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

www.coe.int/cybercrime

Version 15 June 2017

Report

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

15 - 16 March 2017, Ankara
Turkey

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 using 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 several 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 1.3.6, as a scoping mission aimed to gather specific information regarding online fraud and other types of cybercrime reporting in Turkey. 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 ad have an interactive discussion.

Participants

The scope of this mission was to visit investigation and police authorities in Turkey, 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:

- The Ministry of Justice
- The Prosecution for cybercrime, Ankara
- The Financial Crimes Investigations Board (MASAK)
- Turkish National Police (TNP):
    - TNP Police Station in Kavaklidere, Ankara
    - TNP National Cybercrime Department, Ankara
- The Information and Communication Technologies Authority, ICTA (host of the national CERT team, USOM)
- The Ministry of Family Affairs
- The Turkish Banking Association.

The workshop at the end of the mission was used to discuss international best practises and the preliminary findings of the experts and involved representatives from most of the institutions visited.

Visit Summary and factual findings

Day 1 – 15 March 2017

Meeting 1: Visit to the TNP police station in Kavaklidere, Ankara

The TNP Police Station of Kavaklidere, Ankara is a regular local police station of the Turkish National Police. The station covers an urban area of Ankara and is one of 40 stations in the city. This station covers a district of 100.000 people.

Police and gendarmerie share the Turkish territory. The police manage cities and urban spaces in 59 districts; the gendarmerie covers the countryside, where there is no police presence.

There are no dedicated cybercrime officers or specialised investigators in the local police stations. The regular police stations do not face many cybercrimes. There are, however, many phone scams and fraud complaints to deal with. The few cases of cybercrime that were received were brought to the attention of the specialised cybercrime unit.

In the event of a criminal complaint, including one related to cybercrime, a complaint may be lodged directly with the local police services (police station or gendarmerie brigade) or directly with the specialised cybercrime unit in the provinces or with the public prosecutor. The 59 cybercrime units used to be part of the Smuggling, Serious and Organised Crime Department but were made into specialised units after cybercrime was given priority. These exist since 2011. The gendarmerie has also recently set up a cybercrime unit.

The initial training for police officers does not include first responders training. Police officers do not receive feedback of the complaint they take and send to the specialised cybercrime unit.

The cybercrime units investigate the cases, under the lead of the prosecutor and send them to the prosecutor when the investigation is concluded. The cases go on Polnet, a special automatized network accessible to police units throughout the country, which registers the status and main information of cases. Forensics is handled by specialised units too; 17 forensic hubs are present in cities and cover the entire country.

Prosecution and police have two separate networks. Prosecutors and judiciary use UYAP, the police use Polnet. Whenever the police take a statement or finds relevant evidence, it goes to Polnet. If there are multiple complaints in different jurisdictions, all statements are sent to one station. In practice Polnet and UYAP only have limited cybercrime related functions or fields and without a suspect it is not easy to combine intelligence and create cases.

Awareness and prevention are seen by the police as tasks for the private sector. It is mainly banks that are active on these issues.

Computer engineers and other specialists can be hired from the civilian side too and are then to graduate from the Police Academy. Computer engineers can also be contracted directly, but in this case, there is a legal requirement for them to be certified.

Reportedly, a problem at the TNP is that inspectors are moved, rotated or assigned different tasks in relative short periods of time. In this context, specialisation appears to be a problem. The initiative to transfer or promote officers lies with the governor and a provincial police chief. After graduation, it is difficult to keep people in their specialty roles. Another difficulty lies in the fact that police officers have the obligation to spend two years in eastern Turkey, considered as a difficult region. However, cybercrime is not a major issue in that region. This mandatory placement also interferes with specialist training and development.

Meeting 2: The TNP National Cybercrime Department in Ankara

Next to a total of 59 regional specialised units, Turkey disposes of a central Cybercrime Department in Ankara. Serious (cyber)crimes will be reported directly to the specialised units, often even before statements are taken. Electronic evidence can be seized by the local police and is sent to forensic units or the national forensic unit, which is co-located with the national Cybercrime Department. Forensic units (hubs) are responsible for several districts at the same time.

