall view of cybercrime reporting situation from the perspective of different players.

The following organisations were visited as part of the mission:

- A Security Centre in Podgorica, where citizens can report crime in person
- The Cybercrime Unit in the Ministry of Interior
- The Financial Intelligence Unit
- The IT Forensics support Unit of the Police (Ministry of Interior) in Danilovgrad
- The General Prosecutors Office
- The Montenegrin Association of Banks
- The Ombudsperson
- The Judicial Training Institute of Montenegro

Visit Summary and Findings

DAY 1: Monday 3th October 2016

1. Security Centre (Meeting with Police and Cybercrime Unit, Podgorica)

Ways of reporting cybercrime

Cybercrime can be reported in many ways in Montenegro, but the most predominant manner is still to report in person at a police station. The bigger police stations in Montenegro are called Security Centres. Although all 23 regions have a station where cybercrime could potentially be reported, Podgorica is by far the largest contributor to the overall figure. Security Centres are the larger stations and these are present in 14 municipalities. The centre in Podgorica handles 60% of the complaints, 30% come from the Nikšić municipality (which is the second largest municipality) and 10% from the rest of the country.

As the major centre in Montenegro, the Security Centre in Podgorica takes the majority of complaints from citizens about (cyber)crime. The citizen's complaint is registered by a team of police officers. They will register each criminal complaint in an electronic database that is accessible to units throughout the country. In total 3 staff are available to take complaints in this centre. They forward complaints to the most relevant unit. For harassment or ID theft on social media, this may be a public order unit, for commercial crime, the commercial crime unit, etc. The high tech crime unit is only contacted when the complaint needs further elaboration (because of its nature – for instance), or when there is a need for further investigation (then often it is the prosecutor that contacts the unit).

Cybercrime is most commonly reported by "walk-in" complainants. Reporting may also take place via e-mail through the address of the Security Centre (this appears to be less common for cybercrime, at least). The email address is central and again, the information received there is routed to the appropriate field unit for further investigation.

Lastly complaints may come by phone.

The officers that take the complaint are responsible for forwarding the complaint to the prosecutor, if they believe, beyond a reasonable doubt, that a criminal offence has taken place. The prosecutor is in charge of the investigation that then ensues. Citizens may also report at the prosecution service directly.

Reporting is increasingly done through the national CSIRT operating under the Ministry of Information Society (http://www.cirt.me/) which has an online form for reporting incidents on their website. These reports are usually shared with the Cybercrime Unit and cooperation is reported to be very good.

International reports are mainly received through Interpol. Foreigners may also report, but the main source of foreign complaints are those of tourists, who come to the Security Centre.

Cybercrime trends in Montenegro

The receiving police units do the classification of the complaints in collaboration with the prosecutor. This data is used for monthly reports. There is also a limited intelligence function performed on all reports that are stored (such as easy counts: number of people involved…). More elaborate intelligence on cybercrime is generated manually, by forwarding all complaints to the Cybercrime Unit, who do an annual assessment.

On average, 10 complaints related to cybercrime are reported every month, including credit card fraud and excluding sexual abuse against children.

Regarding cybercrime: the most recent trend is computer fraud using a "man in the middle" attack to change or forge a new bank (or payment) account number. On this topic the police have issued 2 press releases.

Businesses also report cybercrime, such as man in the middle attacks, using the same procedure. In some cases, it is also possible for security managers of businesses to approach the deputy director of the crime police or the head of the security centre or the prosecutor.

There was an estimate of the 1.5 M€ worth of damages due to these Man-In-the-Middle attacks in recent years.

Example of a major cybercrime case (man-in-the-middle)

In one case alone - a Man-In-The-Middle attack against a company in online gambling - the damages were 1M€ of which 0.5M was recovered, covering 9 transactions. The case was that the businesses server was compromised: the criminals then opened another account with one minor difference in the name, and then approached the bank asking for a balance. Upon success, the hacker returned 900K to build trust, and then did 9 transactions extracting some of the funds. They could not recover all as they did not have enough mules. In the following investigation police closed 5 accounts in Hong Kong. No-one noticed the disappearance EUR 1.5 million because the bank had good relationships with the hacked client, and the hacker impersonated them well. Noting seemed out of the ordinary.

