This Project is co-funded by the European Union and the Council of Europe.
Bu proje, Avrupa Birliği ve Avrupa Konseyi tarafından birlikte finanse edilmektedir.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

PREVENTING AND COMBATTING CYBERCRIME: KEY FINDINGS AND RECOMMENDATIONS FOR TÜRKİYE

Strengthening the Criminal Justice System and the Capacity of Justice Professionals on Prevention of European Convention on Human Rights Violations in Türkiye

European Union – Council of Europe Joint Project

This Project is co-funded by the European Union and the Council of Europe.
Bu proje, Avrupa Birliği ve Avrupa Konseyi tarafından birlikte finanse edilmektedir.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

PREVENTING AND COMBATTING CYBERCRIME: KEY FINDINGS AND RECOMMENDATIONS FOR TÜRKİYE

Strengthening the Criminal Justice System and the Capacity of Justice Professionals on Prevention of European Convention on Human Rights Violations in Türkiye

European Union – Council of Europe Joint Project

PREVENTING AND COMBATTING CYBERCRIME:
KEY FINDINGS AND RECOMMENDATIONS FOR TÜRKİYE

Prepared by
- Esther George
- Dr. Michael Jameison
- Kemal Kumkumoğlu

This Report is prepared under the Joint Project on Strengthening the Criminal Justice System and the Capacity of Justice Professionals on Prevention of the European Convention on Human Rights Violations in Turkey. The Project is co-funded by the European Union and the Council of Europe and implemented by the Council of Europe. The final beneficiaries of the project are the Ministry of Justice of the Republic of Türkiye, the Directorate General for Criminal Affairs, and the Justice Academy of Türkiye. The Central Finance and Contracts Unit is the Contracting Authority of this Project.

This Report was produced with the financial support of the European Union and the Council of Europe. The views expressed herein can in no way be taken to reflect the official opinion of either party. The views and opinions in this Report are the sole responsibility of the authors.

Design
Bilge Bostan

Printing
Tam Pozitif Reklamcılık | Matbaa
Çamlıca Mahallesi Anadolu Bulvarı
145. Sokak 10/11
Yenimahalle/ANKARA
Tel: 0312 397 00 31 | Faks: 0312 397 86 12
E-mail: pozitif@pozitifmatbaa.com

Project Stakeholders
- Constitutional Court
- Court of Cassation
- Council of Judges and Prosecutors
- Union of Turkish Bar Associations
- Financial Crimes Investigation Board (MASAK)
- Gendarmerie General Command
- Directorate General of Security
  - Department of Cybercrime
  - Department of Counter Terrorism
  - Department of Anti-Smuggling and Organized Crime
- Information and Communication Technologies Authority
- Council of Forensic Medicine

www.coe.int/tr/web/ankara
Council of Europe Programme Office in Ankara

✉ cas.ankara@coe.int
Ceza Adalet Sisteminin Güçlendirilmesi Projesi
cas_projesi
@project_cas
Ceza Adalet Sisteminin Güçlendirilmesi Projesi

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Context

Cybercrime is one of the fastest growing crimes in the world today. It is silent and deadly and affects individuals, companies and government infrastructure. It is not only about financial fraud and data loss, but also targeted criminal activity such as cyber-bullying, loss of personal data amongst others. It is not restricted to any one country, as cybercrime is carried out across borders, hence cooperation and collaborative international and national strategies are required more than ever.

In an effort to ascertain the challenges that Türkiye faced in the field of criminal justice, including with respect to cybercrime, the Council of Europe facilitated a Needs Assessment at the onset of the European Union – Council of Europe 'Joint Project on Strengthening the Criminal Justice System and the Capacity of Justice Professionals on Prevention of the European Convention on Human Rights Violations in Turkey' (Joint Project), a programme which aims to further strengthen and make the Turkish judiciary more efficient, effective and visible by ensuring its compliance with the international and European standards in the field of criminal justice.

Important recommendations of the ensuing Needs Assessment Report revolved around the need to further strengthen coordination amongst authorities involved in the investigation and prosecution of cybercrime, and in particular:

- To encourage the Turkish National Police and the Gendarmerie units dealing with cybercrime to share their experience in this field (§266);

- To consider establishing a centralised filing system for investigations of cybercrimes in different jurisdictions within the country (§268);

- To consider establishing dedicated prosecutorial departments or units within the public prosecution offices to deal solely with cybercrime cases (§274); and

- To implement guidelines and templates in order to enable faster communication between services, including requests for international exchanges from the Ministry of Justice to prosecutors (§291).

Accordingly, eight coordination meetings were held in partnership the Ministry of Justice of Türkiye to gauge the challenges faced and determine how better coordination and co-operation could be established and/or improved among the competent authorities in the investigation and prosecution of cybercrimes. The events were held in the following locations on the following dates:

- Ankara - 25th- 26th October 2021,
- Istanbul - 16th-17th December 2021,
- Izmir - 10th-11th February 2022,
- Adana - 24th-25th February 2022,
- Antalya - 17th-18th March 2022,
- Samsun - 7th-8th September 2022,
- Diyarbakir - 23rd-24th November 2022,
- Konya - 10th-11th January 2023.

The present report consolidates policy briefs made by the authors, Esther George (former Prosecutor in the UK), Kemal Kumkumoglu (Lawyer in Türkiye) and Mick Jameison (former Law Enforcement Officer in the UK), in an effort to review and summarise main recommendations formulated by law enforcement officers, forensic specialists, IT specialists, prosecutors, members of the judiciary, and representatives of the banking sector, at the occasion of those eight coordination meetings convened as part of the Joint Project. Other sources of material are notes from Dr Burcu Baytemir Kontacı.

It is hoped that this report could be used as the first step to Türkiye developing an overarching strategy to combat cybercrime. It is viewed as a long-term strategy which should identify different phases for implementation and ensure that it resourced appropriately. The challenge of combatting cybercrime requires a wide range of responses, for example, training, cooperation (nationally, regionally and internationally), exchange of information, public awareness, reporting, appropriate legislation and deterrent sentences. As Türkiye is a signatory to the Council of Europe Convention on Cybercrime ('Budapest Convention'), the country has access to capacity building resources which will help towards devising a dynamic and sustainable strategy to combat cybercrime in all its elements.

A. BACKGROUND

Findings

The primary hurdle in fighting cybercrime lies in identifying and capturing the culprits behind these digital offences. Cybercriminals frequently operate from different jurisdictions, often leveraging anonymity or pseudo-anonymity to avoid being traced. Additionally, there are significant obstacles in conducting international investigations and fostering collaboration. Another major issue is the underreporting of cybercrime incidents by both individuals and large corporations. In relation to ransomware cases, the 'ransom' is usually paid to avoid further complications and repercussions such as loss of trust in the company to secure personal data.

It is recognised that the methods used by law enforcement agencies are often ineffective due to the fast-changing landscape of technology. This is hampered by lack of timely cooperation by external agencies such as banks and even forensic departments. Furthermore, cybercriminals can resort to new cutting-edge technology to facilitate their criminal activity while law enforcement struggles to keep up in terms of resourcing and training.

It was found that the Prosecution and the Judiciary both faced many challenges in this sphere such as technical complexity, and high workloads relating to cybercrime and electronic evidence which continue to grow in volume and sophistication. There was a consummate failure by private businesses, banks, and service providers to respond in a timely manner to requests for information which in turn had a detrimental knock-on effect on cases.

An assessment of the challenges facing digital forensics a major issue was the workload, that is the quantity of devices requiring analysis (rather than the quality of the examination) and the lack of direction given to forensic examinators due to a lack of technical understanding by prosecutors. Exhibit submission and exhibit handling were also a problem in how they were dealt with and sent to the lab.