The national Cybercrime Department of TNP falls under the Security Department of the Ministry of Interior - they are a separate hierarchy. The department is mandated for any investigation regarding cybercrime. The specialised units oversee cybercrime related investigations which are not conducted by the national Cybercrime Department. The Cybercrime Department deals with cases having a national impact, a multiplicity of victims or offenders in Turkey and/or abroad. The specialised units also give technical support to other units in other crime investigations. They function as mixed forensics and cybercrime units.

Turkey started its cybercrime structure in 1994. The current cybercrime units were initially local support units. It soon appeared that financial crimes often overlapped significantly with many cybercrime investigations, so they were then structured accordingly as a part of the provincial organised crime units. Only when electronic evidence and cybercrime became pervasive, was it made into a separate department, growing from units to divisions, to a national department. As a result, reports can still come in at many places – even though some steps were taken to have a more central system at the Cybercrime Department in Ankara.

The prosecutor leads all the criminal investigations. Law enforcement officers conduct investigations on behalf of the prosecutor. They are also tasked with pre-investigative intelligence gathering, but as soon as officers learn of a crime, it should be promptly reported to the prosecution.

As regards IT systems, in practice, the Polnet and UYAP systems are both used for intelligence especially to review whether cases are reported across regions. Any overlaps are detected across the automated files and are obvious in the system. The two separate systems mean that the police have to manually transfer files to the prosecution, which do not have access to Polnet. To improve this, in the long run, the main ICT system will be UYAP and Polnet will be phased out. UYAP can also work (and, in part, already works) with gendarmerie and other law enforcement agencies. As a universal system, it helps the prosecutor to choose between the different enforcement agencies. It can send correspondence between them securely using digital signatures.

An issue is that these systems works well with known suspects or fixed identifiers (addresses, telephone numbers), but it is difficult to combine cases based on other, less individual markers. When they are dealing with unknown suspects the results are less, therefore: the system was not designed for this and police must coordinate intelligence manually. In practice, the Cybercrime Department tries to recognise patterns and combines intelligence and looks at the modus operandi. All cybercrimes are classified with a default form, which is sent to the Department from provincial units. This way any overlap or similarity should be detected between provinces, for example. In everyday practice, such a system is not operational and the current systems are not always able to do this.

For example, when it comes to online complaints, often citizens file complaints many times over by email and at multiple stations and institutions. 57 analysts work on analysing the incoming complaints, although citizens may file them elsewhere too. Since most of the time no feedback on complaints is given to the public, this often prompts them to file a complaint at several institutions (cybercrime units and prosecution, in several regions, for example). According to legislation, law enforcement officers must act on all reports and reporting can be done in many forms and at many institutions. This makes the task of creating meaningful intelligence on cybercrime much harder.
Given their experience with decentralised (mostly email based) reporting, the Cybercrime Department is working on a more advanced reporting system. It will include a mobile application, a browser plugin and will incorporate reporting related to social media. It will relay all relevant information, such as URLs and usernames, to a central database.

In practice, complaints come in through letter, are made at the police station in person, or come through online means (either at the police website or via online reporting systems at the President of the Republic of Turkey and Prime Minister’s office). Complaints and statements are made to police in the street. Merged cases are forwarded to the relevant province.

When it comes to territorial jurisdiction, when there is a clear place of the crime the investigation is started at the place of the crime. International complaints, cases with unknown suspects and unclear jurisdiction are more difficult. The location where the crime was learned about, then determines where the investigation is started. For example, a request via the 24/7 network that contains relevant information will be dealt with in Ankara as there is no “place of the crime”. The 24/7 contact point is with the national Cybercrime Department.

Each provincial cybercrime unit keeps its own statistics and sends them to the Department in Ankara that elaborates and forwards them to other authorities. Cybercrime statistics are not made public. At the end of the year the Ministry of Interior publishes statistics and makes them public, but there is no easy way to access the statistics online.

Meeting 3: Visit to the Digital Forensics Unit

The Forensics Unit is co-located with the national Cybercrime Department in Ankara. In Turkey, the forensics procedure for IT-forensics is regulated by Article 134 of the Criminal Procedure Code (CPC). According to the CPC, law enforcement can only resort to electronic evidence if no other evidence is available. There needs to be an appropriate level of doubt regarding the suspicion, and a decision of a judge is necessary to proceed with any search for/on electronic evidence.