Only 10 days later they started an investigation. Since there was no breach, they had invoices, signatures, and the only difference was the email address, they don't have hard evidence on the hacking: the police were not able to seize the computer systems. The hacker provided so much information that investigators now believe the clients server had been compromised.

The 9 transactions came from different places, so that could have been noted. The police (cybercrime Unit) were assisted by the Ministry for Information Society and Telecommunications (there was no support from the Financial Intelligence Unit – as the Financial Intelligence Unit has 3 days to suspend the account but only with countries with which they have MoUs, but this time was Hong Kong). The money was sent back through interbank cooperation (SWIFT messages). Two Chinese nationals were apprehended in Hong Kong.

The case demonstrates that further improvements can be made, but co-operation is certainly possible. The cybercrime unit dealt effectively with the case and the case clearly demonstrates the complexity of the investigations that they work on, and highlights the need to extend capacity.

2. Dedicated meeting with the Cybercrime Unit (Podgorica)

Statistics

The unit is currently dealing with 1 to 2 charges a month. Such charges appear to be the only type of statistics which are of interest to the Ministry of Interior. They do not, however, seem to be an accurate reflection of the threat of cybercrime in Montenegro and the amount can likely increase if the Unit were expanded. There is a likely underreporting and under-investigation of cybercrime.

Compilation and tracking of statistics are not performed according to international standards, statistics are not kept through the use of databases or automated systems in the Unit. With the current capacity this will be hard to achieve, and it is worrying that work on these important issues is not possible due to capacity problems.

Staffing and training

The unit is severely understaffed, as it consists only of the Head of the Cybercrime Unit, who has been in the same role for 12 years and was the first officer in this Unit. Although 2 positions have been open since December 2015, hiring is made more difficult by a variety of circumstances, including the requirement that the successful candidate must come from within the police force and have significant police experience. The expansion of the unit is also difficult because it requires staff with a significant understanding of English and a variety of technical and investigative skills that are not very common or not readily available in the country. External recruitment is impossible at this time, due to a recruitment freeze. Should the external recruitment be possible, an issue would be the capacity to select candidates that are trustworthy. It should be expected that the number of charges brought by the unit can increase significantly if capacity is increased (over the mid term, after the team has finished induction training), since the amount of investigators time spent, given, also other important areas covered by the Unit, such as awareness and international cooperation, is likely leading to the under investigation of cybercrime.

There is no course on cybercrime in the police academy. Training could perhaps be used to expand the knowledge of those in the force dealing with cybercrime, starting with the high tech crime unit and its officers. In an ideal situation, one officer would be hired that focusses on network and IT related crimes, whilst the other could focus more on content related crimes such as IP theft, credit card fraud and child abuse. For trainings, a preferred format is workshops lasting anywhere from a few days to two to three working weeks, as a lengthier training would have too much impact on the Unit. Training for English language skills was also mentioned and deemed beneficial.

Cooperation with industry

A Fraud forum has been established between banks, which is very functional. The Unit cooperates there a lot despite the low capacity available. The focus is mainly on card fraud. The unit indicates that furthering cooperation will require its capacity to be expanded first.

As regards reporting, there is no observations that the system could be improved much, from the side of the cybercrime unit. People seem to be happy to report offline and nothing would likely change this. Montenegro is a small country, and more central processing is not needed, ad-hoc processes are relied upon to receive the required intelligence and complaints, and this, for now, seems to be the most functional system for the unit.

Awareness activities

Awareness is also taken seriously by the head of the Cybercrime unit. To give specific examples, he was due to speak in a secondary school on hate speech the day after the meeting with the Council of Europe, and the week before he had a panel where he discussed cyber threats as the police's main responsibility. He also lectures in primary schools on the harmful aspects of piracy. The Unit targets primary and secondary schools and adults. There were safety awareness sessions on how to use internet safely.