Selected recommendations

There were many recommendations arising out of the eight coordination meetings, as detailed in the body of this report, as well as in the concluding chapter. The most important recommendations are as follows:

- Creation of a National Cyber Crime Unit (NCCU).
- Promotion of best practice in cybercrime investigations and handling and submission of electronic evidence.
- Creation of a Unit dedicated to fighting online abuse against children.
- Creation of an online national reporting centre for cybercrime.
- Implementation of a holistic training strategy, including staff retention plans, by law enforcement authorities.

• Establishment of a screening system through a collaborative agreement between prosecution services and the police, so that crimes that are unlikely to be solved or are of so little financial loss to be a viable investigation, will be screened out and not investigated.

• Implementing the recommendations of iPROCEEDS document titled, Interagency Cooperation Protocol.

• Rolling out of crime prevention and awareness campaigns in schools and for the general public.

• Creation of dedicated departments for the prevention of cybercrime at national and local levels.

• Dissemination of information about the role of 24/7 Single Point of Contact and communication information to share ways to reach the contact point.

• Delivery of specialised training to judges, prosecutors, and law enforcement officers.

• Development of a strategy for providing support and resources to victims of cybercrime.

• Addressing the gaps in legislation such as criminal procedural provisions related to gathering of electronic evidence and power of jurisdiction.

• Establishing new crimes such as cyber grooming and ransomware.

• Regulating an umbrella cybersecurity legislation and reforming the data protection provisions related to law enforcement activities.

• Transposing the 2nd Protocol of the Budapest Convention.

1. Stakeholders and Other Information

Representatives from various institutions participated in the meetings held in 8 provinces. These are, respectively:

Representatives From Judiciary Authorities,
- Court Of First Instance Judges
- Regional Courts of Appeal
- Regional Administrative Court
- Public Prosecutors

Representatives From Public Authorities,
- Banking Regulation and Supervision Agency
- Council of Forensic Medicine
- Information And Communication Technologies Authority,
- MASAK (Mali Suçlar Araştırma Kurulu)
- Ministry Of Justice

Representatives From Bar Associations,

- Izmir Bar Association
- Adana Bar Association
- Antalya Bar Association,
- Samsun Bar Association,
- Union Of Turkish Bar Associations

Representatives From Police and Provincial Gendarmerie Command Department,

- Adana Provincial Police Directorate
- Antalya Provincial Police Directorate,
- Antalya Provincial Gendarmerie Command,
- Diyarbakır Provincial Security Directorate,
- Diyarbakır Provincial Gendarmerie Command
- Konya Provincial Security Directorate,
- Konya Provincial Gendarmerie Command,
- Samsun Provincial Security Directorate,
- Samsun Provincial Gendarmerie Command

Representatives From Other Associations,

- Turkish Penal Law Association
- Computer Forensics and IT Law Association
- The Banks Association of Türkiye
- International Children's Centre and Centre of Children Rights
- IT Law Association

B. FINDINGS

1. Impact of Cybercrime in Türkiye

a. Brief overview of the growing threat of cybercrime

As the world becomes more interconnected through the internet, cybercrime has become a major concern for individuals and organisations alike.

Cybercrime continues to be a growing threat, to not only individuals but also to businesses, and government agencies of all shapes and sizes, across all countries and sectors. It is the fastest-growing crime in the world and organisations and individuals are facing even more cyberattacks than before. Criminals are increasingly moving their operations to the Internet since that is where the money is. The reasons for cybercrime's appeal are simple to comprehend as it is essentially a low-risk crime with extremely big payoffs. Cybercriminals may make large financial gains without the fear of being caught. This is due partly to the reluctance of companies to report cybercrimes such as ransomware because of public repercussions and risk reputation. It is also because criminals are growing more adept at working across global networks, they have access to and develop technologies to aid them. Furthermore, because cybercriminals have access to secure and pseudo-anonymous payment systems, it makes it a lot harder to catch them.

The concepts of cybercrime and cyber-enabled crime are both subsets of crimes involving technology, but there are key differences between the two.

Cybercrime refers to offences that are committed directly against computers and computer networks. This type of offence can only be committed with the use of information technology. Examples include spreading computer malware, offences against networks, computers, program or data; offences against the confidentiality, integrity and availability of computer data and systems.

On the other hand, cyber-enabled crime involves instances where the computer serves as an instrument to facilitate traditional crimes. For instance, fraud, a crime that predates computers, falls into this category when it's committed using digital technology. This category also covers offences linked to intellectual property rights and similar rights, along with the criminal use of the internet to perpetrate conventional crimes, such as computer-related forgery and the distribution of child sexual abuse material among others.

The growing threat of cybercrime in Türkiye is a major concern for both individuals and businesses. One of the subtopics that can be explored in this area is the different types of cybercrime prevalent in the country. Phishing, ransomware attacks, identity theft, and data breaches are some of the most common types of cybercrime encountered in Türkiye.

Phishing involves fraudulent attempts to obtain sensitive information such as usernames, passwords, and credit card details. This type of cybercrime often takes the form of fake emails or websites that appear to be legitimate.

Ransomware attacks are another type of cybercrime that has become increasingly prevalent in recent years. These attacks involve malicious software that encrypts a victim's files and computer hard drives, before making demands for payment in exchange for their release.

Identity theft is also a significant problem in Türkiye's cyberspace. Criminals may use stolen personal information to open bank accounts or make purchases without the victim's knowledge.

Finally, data breaches can occur when sensitive information stored by organisations is accessed by unauthorised individuals. This can lead to financial losses for businesses and pose a risk to individuals' privacy.

Cyberattacks have impacted the economy by causing financial losses to companies. The impact of cybercrime on businesses can be severe as companies may lose their customers' trust and reputation due to data breaches. The damage caused by cyberattacks can be extensive, leading to significant financial losses and even bankruptcy in some cases. Cybercriminals are continuously evolving their methods, making it increasingly difficult for companies to protect themselves from these attacks. Businesses and government agencies face more severe consequences as a successful cyber-attack can result in the loss of sensitive data, intellectual property, and financial information. The costs associated with these types of attacks can be astronomical and have long-lasting effects on the organisation's ability to operate effectively. Additionally, it can lead to a loss of trust from customers and stakeholders which may take years to regain.

Cybercriminals, like all criminals, strive to communicate with and learn from one another. Criminal forums, markets, group chats, and even Facebook pages serve as breeding grounds for this underground economy, allowing threat actors to adapt strategies to their specific contexts and targets all around the world. For example, during covid in the United Kingdom scammers were attempting to hijack personal tax accounts in order to conduct tax fraud.

The increasing use of mobile devices has also led to an uptick in mobile-related cybercrime, including malicious apps and phishing attacks targeting smartphone users. As these trends show, the threat of cybercrime is constantly evolving and becoming more sophisticated, making it essential for individuals and organisations alike to stay vigilant against potential threats.

b. Importance of developing an effective strategy to combat cybercrime

In Türkiye, *cybersecurity* incidents are reported and handled by the national CERT and do not routinely involve law enforcement. Cybersecurity incidents are events that may indicate that an organisation's systems or data have been compromised or measures that have been put in place to protect them have failed. The reports are typically classified against a cybersecurity taxonomy.

The role of CERT and the combatting of cybersecurity in Türkiye is strengthend by the National Cyber Security Strategy and Action Plan (2020-2023).[1]

Cybercrime matters are criminal activities that are contrary to the national legal framework and these reporting systems are classified accordingly. Full reporting and investigation mechanisms for cybercrime are generally managed by prosecutors and law enforcement. The National Security Strategy and Action Plan has limited commentary about cybercrime, indicating improvements in capacity, international information sharing and international partnerships being important. Beyond this, there are limited points to put in place action plans to confront cybercrime.