Once a search is conducted and material is detected, it can be investigated on-site (as defined in the judge’s order) or it can be seized and investigated later if there is no possibility to do it on-site. The first step is always to make a forensic image. Since 2014 Article 134 CPC stipulates that a copy is always given to the suspect. In practice, at least two copies are made from the original copy: one for the prosecutor and one for the suspect.

The original material is not touched. Any seizure of computers or data carriers is only temporary in principal. Only copies are made and this leads to issues. With big data or large file systems, partial imaging or live investigation can be done with help of experts in the system.

Article 134 does not allow for seizing the computers involved. However, giving back illegal material is an issue in many cases. Also, copying on-site is not always perceived as an ideal solution.

Given these drawbacks, it may be needed to change the system as currently it is not always possible to seize computers and all seized computers must be given back after forensic copying. Paragraph 2 of Article 134 CPC lays down cases when police can seize computers: for example, when encryption is found, or when on-site copying does not work. The provision also makes clear that no passwords can be asked from suspects due to the prohibition of being forced to self-incrimination.

There is no standard operating procedure for the seizure and confiscation of virtual currencies. It would both be possible to convert it in the fiat currency, and to hand them back in "digital" form. In case of online wallets, the password could perhaps be changed as a means of "seizure". In fact, the current Article 134 of the CPC makes it impossible to keep a wallet on a copied system in possession of the police, as seized data carriers are to be handed back to the suspect. If it is clear that they are crime proceeds, they should be seized however – and AML legislation provides for the possibility. The virtual currency can either be handed back after the investigation or converted after being obtained. In the latter case, there is a risk that the currency goes up or down due to the volatile exchange rate, so if a court finds against the prosecution, there may be a claim for damages.

The most significant cases are dealt in the central lab and different labs in the main cities. In 67 of them, there are mobile forensic capabilities: 54 provincial units and the 17 regional forensics hubs. The provincial units oversee first response, work with the provincial units; so only in exceptional cases is material forwarded to Ankara. In the few provinces without specialised units, the Smuggling and Organised Crime Department oversees cybercrime cases.

Meeting 4: Ministry of Justice and the Prosecutor for Cybercrime cases in Ankara

The prosecution is independent from the Ministry of Justice and the latter is involved in some aspects of human resources, international relations and general legal affairs in relation to the prosecution. The High Council of Judges and Prosecutors (HCJP) is in charge of the organisation of the prosecution, although prosecutors have operational independence. A dozen prosecutors are responsible for all types of cybercrime within the country. They take reports from the public too.

Turkish legislation has been harmonised with the Budapest Convention. The Ministry of Justice is currently working on amendments regarding ATMs and skimming, criminalising the installation of skimming devices, and article 134 CPC, related to the search of computer data. The latter may make it clearer what the status of mobile phones and tablets is, as the current Article 134 only mentions "computers" as object of searches. The current accepted interpretation of this article is broad, thus no immediate issue exists.

Preventive measures and awareness related to cybercrime are under the mandate of the Ministry of Interior. There is a lesson on law and justice in schools.

In the Ministry of Justice, there is a specific General Directorate dealing with judicial statistics. They mainly focus on common crimes, which are classified by category. This information is public. The source of this data is the UYAP system. 2017 was named the judicial statistics year and there are activities to improve data entry into UYAP as complete data entry is important.

UYAP also holds the applications and/or complaints filed by the public. This data is also categorised by article of the Criminal Code and is entered in the system accordingly. It may sometimes be reclassified. UYAP currently works with two enforcements agencies: the police and gendarmerie. Because the gendarmerie is fully integrated in UYAP no exchange of paper is needed. The police still use Polnet and exchange complaints and case files with the judiciary on paper. UYAP is scheduled to be integrated at the police so they can use digital signatures and communicate electronically.

The prosecutor will choose which LEA to work with in each case, and will communicate with them via UYAP. UYAP also has several measures to inform other parties. For example, a citizen's cell phone number can be integrated so they can then be informed by SMS on any of their on-going cases. The Turkish e-government website also lists on-going investigations that a citizen is involved in.

Reports received from the public can be used as evidence directly. Complaints form part of the case file of the prosecution. The probative value is for the judge to decide on. In many cases the police must act upon information received about a crime, it is mandatory for the police to start an investigation. Complaints often constitute a starting point of such investigation, but are often not used as the only evidence. Anonymous complaints, by email, for example, are possible, but may not be taken as seriously as others.