3. Meeting with the Digital Forensic Centre (Danilovgrad)

The Forensic Investigation Centre supports the gathering of digital evidence throughout the whole country from its central location in Danilovgrad. It supports all departments of the Montenegrin Police (Ministry of Interior) with a range of forensic services, and it is seen as the most promising in the Centre together with the unit performing DNA analysis.

Recently the centre has expanded the IT forensics Unit and a further 2 positions are envisaged to achieve 5 staff total. The unit is currently under provisional management: one of the deputy

directors is currently responsible for the unit despite having no background in IT forensics. This will be a temporary situation.

The unit supports the work of police directly by providing reports on the evidence that is provided to it. They only work for the police or the prosecutor. Typically, they deal with payment cards, mobile phones and computers

For IT forensics they rely on single tools, EnCase V7 is used for computers and XRY for forensics on mobile devices. The representative present (the deputy) was not aware of the precise tooling and the project team had to rely on the expert from the cybercrime unit for answers to technical questions. Dual tooling (a best practise is to have two tools, to be able to verify results) was not mentioned or practised, it seemed.

The unit clearly needs training. OSCE has provided basic training in this field, and the new staff is expected to also complete this training. More advanced level training will likely follow. The unit may well be interested in sending one of its staff to the remote learning masters that is offered by the iProceeds project. The fact that this requires visa for Dublin is seen as a problem, however. The trips to Ireland are costly and the visa process is time consuming. It is better if the training is provided in-country or somewhere with less visa restrictions. Live forensics is also a new development that they may need training for.

The high tech crime unit has good cooperation with UNICEF: they have recently sponsored the acquisition of FRED forensics machines (from Digital intelligence, US) and various other tools such as CPS (access and training on the Child Protection System, a solution for investigation on peer-to-peer networks). The process was easy and they provide easy access to their funds.

ISP Cooperation nationally and internationally was discussed at this meeting and nationally is considered quite good. 75% of the market is in the hands of Telecom Montenegro – which makes it easier. Internationally cooperation has been rather sporadic, and experience is not good, with the exception of the cooperation with Facebook which is deemed adequate.

4. Meeting with the Prosecutor's Office

The Prosecutor's Office is at the centre of the investigation and should have the best intelligence based on cybercrime reporting. The police have a duty to report all cybercrime to the prosecutor. In normal cases 90% of crime is reported to the police, and only a small percentage is reported directly at the prosecutor. This is different for cybercrime, in Montenegro. For this category, a much lower percentage of crime (60-70%) is reported to the police, and the remainder to the prosecutor directly. This is also caused by the fact that businesses often choose to report directly to the prosecution.

The police will report any criminal complaints to the competent prosecutor, who, in turn, usually opens an investigation. In relation to cybercrime, usually the high tech crime unit is contacted as a matter of course, but there is no operating instruction that governs this process. If further evidence is needed to prove a case, the prosecutor is responsible for gathering it, with the help of the police.

The prosecutor leads the investigation and directs the police throughout the process. Statistics on the types of cybercrime are not readily available for the recent times, but for the chapter 23/24 negotiations with the EU a set of statistics was especially made. It will be sent to the project team later, via email.

The prosecution service has a joint investigative team with some other authorities. One of its members had received the UCD forensics master's degree in his former role at the police (through

the assistance of the Council). This person is often referred to by the prosecutor in cybercrime cases – if the need arises.

Example of a successful cybercrime investigation (blackmailing of minor)

A good example is a 2014 case reported by the parents of a 14-year-old girl. They had approached the prosecution office directly since a 20-year-old man had contacted the girl through Viber and Facebook. Over several months they entered into chats (sexting) where she would send naked photos of herself in different positions. He then wanted to have sex with her lest he would publish the images.