It is imperative that Türkiye develops and implements an overarching effective strategy (encompassing national, regional and international aspects) to combat cybercrime, as this is one crime that is growing exponentially especially as new

[1] https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf

technologies emerge and are further developed. It is highly sophisticated, exploits vulnerabilities on a large scale using innovative tactics and the situation is not likely to improve in the short to medium term. This is the digital age and everything from our personal data through to how we conduct our lives on social media is there for exploitation by cybercriminals.

The biggest challenge in combating cybercrime is tracking down and apprehending those responsible for committing crimes in cyberspace. When cybercrime is reported the traditional methods used by law enforcement agencies to investigate are often ineffective in this evolving digital landscape, making it difficult to bring cybercriminals to justice. To combat this issue, law enforcement agencies need to and are adopting new strategies, tactics, and tools to help track down and prosecute those who commit cybercrimes.

One such strategy is the creation of specialised units within police departments that focus solely on investigating cybercrimes. These units are staffed with officers who have specialised training in digital forensics and other relevant areas.

Another strategy is the growth of international cooperation between law enforcement agencies. Cybercrime knows no borders, so it’s essential that countries work together to track down criminals who may be operating outside their jurisdiction. Cross-border cooperation and information sharing among law enforcement agencies is a critical aspect of effective cybercrime strategies.

One international example of this is the European Union’s “Joint Cybercrime Action Taskforce” (J-CAT), which brings together law enforcement agencies from across Europe to share intelligence, coordinate operations, and target cybercriminals. J-CAT has been successful in disrupting numerous criminal networks involved in activities such as online fraud, malware distribution, and hacking.

Another example is the “Five Eyes” alliance between Australia, Canada, New Zealand, the United Kingdom, and the United States which allows for the sharing of intelligence on cyber threats and for member countries to collaborate on investigations and prosecutions.

The International Criminal Police Organization (INTERPOL) also plays a crucial role in facilitating cross-border cooperation on cybercrime. Through its Global Complex for Innovation (IGCI), INTERPOL provides training and support to law enforcement agencies around the world and facilitates joint investigations into complex cybercrimes.

Türkiye has ratified the Council of Europe Convention on Cybercrime (Budapest Convention) which means that they have access to capacity building, international co-operation, and procedural law tools which will enhance their approach to combatting cybercrime.

Türkiye should consider signing and ratifying the Second Additional Protocol to the Budapest Convention, which provides additional and expedited tools for enhanced co-operation and disclosure of electronic evidence, such as direct co-operation with service providers across borders or co-operation in emergency situations.

Cross-border cooperation and information sharing among law enforcement agencies are essential components of effective cybercrime strategies. Public-private partnerships and collaboration have been identified as key components of effective cybercrime strategies in various countries around the world.

The eight workshops held across Türkiye highlighted that the effort to combat cybercrime had to be a 'team effort' both nationally, regionally and internationally. That it is about co-operation between national, regional and international agencies; training (in all areas); mutual assistance between banks, investigators and prosecutors; public awareness; risks and compliance; cyberethics; education in schools involving both parents, carers and children; reporting; and the quality of the evidence collected.

A well thought out long term overarching strategy encompassing these areas will assist Türkiye in their fight against cybercrime. The strategy has to be well resourced with implementation phases and continuous review. It has to keep up with the growth of the evolving technologies and ways in which to counter them.

2. Legislation

The deficiencies in the current legal framework regarding cybercrime and the resulting challenges were widely accepted by participants of the workshops. When domestic and international legislation is considered together, the main provisions that can be relied upon for combating cybercrime are the provisions related to cybercrimes in the Turkish Penal Code. These include offences such as;

- Unauthorised Access to the Information System (Article 243),

- Hindering, Damaging, Rendering Inaccessible, Destroying or Altering Data (Article 244),

- Misuse of Bank or Credit Cards (Article 245), Using prohibited devices or programs (Article 245/a),

- The Law on Regulation of Publications on the Internet and Combating Crimes Committed through These Publications (Law No. 5651),

- The Law on Protection of Personal Data (Law No. 6698), the National Cybersecurity Strategy and Action Plan prepared by the Turkish Presidency Digital Transformation Office,

- The Council of Europe Convention on Cybercrime (Budapest Convention) includes provisions referring to cybercrime.

It was discussed during the workshops that both law enforcement personnel, judges and prosecutors are not sufficiently familiar with the existing legal framework regarding cybercrime. This combined with a lack of technical understanding demonstrate some of the reasons laws and regulations related to cybercrime is not implemented in some cases. Many officials, described their general lack of knowledge on these matters and their dissatisfaction with the current situation.

In principle, investigations and prosecutions are generally conducted solely within the framework of the Turkish Penal Code and the Code of Criminal Procedure. During the workshops it was apparent that several law enforcement personnel, judges, and prosecutors were not even aware of the Budapest Convention on Cybercrime. They also stated that they do not have a resource to rely on in their investigations regarding the reports and complaints they encounter.

Furthermore, the fact that almost all traditional crimes can be committed through information technology increases the workload of specialised law enforcement officers, judges, and prosecutors. It requires the implementation of special procedures regarding cybercrimes in the investigation and prosecution stages, especially in the collection and evaluation of evidence. In terms of the investigations conducted regarding cybercrimes, it is observed that the key point in these special procedures is "speed". In this regard, a specific example is the offence of "Fraud committed through the use of information systems, banks, or credit institutions" regulated as an aggravated form of fraud. Indeed, the offence of fraud, which is a traditional crime, transforms into cybercrime in this form. Almost all shreds of evidence could have the risk of disappearing from the moment of identifying the perpetrator to the collection of evidence.

The lack of a comprehensive and explanatory independent regulation on cybercrime, the inadequacy of the current legislation in force, the fact that almost all crimes can now be committed through information technology, the inability to determine the location of the crime and correlatively the conflicts of jurisdiction arising between judicial authorities, the difficulty and even impossibility of accessing electronic evidence over time, and the low level of digital literacy in law enforcement personnel and judiciary are the main problems on cybercrime landscape.

c. Determining the competent authority of jurisdiction in cybercrimes

During the coordination meetings especially prosecutors and judges stated that, due to jurisdictional conflicts, investigations are excessively prolonged, evidence is lost and therefore investigations remain inconclusive. At this point It is considered that an amendment should be made to the Article 12 of the Code of Criminal Procedure regulating jurisdiction. Although the sixth paragraph of the mentioned article clearly establishes the jurisdiction of the courts of the domicile of the victim in crimes committed by using information systems, debit or credit institutions or debit or credit cards as a means, it has been stated that this regulation is insufficient.

Indeed, a participant from the Higher Judiciary also cited one of the examples where this situation emerged as the files in which there is a low amount of damage for each victim with a large number of victims. It is evident that criminals especially design this strategy to block the investigation processes.

The circulation of the files between the prosecutor’s offices in different regions and the courts due to lack of jurisdiction hinders the collection of critical evidence. Therefore, at the end of the day there is no substantial evidence that can be collected at the prosecution stage except for witness statements.

Since the issue of jurisdiction interferes with the “collection of evidence”, which is one of the most important procedures in the investigation and prosecution stages of crimes, for the effectiveness of investigations, it is necessary to clarify the issue of jurisdiction. In this sense, it may be advised to impose a regulation pointing an exact place of jurisdiction for cybercrimes.

d. Introducing more comprehensive regulation for the collection, packaging, preservation, transportation, and examination of electronic evidence

Electronic evidence is not suitable for collection and examination as of the moment it is detected. On the other side, its analysis requires additional time, labour, and expertise. It has been stated that the collection and examination of this evidence require special care due to its sensitive, easily falsifiable, and completely destructible nature.