Meeting 5: The Information and Communication Technologies Authority, ICTA and national CERT, USOM

The National Computer Emergency Response Team (TR-CERT) is called USOM in Turkey. It is Trusted Introducer accredited since 2014 and is a FIRST member. The CERT is hosted by the Information and Communication Technologies Authority, ICTA.

Corporate or institutional CERTs (called SOMEs) are working under by USOM and some 500 are in operation at various institutions and businesses. For critical infrastructure providers, such teams are mandatory. They are involved in designing security measures and perform incident handling. There is mandatory breach reporting and SOMEs report breaches to USOM. Internet Service Providers (ISPs) and other telecommunications service providers also have corporate institutional CERTs (for example, mobile operator Türkcell and ISP Superonline both have a SOME team).

User complaints and especially incidents are relayed by corporate CERTs, who will first define if a case is a criminal case or a mere cybersecurity incident. Their reporting takes place accordingly, if it is a criminal case, it is communicated to the prosecutor or the Cybercrime Department since USOM is not mandated to receive criminal cases. If it is not a criminal case, it must be reported at USOM, and the institutional CERT will fill in a designated notification form. Other procedures follow depending on the notification that is made.

There is also an assessment form in which the applicants assess the size and impact of the incident. The forms are forwarded via email or on paper. USOM collates these notifications for threat intelligence purposes. Although reporting is mandatory for institutions (not citizens), it is believed that there is underreporting. Administrative fines (issued by the sectoral regulators) may be issued if reporting is not performed. Some incidents, such as outages, are detected via USOM directly. USOM then asks for feedback on the incident from the corporation or institution involved.

Between the institutional CERT teams (SOMEs) and the national CERT (USOM) there are sectoral CERTs. A total of eight CERTs serve different sectors such as the energy, telecommunications and financial sector. USOM also acts as the government sectoral CERT. The main threats that are perceived are Internet of Things (device) security and the low security awareness throughout the private sector. Although cooperation between national CERTs is good, private sector cooperation reportedly could be improved.

Day 2: 16 March 2017

Meeting 6: The Ministry of Family Affairs

Turkey has a national action plan on children rights spearheaded by the Ministry and involving ICTA – the latter in relation to online activities and behaviour. ICTA have a special website that raises awareness for child safety online, as well as a generic one.[1] In every province there is a separate children’s unit in the police that cooperates with the local directorate from the Ministry.

[1] See: http://www.guvenlicocuk.org.tr/ (children) http://www.guvenliweb.org.tr/ (all audiences)

Complaints are often related to abuse and may come in via a national hotline available at telephone number 183. The relevant ministries work together on (abuse) cases. As an ultimate measure a child may be removed from its parents and be returned only after counselling and an extensive period in state care. The Ministry of Health has Child monitoring centres. These centres are placed in the country according to the needs of a province or region.

There is also cooperation with civil society organisations and the Ministry strives to give child victims appropriate care, so they are not with the police for long, but instead they try to keep the child in home type environments.

The Ministry does not use the internet for receiving complaints but mainly relies on the 183 hotlines. Children can use it and make complaints there if they can express themselves. Complaints may come to the Ministry via different routes as well – mostly via institutions such as schools and hospitals.

ICTA operates a hotline for several types of illegal content. The hotline is a member of INHOPE. A website takes reports of different types of illegal content, including child sexual exploitation, but also prostitution, drug abuse and a variety of other contents.[2]

There are also Child Ombudsperson in Turkey, under the auspices of the national Ombudsperson's Office, where children can report issues. Children can call or write to the institution.

Meeting 7: MASAK - The Financial Crimes Investigations Board (FIU)

The function of financial intelligence units (FIUs) operating in many countries is to fight against laundering proceeds of crime. In Turkey, this is the task of the Financial Crimes Investigation Board (MASAK), which is a main service unit of the Ministry of Finance and is directly attached to the Ministry as an administrative agency.[3] Today, MASAK's mission is to create a clean society by preventing money laundering and terrorism financing. Terrorism Financing was formally added to MASAK's tasks after 11 September 2001 but legal arrangements only followed in 2009 and operations began in 2013.