This was enough to build a case for child pornography. However, all information was deleted from Viber, and some information from the mobile phone. A search warrant to get access to material on his mobile and other devices was issued. The prosecution wanted to be very cautious, without knocking at the door - so devices were not hidden. So they arranged to call him at the police station for a traffic issue, so they could get his phone, obtained 9 photos and a direct link to photos that were found on both phones and hence they could recover the complete communication. The suspect was convicted and got 6 months. The grooming offence could not be used due to the restrictive age limit of 14 years.

The case also highlights the need for better awareness and parental supervision. The Prosecutor would welcome initiatives in this area.

Areas of improvement

Generally speaking, there is no immediate need for developing online reporting beyond what exists today (reporting by email and CIRT.me website). The Prosecutor has no access to archived complaints that were not forwarded by the police, however. The possibility to report via email already exists. The main issue for Montenegro is a lack of qualified police officers that can do the type of investigation that is increasingly needed. The demands placed on new hires are perceived as potentially problematic.

This being said, the Prosecutor is not satisfied with the current level of prevention in two areas:

- online fraud (phishing, fraud using email communication)
- blackmailing related to indecent images.

In these areas, the risks are increasing and the Prosecutor would welcome online reporting from that perspective, since the low amount of loss incurred by each individual (online fraud) or the intimate nature of the offense (blackmailing related to indecent images) may lead to underreporting. A combination of more awareness and online reporting would be strongly supported by the Prosecutor.

Also increased public-private cooperation is welcomed: while the fraud forum is a best practice, the Prosecutor does not consider the cooperation with the private sector satisfactory, including with the financial sector.

DAY 2: Thursday 4th October 2016

5. Meeting with the Ombudsman office

The Ombudsman is particularly involved in the protection of children and in the five past years put a special focus on increasing the interaction with this type of victims.

Children may approach the Ombudsman directly, or by email. The Ombudsman can also take initiatives on its own, based for example on information from the media.

Until 2009, children were reluctant to approach the Ombudsman, and it was decided to start outreach activities, through workshops, a Facebook page, a blog, a complaint box online and physical boxes in educational institutions ("brave boxes"), in order to change this situation.

The impact can be seen in statistics:

- In 2009, 49 complaints had been filed by parents
- In 2016, more than 160 complaints were reported, plus other suggestions and proposals coming from children.

In the meantime, 3 surveys have been conducted on children. The first was on economic exploitation, especially begging in the streets. The second was on sexual abuse. The third was on online abuse. The need for the third survey came from the second and the focus was to understand the actions of authorities with abuse and the level of awareness.

The findings indicate that professionals working with children lack awareness on the online aspect of abuse against children. Schools also do not do enough to raise awareness of the issue by way of prevention and how to detect early warnings. In terms of enforcement, there very few closed cases regarding online abuse and only one resulted in an arrest (see above). Overall resources are extremely scarce.

The findings regarding the children are that they spend a lot of time online and have a small awareness of risks. They all know someone with a negative experience but they don't believe it will happen to them and they will not discuss it with parents and authorities but rather with their peers.

The finding regarding parents is that they have a lack of knowledge on the threats and have trust in what their children tell them and what they do.

Based on this work, the Ombudsman issued the following recommendations in 2013:

- Establishment of a national CSIRT;
- Providing a "brave box" (a physical letterbox to post issues and reports);
- Amendment of legislation to cover online abuse;
- Development of strategy papers, with one focused on online abuse;
- Making databases from different institutions comparable: so far the databases are not comparable which prevents to understand trends, connect cases, have reliable statistics on the number of cases;
- the Ministry of Justice is to act as coordinator among institutions and to coordinate with the private sector (for instance with the initiative Smart Surfing by Telenor)
- the Ministry of Education is to include content on online abuse of children (in particular cyber-bullying), train the teachers and raise awareness among the general public.

The surveys have also made it possible to understand trends on online threats:

- Cyber-bullying, which is the most prevalent threat;
- Peer violence through social media/Facebook, group mocking;
- Meeting people further to initial online contacts;
- Online Gambling;
- Indecent images and pornography.