Due to the perishability of electronic evidence, the utmost care and diligence must be exercised from the first contact with this evidence until it is presented to the prosecutor’s office or the court.

The lack of a guide on how to collect, preserve and transfer electronic evidence is a major deficiency. Indeed, electronic evidence plays a key role in the investigation of cybercrimes. The fact that this evidence, which is already highly vulnerable to damage, becomes useless due to the actions of law enforcement personnel at the stage of collection. The preservation of the integrity and validity of an electronic evidence that is subjected to wrong persons and wrong transactions at the moment of its first acquisition carries a great risk. It causes questions in the later stages of the proceedings due to the lack of concrete evidence and therefore, it has a profound impact on the fate of investigations and prosecutions.

Since there is no comprehensive legislative regulation on this issue, the process is carried out at the initiative of the law enforcement personnel who will collect electronic evidence. A regulation to be issued should clearly stipulate the general principles and mandatory procedures to be followed during the collection of electronic evidence, how the law enforcement personnel who will collect the evidence should act, and that transactions against the regulation will be considered as violations and criminal proceedings will be taken in this regard.

In this context, some of the procedures to be carried out during the collection of electronic evidence can be advised as follows.

- Attentive and separate packaging of electronic evidence,
- Creating a chain of custody, chronological report of the documentation process of electronic evidence,
- Live analysis of collected electronic devices,
- Noting down the passwords and patterns of the electronic devices before turning off for the transfer,
- Shadow copying of the digital material in the electronic device,
- Collection of hashing algorithms (Cryptographic hash function) to preserve the data integrity of the electronic evidence,
- Time Stamping.

Currently, Article 134 of the Turkish Criminal Procedure Code regulates the protection measure of Search, Copying and Seizure of Computers, Computer Programs and Stores. It is essential for the regulation explaining the processes of collecting electronic evidence to be regulated in harmony with the relevant provision of the law. In addition, whether electronic evidence or not; the principles that must be followed in all kinds of evidence-collection procedures will also apply here. Indeed, a mistake made during the collection of evidence collected at the crime scene renders the evidence unlawful and consequently prevents the evidence from being the basis of the proceedings and the verdict. The same Article should be also amended, especially with regard to the delivery of files containing images of child pornography to the suspect or defendant.

During the coordination meetings, a discussion was also held between forensic experts and judges and prosecutors regarding the correspondence concerning the examination of electronic evidence. The main problems were identified as the fact that the letters written to the Council of Forensic Medicine regarding the examination of electronic evidence contain very general requests, the issues to be investigated are not specific, the evidence sent to be examined is sent without being selected, and hence, there is a loss of time during the sorting of information and personal data that are not related to the crime.

e. The responsibility of banks regarding the fulfillment of letters sent in the investigation and prosecution stages of cybercrimes

During the coordination meetings, the negative effects of the communication traffic between banks and law enforcement, judges and prosecutors on the collection of evidence and the prevention of damages arising from the crime were frequently mentioned. Cooperation between banks and judicial authorities is of great importance, especially in fraud crimes committed through information technology. It is clear how important the responses from the banks are for the fate of the investigation and prosecution, and even the continuation of the investigations depends on the responses from the banks. Accordingly, the importance of "rapid response" is emphasised.

The problem of rapid response in the investigation and prosecution of fraud crimes committed using information systems is the main problem between banks and judicial authorities. There is already a loss of time before notifications and complaints are received by the judicial authorities. In addition to this loss of time, the delay in the responses to the letters of inquiry written to the banks after the opening of the investigation on the complaints causes the evidence from the banks not to be obtained because of the extermination of the records.

One of the most prominent examples of this situation is the fact that the security camera recordings of ATMs are kept for a short period of time, such as 6 months, and destroyed at the end of this period. In such cases, it becomes impossible to obtain evidence from the security camera records of the banks where the bank accounts used to commit crime are located, and to identify the perpetrators of the crime through these images.

Likewise, the short-term preservation of records of account statements causes similar problems. While it is possible to identify money transfers by examining account transcripts, the procedure it takes to access these transcripts can be time-consuming. In fact, during the coordination meetings, some participants from the judiciary explicitly stated that they had given up hope of such evidence during the investigation and prosecution phases.

Another issue as important as the problems of speed and time in obtaining evidence from banks was the process of blocking of the bank accounts. Since it takes a long time for judicial authorities and banks to communicate for the requests for account blocking, it was argued that victims should be made aware of this issue and take action primarily. It was also stated that the account holder should notify a suspicious transaction as quickly as possible, since the amount from the victim's account is withdrawn very quickly.

Unless account blocking is done quickly, the money seized by fraud is transferred to different accounts and withdrawn. Correspondingly, it becomes almost impossible to recover money that is no longer available in the bank account and enters physical circulation.

Even though the money subject to the crime has not yet been withdrawn, it is transferred between different banks, and it becomes very difficult to trace these transfers. Indeed, if it is seen in the warrant responses obtained from each bank that transfers have been made to different accounts, a new warrant will have to be written to the bank from which the transfer was made. All this prolongs the processes and will cause the grievance to remain unresolved. Accordingly, it may be advisable to establish a central umbrella organisation for interbank money flows.

It is important to ensure that bank accounts are blocked quickly and that letters to banks are responded to in the same manner. The example of the UK is important with regard to issues such as the lack of timely responses to letters to the banks and the long period after which blocking requests are made. Indeed, it is a major deficiency that no sanction is envisaged for the delay in the return from the banks to the judicial authorities.

Therefore, the use of production orders that are served on banks is recommended. According to this procedure, law enforcement or the judicial authority signs an order that is electronically sent to the bank or an institution and gives them a time period for a full reply. If the bank or the relevant institution fails to adhere to the order, an order instructing a representative from the bank to appear before the authorities is issued.

There is a clear need to improve the time taken for institutions to respond to legal requests and it is highly recommended to implement a legal framework with sanctions to enhance the time taken in investigations.

f. Defining ransomware as a criminal offence

The use of ransomware should be defined as newly introduced cybercrime.

Ransomware attack is a crime that occurs because of attacking computer systems, where access to the compromised system is blocked, and ransom is demanded from the victim users for the removal of this block. It is discussed that ransomware attacks are one of the most common methods in the field of cybercrime in Europe, similar to the one in Türkiye, and that most ransomware attacks are carried out by clicking on a link sent via an e-mail. It is evident that this latest crime is often cannot be detected or classified.

The victims of this crime, especially the companies pay the ransom, while others choose to update their computer systems. Although this is such a recent phenomenon, such attacks are considered commonplace today. Due to weak policies, system setups and lack of protection shields, companies face the challenge of making difficult decisions, while individuals are willing to pay ransoms to retrieve their various documents. Therefore, victims of ransomware do not generally report or file complaints to law enforcement or judicial authorities due to this crime. They tend to perceive it as a virus attack and seek solutions on their own. In addition, during the coordination meetings, it was stated by the forensic experts that ransomware is very diverse. The intervention in this crime requires special expertise.

It is of great importance to define ransomware as a brand-new crime within the scope of criminal laws and provide appropriate sanctions. This crime distinguishes itself from other existing cybercrimes with its specific actions and requires more severe punishment. Following the establishment of this crime, the necessity of using an international cooperation network should be emphasised for the investigation and prosecution stages. Ransomware is a crime that can be committed internationally, making international cooperation crucial in combating this crime. Indeed, this crime can be committed through an email or message sent over the Internet from anywhere in the world, and in scenarios where the perpetrator is in a foreign country and the victim is in another country, the investigation and prosecution of the crime become significantly more challenging.

g. Defining cyber grooming as a criminal offence

Online grooming of children (cyber servitude / online abuse) should be defined as a newly introduced cybercrime.