STR reporting is largely automated, and is based on an XML scheme that is mandated by law, and uses a system called EMIS. Certain obliged parties still report by mail or courier however. The following numbers (data for 2017 is total for January and February) of STRs and information requests by prosecutors are reported by MASAK over the past years:

Year	**2013**	**2014**	**2015**	**2016**	**2017**
STRs	25592	36483	74221	132493	32532
Denunciations and Demands from prosecutors	498	622	642	6419	4854
TOTAL	**26090**	**37105**	**74863**	**138912**	**37386**

The distribution of STRs across the reporting entities clearly shows that banks are the most active reporters. This can, in part, be explained because they use an automated system that processes a large volume of transactions.

[2] See: https://www.ihbarweb.org.tr/
[3] http://www.masak.gov.tr/en/content/presentation/146

Years	**2013**	**2014**	**2015**	**2016**	**2017**
Banks	22086	31146	66719	117007	28812
Capital Markets Brokerage Houses	177	209	151	371	158
Financing and Factoring Companies	775	2065	2597	7252	1321
Insurance, Reinsurance and Pension Companies	629	693	491	1980	449
Authorized Exchange Offices	897	498	603	844	186
Payment Service Providers & Electronic Money Institutions	*NA*	*NA*	*NA*	671	569
Others	1028	1872	3660	4368	1037
Total	**25592**	**36483**	**74221**	**132493**	**32532**

STRs are analysed by an automated system and receive a score based on several factors such as:

- Relationship of any of the entities persons or accounts to previous reports;
- Presence of a criminal record for persons involved (to the first degree: also, family);
- Characteristics of certain scenarios or of the account (such as opening and closing dates)
- Relationship to the other account traffic (the mean transaction amount, or account turnover);
- The indication of the type of STR (obligors choose from 28 categories many of which are directly related to criminal activities);
- The free text fields are also scored based on keywords. For certain categories keywords are analysed and scored for presence.

Scoresnare calculated both for the money laundering and for the terrorism financing risk separately. Scenarios are also used to score and their application and scoring is dynamic, and depends on the STRs parameters. A taxpayer with no previous payment records, for example, and no records of income will receive a very high score if he transacts for high amount, for example.

Further analysis is done largely based on access to databases that MASAK has. In total, they have online access to 51 data types at 14 institutions, and an offline data warehouse that holds 120 data types from another eight institutions. With banks, further data can also be exchanged using the automated EMIS system. They also use open source data such as social media and online searches.

All denunciations are investigated this way and STRs are selected. Since the prosecutor is leading their requirements are always observed. For example: if STRs are about an on-going case, they will always be forwarded to the relevant LEA investigator.

STRs are, otherwise, selected in EMIS based on many parameters. High scoring transactions are investigated and analysed but terrorism related STRs will always take priority, for example. The system may also cluster STRs based on common parameters. A special unit in MASAK occupies itself with cybercrime and analyses all STRs related to this category. Reports on cybercrime from the last eight months can be broken down as follows:

Cybercrime related STRs			
Received:	13.913	Analysed:	4000
Analysis reports were sent to:		Related to:	304
TNP Cybercrime Unit	35 reports		
Relevant Prosecutors Office	6 reports		
Banking Regulation Supervisory Authority	2 reports		
Turkish Tax Inspection Board	1 reports		
Total:	44 reports		
AML Cases opened	3 cases	Related to:	>400

MASAK has activity reports which are public and online.[4]

Meeting 8: Visit to the Banks Association of Turkey

Article 73 of the Banking Law[5] allows banks to share information on fraud cases. Next to the Credit Bureau, which is the subject of this meeting and report, two other platforms exist, the Interbank Card Center and the Banks Association of Turkey (Türkiye Bankalar Birligi)[6]. The Card Center is mainly used for card related events, such as skimming and credit card fraud and has a liaison officer to the National Cybercrime Department. The Banks Association is used to communicate between fraud teams directly.

When banks register to the Credit Bureau they commit to sharing information and data. For this purpose, there are two portals:

- SABAS (Sahte Bilgi Belge Beyan Başvuru Alarm Sistemi[7] or the Fraud Detection and Prevention System) is dealing with fraudulent papers and documents that are used, for example when applying to a bank.
- IFAS (Internet Fraud Alert System) is dealing more with internet based fraud attacks, mainly in relation to online banking transactions and operations.

The main task of the Credit Bureau is to assess the creditworthiness of Turkish citizens and residents applying for banking products.