As a way forward, cyber-bullying is clearly a topic that would require a stronger focus, ideally from the Ministry of Education, but where the Ombudsman could play a role. The capacity of the Ombudsman is limited and any specific activity on this topic would require the approval from the Ombudsman himself, but the experts within the institution do recognize that a regional workshop

to be held in Montenegro with the support of the Council of Europe could have an impact on how the country and its different institutions deal with the phenomenon.

It shall be noted that a national hotline has been set up under the Ministry of Labour and Social Welfare, which is managed by an NGO hired to run the hotline.

6. Meeting with the Financial Intelligence Unit

The Financial Intelligence Unit in Montenegro operates according to the international standards and does not differentiate from fellow units in other countries.

Regarding cybercrime, this is certainly a new area for the Financial Intelligence Unit which would benefit from trainings – such trainings would be beneficial to the banking sector as well.

Every bank has a division that is working on security, including IT and internet security. Art 36 of the AML law requires banks to prevent internet abuse for money laundering. They invest a lot of efforts to train their staff and secure cybersecurity of their software. It is also considered that the Central Bank should probably have a more active role, as they have competence for Bank IT systems.

Source of information are the banks and officers have to report to the Financial Intelligence Unit. If there is money laundering, they file the case with the police and the Economic Crimes Unit processes the case further.

In the field of combatting cybercrime, the Financial Intelligence Unit is between the source and destination of funds, which is not a comfortable position. Experience from other countries in dealing with cybercrime reporting and practices would be helpful.

The Financial Intelligence Unit welcomed the following suggestions for trainings:

- Training on improving STRs by using online and social media sources to increase intelligence,
- Tracing assets on virtual currencies,
- Working with AML officers in banks so they can report more information,
- Better cooperation with the entire chain of authorities (criminal justice, national CSIRT) and banks,
- Develop better STR indicators (at the moment the Financial Intelligence Unit uses thresholds such as payment beyond 15000€, or is aware that "man in the middle" attacks involve small changes in bank accounts).

In order to prevent further criminal attempts (like opening almost identical accounts), the representatives of the Financial Intelligence Unit suggest to focus on Western Union, involve banks (through their AML officers) and consider involving the notaries.

In order to improve access to information, the following approaches are considered:

- Provide intelligence from other Financial Intelligence Units and involve other stakeholders (banks, notaries…)
- Get reports from the public and challenge the other stakeholders
- Collect intelligence proactively and challenge the other stakeholders

7. Meeting with the Montenegrin Association of Banks/ Two AML officers from banks

This meeting took place with two AML Officers, one who acts as chairman of the AML officers grouping and another officer who was until recently working at the Financial Intelligence Unit. Both are there on invitation by the Montenegrin Association of Banks.

The situation depicted by the AML officers is indicative of a country where face-to-face interaction between banks and customers is the norm, with a limited use of e-banking services. The result is that online frauds still have a limited impact. Typical frauds are forged credit cards, use of forged documents and social engineering.

The embryonic phase of development of e-banking does not mean that Montenegrin banks are protected from all threats, in particular from social engineering. The predominant way of face to face interaction with customers also exposes the banks, as it can be challenging to ask an ID card to every customer. Banks have insurance against this type of fraud but they nevertheless need some training.

When it comes to IT security many processes are organised and controlled at the group level , especially in the case of international banks operating in Montenegro. There are hardly any examples of banks operating in Montenegro only.

Within banks, AML officers are totally independent. They are nominated by the board of directors, they report to the board and to the Financial Intelligence Unit (they typically are recruited from the Financial Intelligence Unit even). Usually AML officers operate under the compliance department but in Montenegro they started to be appointed before the compliance mechanisms were developed, which give them a special position: the only 2 departments within the banks are AML and internal audits.

Regarding the exchange of intelligence, the AML system mainly works on information coming from within the bank organisation and the AML officer initiates contacts with the FIU based on information collected in the Banks database and Fraud detection systems. These checks are done by banks on their own and AML officers report these incidents to fraud or compliance departments internally: in the case of hacking, the antifraud officer and the AML officer would inform each other: the AML officer has to report formally which is rigid. For this reason, informal reporting through other teams is often more efficient.