Cyber grooming has become more prevalent due to the use of information systems in the commission of traditional exploitation crimes, as well as the ease with which perpetrators can reach victims through these systems. This crime, particularly targeting children, has become widespread. By definition, cyber grooming is the act of an adult building an online relationship with a child or adolescent with mostly the intention of sexually exploiting or abusing them. However, it would not be accurate to limit this to sexual exploitation. The victim can be groomed in various ways. For example, in the computer game called "Blue Whale Challenge," victims were encouraged to harm themselves or even commit suicide.

In various countries, although cyber grooming may not be classified as a separate offence, it is regulated under crimes against sexual integrity. For example, in the United Kingdom, the offence of grooming is covered under the Sexual Offences Act 2003, which addresses various sexual offences, including those committed through online platforms. Similarly, in France, cyber grooming is addressed under the French Penal Code's provisions on sexual offences, particularly those related to the protection of minors and combating sexual violence.

In this context, it is strongly recommended that even if there are criminal provisions which foresee to penalize several related acts of cyber grooming, this new crime distinguishes itself from other cybercrimes and the offence of cyber grooming be included in criminal laws as an aggravated and qualified form of existing offences related to exploitation. In fact, the Lanzarote Convention also emphasises the need to address and combat cyber grooming.

h. Necessity to introduce new regulations

Data Protection regulation and current cybersecurity related legislation do not provide sufficient legal basis for combatting cybercrime. There is lack of legal basis for law enforcement data processing activities, and current legal framework related to cybersecurity is scattered, also far from being compulsory and effective in practice. Parallel to these, critical evidence of cyber incidents is in danger of being completely kept at dark out, data collecting practices of law enforcement authorities being considered unlawful due to lack of legal grounds and adequate safeguards.

Therefore, it was recommended that legal regulations and an umbrella cybersecurity legislation should be prepared to require the reporting of cyber incidents in the public and private sectors. Plus, a complete regulation that provides the legal basis for combating cybercrime in a manner that respects fundamental rights by regulating the legislation on the processing of personal data in public and law enforcement activities, is needed.

3. Law Enforcement

The comments and discussions in paragraph three are based on the discussions of participants at the workshops. Some commentary is added by the International Experts demonstrating the potential value of implementing any recommendation based on their experience with working in other countries in Europe and elsewhere. Where such comments are made, they are indicated in the footnotes.

a. Creation of a National Cyber Crime Unit (NCCU)

Currently the Cybercrime Department of the Turkish National Police (TNP) investigates cybercrime offences and/or provides forensic expertise in supporting other agencies in the Police and Prosecution in matters where technology is a significant factor to a crime or related evidence.[2]

The Cybercrime Department of the TNP also contains the 24/7 Single Point of Contact (24/7 SPOC) relating to data communication requests with international and national service providers.

During the coordination meetings there was consensus of the need to create a national unit to lead in the fight against cybercrime. Such a lead should not be limited to investigations and digital forensics in support of criminal prosecutions, but be expanded to lead in other important areas such as;

- Investigation of the most serious and significant cybercrimes,
- Disruption and dismantlement of cybercriminal infrastructure,
- Prevent and combat the underground economy working impacting upon Türkiye,
- Working in collaboration with Gendarmerie, regional and local policing cybercrime units in country,
- Working in partnership with stakeholders such as TR-CERT *(Ulusal Siber Olaylara Müdahale Merkezi (USOM))*, universities and others,
- Prevention of cybercrime,
- Awareness campaigns to reduce cybercrime, online bullying, and similar matters,
- Information security industry relationships,
- Technical expertise,

[2] https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/turkey/pop_up#:~:text=The%20National%20Cybercrime%20Department%20of,a%20crime%20or%20related%20evidence.

- Intelligence management and intelligence sharing with stakeholders about cybercrime,

- International relationships,

- Specialist investigative skills (such as Covert Investigation into criminal forums on Dark Web and crypto currency investigations,

- 24/7 SPOC,

- Promotion of good practice in cybercrime investigations and handling of electronic evidence.

The creation of a NCCU would further align Türkiye with many other countries in Europe insofar that this dedicated unit should have an independent structure focussed upon national issues relating to cybercrime and electronic evidence, whilst conducting significant criminal investigations and collaborating with the many partners now working to reduce the impact of technology enabled crime[3].

The skills employed in many NCCU's are not limited just to those with Police powers, but added value is gathered through the employment of other technical and industry experts.

b. Creation of a unit dedicated to online abuse against children

The issues relating to the initial reporting by children, who had been subject of online sexual abuse was raised by a number of parties that attended the coordination meetings. At one meeting a representative from the International Child Centre (from Ankara) identified that the current reporting system did not support the reporting of physical or online sexual abuse of children as there were no sensitive or discreet reporting methodologies in place.

Conversations in the meetings identified that other European countries employed dedicated websites for reporting physical and sexual exploitation of children and authorities were prepared to receive reports from child charities and support organisations, who supported young victims.

The use of video statements made by children in these investigations was also discussed, which would reduce the need for children to repeatedly give evidence about these traumatic incidents.

The discussions that took place identified that many of the agreements made by Türkiye in its signature of the Council of Europe Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse[4] (effective in Türkiye 1st April 2012[5]) were either not in place or not being implemented

[3] This paragraph is a comment made by the international expert(s)

[4] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168046e1de

[5] https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=201

during the investigation or the courts hearings for these types of offences when they occurred in the online environment.

It was identified that protection of children could be enhanced through engagement with Social Media service providers in Türkiye. Other comments indicated a lack of a comprehensive strategy to deal with child abuse and bullying matters for young persons in the online environment.

Some delegates proposed a more structured awareness campaign throughout the country in relation to online sexual abuse and bullying of children. Albeit the TNP and Gendarmerie provided successful case studies delivered through local prevention campaigns that had been successful in schools to prevent bullying, sextortion and circulation of self-generated sexual images of children.

The creation of a National Child Exploitation and Online Protection Unit (or similar) could improve the current situation. Such a unit should be created and tasked with the implementation of many of these reported shortcomings. Such a unit should provide the following, in addition to the comments above[6];

- A specialist online facility for children to report online sexual abuse and bullying.

- Investigators specialising in the investigation of online child abuse, seeking to support and rescue victims and identify and prosecute offenders,

- Covert investigation skills aimed at investigation of online sexual abuse of children, identification and rescue of victims and identification of suspects operating in hidden services on the dark web,

- Provide current and relevant data to government about the threat of online sexual abuse of children in Türkiye, and strategic proposals to reduce the harm caused.

Any National Child Exploitation and Online Protection Unit (or similar) in Türkiye should have an independent structure and focus upon national issues relating to Online Child Sexual Abuse and Exploitation. Whilst the unit should be enabled to conduct significant criminal investigations, the resourcing of this unit will also need other skills outside those with police powers, such as trained counsellors and persons trained to conduct interviews of traumatised children.

c. Creation of an online national reporting centre for cybercrime

Discussions at all eight coordination workshops identified that there was a significant increase of reported cybercrime and technology enabled crime that was being handled by law enforcement agencies and prosecutors. Indications were given that reported cybercrime increased annually by 10-20% year-on-year from 2020. Many senior officers in charge of cybercrime units indicated that

[6] This paragraph is a comment made by the international expert(s)

increased staffing and resources was not matching the levels of workload. They identified that more efficient methods of crime reporting and investigation is necessary.

Prosecutors reported that cybercrime cases were often reported directly to their offices, which required a special meeting to receive the allegation. Such meetings often took place by appointment due to the workload of prosecutors and after the meeting the prosecutors were able to direct law enforcement agencies to preserve relevant electronic evidence. Such delays in the preservation and seizure of electronic evidence are known to hinder investigations.