IFAS uses a website to share the information between fraud teams at banks. It is used by the fraud bureau in most banks. Apart from successful frauds attempts, they also log unsuccessful attempts. Information that is accessible mainly pertains to people (name, address, ID card number, email address) and IP addresses involved. The system is only accessible for bank personnel. 99% of the attacks on the system relate to social engineering. Although victims are in the system, they are not provided special protection (for repeat attempts or protection of vulnerable citizens for example); the system is mainly used to identify perpetrators. Banks also rarely provide information on the victim. The capability is there, but is rarely used. Usually a customer has only one bank, so it is believed victim registration is not needed beyond their own bank.

SABAS is used for application fraud and besides the (true or false) name, address, ID card number and email addresses involved, mainly contains any, all identifying information that can be found on the application, such as identifiers of the cell phone used. Information in the system is colour

[4] http://www.masak.gov.tr/userfiles/file/ACTIVITYREPORT201521.04.2016.pdf
[5] https://www.tbb.org.tr/english/5411.doc
[6] http://www.kkb.com.tr/media/12128/kkb-faaliyet-raporu_2016.pdf
[7] https://www.tbb.org.tr/en/home

coded (red for false, green for true, victim related information). The system also logs all information to failed application attempts. Data for the system is fed by the banks fraud teams. In smaller banks this can also be the audit and/or internal control unit.

The wider use of the Credit Bureau data is to vet applicants for creditworthiness not just to make records for fraud they detect. Further to that there is a lot of cooperation in this system overall, regular meetings are organised, and sometimes DG Security or the National Cybercrime Department are invited. If there are major operations or incidents then there are various ways in which they communicate and give information.

There is a strong cooperation and although the following three organisations, the Interbank Card Center, Banks Association and the Credit Bureau, involved in baking fraud overlap somewhat, this does not lead to problems in practice.

Conclusions and Proposals

Turkey has a system for combating cybercrime that is consistent with its desire for good cybersecurity and the various threats the country faces. The training and competence of magistrates and police services is strongly supported by an appropriate level of technical means and a firm will to improve.

In relation to reporting systems, Turkey has a challenge ahead. Although many infrastructures are partly useful to detect and register cybercrime cases, the decentralised nature of the (specialised) police units and (partly specialised) prosecution make it hard to coordinate intelligence on typical cybercrime cases, especially when, as is the case in the majority of cases, the suspect is not known, and the internet resources used vary and require analysis to recognise a connection. A more centralised reporting system to enable better analysis of the available information is needed. This will likely, also, prevent duplication of efforts across regions and law enforcement units. The Cybercrime Department is underway with a project that seems to make the system more effective and centralised, and has the ability to provide the (significant) analysis capability that is needed. More centralised and more structured reporting (as in: reporting resulting in structured data, rather than free-text options such as email) will likely free up capacity to make more advanced (and more useful) intelligence and analysis available.

The banking sector uses some of the most advanced anti-fraud (data exchange) systems (IFAS, SABAS) in the region and can serve as a model for other countries.

Overall, protection of victims of fraud (in the banking system) and vulnerable citizens (children, elderly) could sometimes receive more attention. In the banking sector, no protective registration in the Credit Bureau systems is applied, whereas this could easily protect vulnerable people. Also, awareness and prevention are not receiving the attention they deserve. The Ministry for Family Affairs, for example, has a limited presence online, and reporting is done mainly by phone.

Proposals

The following is proposed to further enhance Turkey's ability to detect cybercrime and obtain timely reports, evidence and intelligence:

- A more central cybercrime reporting system could be developed (along the lines of the project for reporting at the National Cybercrime Department) and should include easy means of reporting structured data, to cut back on the extensive manual analysis done at the Department, and to create a better intelligence picture. The thousands of emails that are currently being analysed seem unfit for this purpose.

- When the public reporting system is developed accordingly: 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, Cybercrime Department, cybercrime units, Gendarmerie, Hotlines, Social Care/Ministry of Family Affairs, MASAK, etc.) to create benefits for all stakeholders.
- Content and a mechanism for training first responders should be introduced in the Police Academy (both for initial training and in-service) to make sure local police units have a basic understanding of electronic evidence.
- Consider adding protective registration of victims in SABAS and IFAS to prevent their (stolen) identities to become victimised several times over.
- 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.
- Consider more joint awareness actions with banks and possibly ISPs, in order to create more awareness of cybercrime with businesses and the general public.