The AML officers expressed strong interest in getting more information on how virtual currencies work and could be a source of fraud. This could be done by joining cross-disciplinary groups with expertise in this field.

Workshop

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

Overall, the population of Montenegro is gradually developing its usage of online services, and awareness of risks remains low especially among adults. Children seem to have a much more acute understanding of online threats, but they don’t share their experience and parents ignore that their children conceal such knowledge. Currently the younger population is faced with cyber-bullying and blackmailing related to indecent self-taken images, and as they will start to own and spend their own money they will be more exposed to online fraud. It sounds therefore more than timely to begin activities that will address both the needs of the younger population in the few coming years, and convince the more senior part of the population and the authorities that the country is facing today some risks and needs to prepare to increased threats in the near future.

In this context, the absence of the Ministry of Information Society and its CSIRT was considered as a gap that should be addressed moving forward. The participation of representatives from the Prosecutor’s Office, the Cybercrime unit and the Ombudsman would also have been valued.

Conclusions and Proposals

Conclusions

The activities were well organised and demonstrated a commitment of the country to engage in the project. Some key players did not respond to the invitation, however. Especially the lack of ISP presence was noticeable, as well as the absence of the CSIRT.

As regards reporting, the Montenegrin system has a heavy reliance on manual reporting methodologies, although online reporting volumes seem low. Speaking to each complainant in some cybercrime cases (mass frauds) seems impossible in the long run. The system produces no or limited statistics and since there are significant numbers of complaints that go directly to the prosecutor, there is a risk that the police are not able to derive the full intelligence value from these reports. The prosecution do not have any regular statistics gathering process. Setting this up could also be a solution to the lack of accurate statistics.

The Cybercrime unit is understaffed and needs expansion. The single officer of the unit is clearly unable to cooperate effectively amongst the multitude of actors in this field. The Unit needs expanding to adequately deal with this complex area, and a focus on charges brought is not a fair measure of the Units effectiveness, especially when no adequate statistics are kept on the threat of cybercrime. Adding to this are the international nature of cybercrime, the many projects in this area and the demand placed by the police organisation. It is recognized that the current staffing is insufficient but the hiring process is slow to take place. The requirement that any candidates have 6 years of police experience may well be overkill, and could be reconsidered. The forensics unit is currently being expanded too and expects to be adequately staffed in the near future. They are in need of training.

There is a gap between the young population which is already commonly exposed to online threats (cyber-bullying) and the older generations who have yet little use of online services and are not aware of the current and upcoming online threats that the younger people face today and will face tomorrow. This gap can be turned in a positive exercise where the different generations can be made aware of the threats and provided with adequate ways of reporting incidents.

Proposals

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

- Create a working group of the relevant players to engage and discuss future collaboration in the issue of iProceeds, in particular and wider issues such as reporting, training, identifying crime patterns, laundering typologies, STR indicators and other relevant subjects.
- Consider an online reporting system.
- Engage all stakeholders and manage the information flow that comes from the reporting mechanism to create benefits for all stakeholders. Consider centralizing the processing more either at the prosecutor or the police, and consider using the reports more for intelligence purposes and statistical purposes.
- Conduct an iProceeds desktop case exercise with all relevant players in order to identify the challenges of this type of investigation, also in relation to reporting, and assess the distribution of responsibilities and opportunities for future collaboration and possible training needs.
- Improve the cooperation of the government agencies involved in cybercrime and financial investigations, with the ISP industry and the national CSIRT. Awareness and reporting are

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

- Consider training for the new staff of the Forensics Unit. They have recently been expanded and may have good use for a forensics master training.
- Other training is likely more effective if delivered as workshop (short) and in-country.
- Consider joint awareness action with banks and possibly ISPs. The Prosecutor was very open to this suggestion.
- Consider regional workshop on cyber-bullying led by Ombudsman with a focus on awareness raising, improving online reporting and developing common criteria for databases among different institutions