Where matters were reported to Police, they had the capability to preserve data and could do this as soon as the matter is reported. Whilst this capability existed, it was implemented inconsistently (see paragraph 3d).

At one workshop a case study was presented by a judge that demonstrated how he had linked together other cases because a unique phone number was used by the offender. He explained how he had researched indices that were available to him and provided some good learning for the plenary. But the creation of a national reporting centre for cybercrime would see the implementation of a dedicated system to record information about the offenders in all reported matters in Türkiye. The analysis of this information and the fast time preservation of electronic evidence could be undertaken in a timely fashion and then transmitted to a cyber investigation unit and suitable prosecutor.

There are several examples of how to create national reporting centres for cybercrimes, and the benefits of creating one detailed within the publications by INTERPOL and Council of Europe called "Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence." [7][8]

d. Training and specialist skills

During all the coordination workshops it was identified that significant skill shortages existed within police and the judiciary. In the police it was identified that training was needed for front line police in the search and seizure of electronic evidence and at cybercrime units there were specialist skills needed to support them investigate more complex matters such as electronic evidence, malware, software, cryptocurrencies, and the dark web.

It was regularly discussed that training shortcomings in the investigation of cybercrime and the handling of electronic evidence existed throughout all the relevant public institutions. It was also described how resources in cybercrime (nationally and locally) had increased, but not enough to keep pace with the level of crimes being reported. Budgets and training of new staff caused various challenges. It was mentioned in all events that training was needed in crypto currency dark web investigation.

[7] https://www.interpol.int › content › download › file

[8] This paragraph is a comment made by the international expert(s)

Other challenges that were identified included staff changing roles and moving out of the cybercrime arena. This meant that the investment in training was lost, and new officers had to take their place, which meant further training and experiential learning became essential to maintain capabilities.

Whilst many important matters about the need for training were discussed, what was not raised was a meaningful training plan or roadmap to deliver sustainable capacity building. **It is recommended** that the law enforcement agencies implement a holistic training strategy and include staff retention plans within it. The Council of Europe (in partnership with Interpol) have published a Guide for Developing Law Enforcement Training Strategies on Cybercrime and Electronic Evidence.[9] This document explains, *"A well-developed strategic plan can play a pivotal role in responding to multi-layered, complicated problems such as cybercrime and electronic evidence. However, the mere existence of a strategic document is not enough: strategies are only useful when they become the part of organization's culture through continuous communication among its members and stakeholders. To be effective, strategies must also be rooted in – and respond to – the needs of the organization, which should be identified on the basis of broad-based consultations with relevant stakeholders."*

Any training strategy that is introduced in Türkiye should be targeted at officer's requirements at all roles, from patrol officers, detectives and cybercrime specialists.

There is already some training material provided by the Council of Europe through the online training platform dedicated to Human Rights Education for Legal Professionals ('HELP').

Registration for HELP is a simple activity at this URL https://help.elearning.ext.coe.int/login/index.php. Currently there are nine modules relating to cybercrime investigation, which have been translated to Turkish under the European Union – Council of Europe Joint Project on strengthening the criminal justice system in Türkiye, and would take ten hours to complete.[10]

Other training requirements included the provision of guidance for police officers who received a cybercrime report whilst on patrol or at the police station as infrequently basic steps were not being taken to preserve or seize electronic evidence, resulting in losses of opportunities to successfully prosecute offenders. In relation to this challenge, the Council of Europe have prepared and published a guideline, titled Guide for first responders to cybercrime investigations which is available upon request.[11]

[9] https://rm.coe.int/guide-for-developing-training-strategies-final/1680a62c72

[10] This paragraph is a comment made by the international expert(s)

[11] https://www.coe.int/en/web/octopus/training#{%2264860563%22:[5]}

To support Türkiye further the iPROCEEDS-2 project provided a two-day online presentation in January 2022 explaining the guideline to over 100 participants. **It is recommended** that Türkiye continue to roll out this training to front line police officers and investigators using this guide as a template[12].

e. High workload

The workshops consistently identified high workloads relating to cybercrime and electronic evidence, which are continually growing in volume and sophistication. It was commented that insufficient resources are being implemented to meet these demands. Often Police and Prosecutors indicated that they needed more staff, resources, capabilities, and training.

Other parallel discussion points were the time that it took to conduct cybercrime investigations, with invariable internal frictions. The Prosecutors have an incredible workload, and in seeking to solve cases they send high numbers of requests and directives to the Law Enforcement Agencies and other third parties. The Law Enforcement Agencies also have high demands on their resources and try to respond as quickly as practicably to crime allegations and requests from Prosecutors. To undertake these investigations, they send requests for information to third parties, such as banks, ISP's, telecoms companies and alike. These third parties tend not to have dedicated units to respond to the requests from Law Enforcement officers (and Prosecutors), which results in further delays. Consequently, cases, which theoretically could be completed in months, are often taking years to finalise.

Whilst Türkiye is a very developed country and a member of G20[13], any introduction of additional resources comes at a cost to the Government and in turn the taxpayers. Türkiye, like most other countries must effectively manage its resources and get significant results on the financial investments made in the public sector. To improve this current situation, efficiencies and effective management of the workload is needed and consideration of some difficult and challenging decisions is necessary.

The Council of Europe experts provided overview from an international perspective during the workshops that many cases of cybercrime are not solvable using traditional reactive investigative techniques. There are other factors such as minor cybercrimes which result in minimal losses have disproportionate resources put in place to solve them. **It is recommended** that a screening system is put in place through a collaborative agreement between the Prosecutors and Police so that crimes that are unlikely to be solved or are of so little financial loss to be a viable investigation will be screened out and not investigated[14].

[12] This paragraph is a comment made by the international expert(s)

[13] https://www.g20.org/en/about-g20/

[14] This paragraph is a comment made by the international expert(s)

Furthermore, **it is strongly advised** that where any screening decision is made, that the facts of each case are used for intelligence and statistical reporting, whether the cybercrime is screened out or fully investigated.

f. Inter-agency cooperation

Significant discussions and comments throughout all the workshops indicated that inter-agency cooperation needed review and improvement. This echoed several of the recommendations made in the Needs Assessment Report about coordination between different agencies involved in the investigation of cybercrime.

Participants in the workshops commented about poor information and intelligence sharing between TNP and the Gendarmerie. Other comments from participants raised similar shortfalls in communication between law enforcement officers and Prosecutors. These communications and cooperation did not appear to be intentional, but they indicated that there was too little communication regionally and nationally between stakeholders about cybercrime and electronic evidence. For example, many problems that were identified in the first workshops were repeated in the remaining seven. It appeared that there was no mechanism at a central point to collate these issues, identify solutions, and put remedies in place.

We are grateful to the Ministry of Justice that attended the workshops and used the discussions to put appropriate activities in place to deal with matters raised. Examples included the changes of banks retaining CCTV images for increased periods of time, steps to improve regulation of the issue of non-attributable mobile phones (potato lines), and the plans to change of legislation regarding the restoration of digital evidence after a forensic image is obtained (Article 134 Criminal Procedure Code).

Other activities relating to inter-agency cooperation in Türkiye have been conducted as far back as 3rd and 4th April 2017, when meetings were held with the stakeholders that included TNP cybercrime Units, financial investigation units, MASAK and prosecution services in relation to the search, seizure and confiscation of online crime proceeds. The document titled, Turkey Inter-agency Cooperation Protocol, which contains a series of recommendations and agreements were made then and appear just as relevant today. Details about the event can be found on the Council of Europe Cybercrime website[15]. The full document can be obtained from the iPROCEEDS-2 project in Bucharest upon request[16].

Some of the key conclusions and agreements are titled as follows;

- Cooperation during criminal investigations

[15] https://www.coe.int/en/web/cybercrime/-/iproceeds-workshops-on-inter-agency-and-international-cooperation-for-search-seizure-and-confiscation-of-online-crime-procee-1

[16] This paragraph is a comment made by the international expert(s)

- Domestic measures
- International measures
- Exchange of intelligence, information, and evidence
- Multi-agency groups
- Public-private sector cooperation
- International cooperation
- Statistics
- Recommendations for drafting protocols for interagency cooperation.

g. Developing proactive capabilities for cybercrime

The use of covert surveillance and other investigation techniques often described as special measures are a key area of law enforcement capabilities in the investigation of organised crime. The use of these measures, which include interception, undercover operatives, test purchases and surveillance in the online environment are necessary to complement the national response to cybercrime.

These techniques can be used to gather information and evidence about suspects and offending from other online resources such as criminal forums and chatrooms. Anyone involved in covert investigation (either on the Internet or in the real world) must always be appropriately trained, competent, and authorised. Consideration should be given to sourcing any equipment and associated services necessary for undertaking such an investigation in a covert and untraceable way. It should not be possible to track any of the equipment or services back to a law enforcement agency under any circumstances.

We recommend that covert activities are located centrally in a dedicated unit and work in support of investigations as necessary. There are many challenges when operating in a covert role, for example officers must adhere to appropriate and ethical standards. In gathering information, establishing and maintaining contact with the subject of the investigation they should act in accordance with any conditions set out in their initial deployment instructions.

Agents must:

- Be able to identify the legal limits to their actions (including to be able to recognise what constitutes participation in crime);
- Understand thoroughly the need to corroborate evidence;
- Consider the Human Rights implications of the subject and all other parties affected by the investigation.

By placing these officers in a central unit, their activities can be closely monitored by supervisors and managers. Dedicated standard operating procedures can be developed to meet necessary controls and oversight.

Covert investigators must always ensure that all material relevant to the investigation is retained and recorded in a durable and retrievable form. This may require the development of secure systems not normally available within the TNP or Gendarmerie[17].

h. Crime prevention and awareness

During the workshops, participants recognised the importance of crime prevention and awareness campaigns. In the face of so much cybercrime, there was a recognition that reliance on prosecution of cybercriminals alone is not likely to reduce the levels of offending. Some examples that were cited included,

- Activities should be introduced to prevent children becoming victims of cybercrime (and online abuse),

- Public information campaigns regarding people being duped into offending by acting as money mules or drop off points for illegal commodities,

- Awareness raising so victims know how to report cybercrimes.

The TNP and the Gendarmerie were able to provide case studies of prevention campaigns that they had conducted in the different regions in schools to prevent bullying, sextortion, and circulation of pornographic images of children. Whilst these would have made some impact, the lack of a cohesive strategic plan to reduce cybercrime is apparent.

The Turkish National Cyber-Security Strategy states, *"The establishment of a cyber security culture in all segments of society is one of the requirements of the age. The basis of this culture is based on providing a high level of awareness. When the importance of safe use of technology is embraced by all individuals, the negative effects of risks and threats on life will be reduced visibly.*

In this context, carrying out awareness-raising activities at individual, institutional and national scales, that is, throughout the society; Reaching all segments of society through activities for families, children, students, youth, women, the elderly and the disabled is among the priority targets. Awareness campaigns for the protection of children in cyberspace and activities to raise awareness of the responsibilities of families will also be activities of high importance in this context[18]."

Elsewhere the strategy adds, "It is necessary to continuously develop methods of combating cybercrime, and to carry out preventive, deterrent and effective studies. In this context, it is aimed to increase the national capacity and technological opportunities in this field in order to continue the fight against cybercrime more strongly in the 2020-2023 period[19]."

[17] This final two paragraphs are comments made by the international expert(s)

[18] https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf - page 24

[19] https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf - page 26

To deliver these strategic aims, **it is recommended that law enforcement should create a holistic cybercrime prevention plan** that includes how messages will be delivered at national and local levels. Such a plan should make the most effective use of resources, prevent duplication, and provide measurement of activities undertaken.

It is recommended that the creation of dedicated departments whose role is to concentrate on the prevention of cybercrime takes place, ideally at both national and local levels.

Many other countries have online resources providing information to the public about cybercrime and the ways to avoid being a victim. These are in addition to those public information messages created by national CERTS (such as TK-CERT). An example that was discussed in the workshops is a website in the U.K. called Get Safe Online (https://www.getsafeonline.org). **It is strongly recommended that the Turkish Government in collaboration with law enforcement create a similar resource** and keep it up to date in response to daily changes. Many other countries have found that direct engagement with personal from Get Safe Online has provided a good starting position and advice on the creation of similar national entities[20].

i. 24/7 Single Point of Contact

At every workshop the role of social media companies and the regular failure to provide requested information and evidence to Police was raised. Requests for information and evidence generally went unanswered when Police and Prosecutors made a request for matters relating to fraud and defamation cases. Generally, it was identified that the only area where social media companies did provide full and timely information was in child abuse and child sexual abuse material cases.

It was regularly explained to delegates that defamation and other similar types of offending were often caught between 'free speech' and civil law (rather than criminal law) in many countries outside of Türkiye. As such, there was no criminal framework in such countries to deal with defamation and other cases, which is the cornerstone of mutual legal assistance and reciprocity. As such any enquiries were bound to fail. There seemed to be widespread misunderstanding of this position and meaningful action is needed amongst the prosecutors and judiciary to clarify the position to prevent requests that are bound to fail.

Other comments related to difficulties in getting information from Social Media companies outside of Türkiye, including not taking down criminal accounts or proficiently dealing with hijacked accounts. Many delegates felt legislation was necessary albeit accepted the reach only went as far as the Turkish borders.

[20] Bu paragraf, uluslararası uzman(lar) tarafından yapılan bir yorumdur.

Discussions about electronic evidence identified that it can quickly be changed, deleted, moved, or overwritten as part of everyday processes or criminal activity. The activity of preserving online data (emails, servers, communication data etc.) was not widely understood and the urgency of preservation requests do not seem to be undertaken efficiently enough. Where there was a need to preserve data, the 24/7 Single Point of Contact (24/7 SPOC) was not utilised sufficiently. From the discussions in the various workshops there are two main reasons,

- The official does not know about the services that the 24/7 SPOC can provide,
- The official does not know how to reach the 24/7 SPOC.

Training could improve this situation as well as wider sharing of the contact details of the 24/7 SPOC.

It is recommended that an online training and instructions about the role of 24/7 Single Point of Contacts dealing with electronic evidence should take place to explain how Social Media companies acted in Türkiye and the role of the 24/7 SPOC. The purpose of these events and communications is to identify what material and requests multi-national service providers and social media companies are prepared to send to Türkiye and identify types of requests that are bound to fail.

The contact information for the 24/7 SPOC should be shared with all prosecutors and cybercrime units (in both the TNP and Gendarmerie) as a minimum.

4. Prosecutors

a. Role of prosecutors in combating cybercrime

The role of a prosecutor in Türkiye when combating cybercrime is multifaceted and crucial. As a legal representative of the state, a prosecutor is responsible for investigating, charging, and prosecuting individuals suspected of committing cybercrimes.

There are many different stages in this process and the following sets out a good practice protocol for prosecutors:

1. Investigation: Prosecutors collaborate with law enforcement agencies and cybercrime units to collect evidence, identify suspects, and build a strong case against alleged cybercriminals. They may also work with private sector partners, such as Internet service providers and tech companies, to obtain relevant information.

2. Indictments: Based on the evidence gathered during the investigation, prosecutors decide whether to bring formal charges against suspects. They are responsible for determining the appropriate indictments, considering factors like the nature of the offence, the severity of the harm caused, and the suspect's criminal history.

3. Prosecution: Prosecutors represent the state in court proceedings and are responsible for presenting the evidence and arguments to prove the accused's guilt. They must ensure that the process is fair, just, and respects the rights of the accused while pursuing justice for victims and society.

4. Collaboration: Combating cybercrime often requires international cooperation, as cybercriminals may operate across borders. Prosecutors must work with their counterparts in other jurisdictions to share information, coordinate investigations, and conduct joint prosecutions when necessary.

5. Legal expertise: Prosecutors must possess a deep understanding of the applicable laws and legal frameworks related to cybercrime, as well as stay up to date with emerging trends and technologies. This knowledge helps them to effectively apply the law and adapt to the ever-evolving landscape of cybercrime.

6. Prevention and deterrence: By prosecuting and securing convictions for cybercrimes, prosecutors contribute to deterring would-be criminals from engaging in similar activities. They also raise public awareness of the legal consequences associated with cybercrime, which can prevent potential offenders from engaging in such behaviour.

7. Advocacy and policy development: Prosecutors play a role in advocating for stronger laws, policies, and resources to combat cybercrime. They can provide valuable input to legislators and policymakers based on their experience and insights from handling cybercrime cases.

8. Capacity building: Prosecutors are involved in capacity-building efforts aimed at improving the effectiveness of law enforcement agencies, the judiciary, and other stakeholders in combating cybercrime. This can include training and education programs, sharing best practices, and developing relevant and appropriate guidelines and protocols.

b. Challenges faced by prosecutors in prosecuting cybercrime

The coordination meetings were held across various geographical regions in Türkiye to establish the challenges facing prosecutors. There were some common issues and some regional differences in how prosecutors dealt with the investigation and prosecution of cybercrime. These meetings were well attended, and the main challenges were identified as follows:

Technical complexity

It was widely recognised and acknowledged that there was a shortage of skills and knowledge amongst prosecutors when dealing with cybercrime cases. Cybercrimes often involve sophisticated technologies and methods, which are ever evolving and unless trained makes it difficult for prosecutors to understand the underlying mechanisms and present evidence in a clear and concise manner. There is also the heavy reliance on experts to explain the technical aspects of the case to the judge and jury.

As such, training on all cybercrime offences including the handling of electronic evidence and other digital exhibits with regular updates is necessary for prosecutors. This is so that they can continue to improve their knowledge of cybercrime and electronic evidence to enhance investigation and detection.

The workshops highlighted a perceived shortage of reliable expert witnesses, a claim contested by the digital forensic expert witness present. He stated that prosecutors often submit unclear and vague evidence requests, improperly package exhibits, and fail to respond promptly to requests for additional information such as passwords. It was proposed that prosecutors should undergo training to better understand digital forensic reports, which they often find confusing. Forensic experts should also strive to simplify their statements, perhaps by including a glossary of terms and visuals. The forensic experts suggested the establishment of an online network for forensic professionals to share experiences and best practices.

It was recommended that there should be a template for prosecutors to send evidence to the digital forensic specialists. The Ministry of Justice are in the process of developing such a template.

Prosecutors also mentioned the evaluation system used for prosecution files, which is, prosecutors are judged based on the quantity of cases they handle. This system incentivises dealing with minor cases such as assault or theft rather than cybercrime cases. This is due to the complexity of cybercrime cases, which require specialised skills, often involve international elements, and take significantly longer to resolve. The current evaluation system for promoting prosecutors handling cybercrime cases is often tied to the number of cases they manage and successfully close. Given the extended duration required to investigate cybercrime cases, prosecutors handling these cases are disproportionately affected as they cannot close the cases swiftly enough.

Since this affects the career advancement of prosecutors It was recommended that cybercrime cases either be removed from this key performance indicator or due to the complexity of cybercrime cases they should be rated or scored higher than other cases. The Ministry of Justice recognised this as an issue affecting both prosecutors and judges and is exploring potential solutions to address it.

Part of the problem is that the prosecutors have too many cases to deal with.

It is helpful to look at what occurs in other countries. For example in the United Kingdom the system is different as judges and prosecutors do not work on the case file, rather that is done by law enforcement officers. The prosecutor in the UK during the investigative stage provides advice and guidance on the case. It was suggested that the work of the prosecutors is examined to see what can be delegated. For example once trained officers could take witness and victim statements. Training and upskilling of criminal justice personnel has occurred in the UK, especially in relation to the seizure and handling of electronic evidence in trials. For example, in relation to sensitive material (child sexual abuse material) and the way in which the prosecution (and investigation) sought to deal with child abuse victims, including video interviewing by police, when appropriate anonymity for victim and /or witness etc.

The Ministry of Justice has assessed what aspects of the work of the prosecutor can be delegated to others so that prosecutors can be freed up to do essential work. Prosecutors will be assigned assistants to whom they can delegate appropriate work.

Having a single point of contact

Prosecutors identified a consumate failure by private businesses, banks and service providers to respond to their requests for information. This in turn had a detrimental knock-on effect on cases. As a result, it was suggested that 'industry', police and prosecutors should have a single point of contact to facilitate active contact and assistance.

Gathering and preserving digital evidence

Collecting and preserving digital evidence can be challenging due to its volatile nature and the ease with which it can be altered or destroyed. Prosecutors must work closely with law enforcement to ensure that digital evidence is properly collected, preserved, and analysed.

There has been a significant rise in the number of reported cybercrimes and there is an increased need for digital forensics to handle electronic evidence in a competent manner. There seemed to be a general lack of communication and guidance between prosecutors and the Forensic Institution on what was required. In the circumstances, better communication and guidance is required between the parties. It was recommended that templates and guidelines on the collection of evidence would assist to remedy the current deficiencies in the system.

It was proposed to create a database integrated with UYAP on IBAN numbers used in crime. It was suggested that IBAN and account information should be made available to law enforcement and/or prosecution offices through the UYAP system.

Cross-jurisdictional issues

Cybercriminals often operate across international borders, which can create legal challenges related to jurisdiction and the enforcement of laws. Extradition, mutual legal assistance, and cooperation between different countries; law enforcement agencies can be slow and complicated.

Anonymity and encryption

Cybercriminals often use tools and techniques to hide their identity and location, such as anonymous networks and encryption. This can make it difficult to trace and identify suspects, as well as to access crucial evidence.

Discussion took place in respect of encryption regarding the UK's Section 49 Regulations of Investigatory Powers Act 2000 (RIPA) which criminalise / penalise a person who refuses to provide the key to encrypted or otherwise inaccessible information. There was an expression of interest in the legislation but also surprise by at least one delegate during the meeting that this legislation is not contrary to the Human Rights legislation. Section 49 has been in force in the UK since 2007 and countries such as Republic of Ireland, France, Australia, and Finland have similar legislation. All such powers as this have and require safeguards. This point does not formulate a recommendation but reflects the discussions that took place looking at how international partners deal with challenges such as encryption.

Rapidly evolving technology

The fast-paced evolution of technology means that laws and law enforcement techniques may struggle to keep up with new forms of cybercrime. Prosecutors must stay up to date with emerging trends and adapt their strategies accordingly. This they could do with the appropriate training.

Legal frameworks

Cybercrime laws vary across jurisdictions, and in some cases, existing laws may be outdated or insufficient to address new forms of cybercrime. Prosecutors may face challenges in applying the law effectively, and there may be gaps in the legal framework that hinder successful prosecution.

All agreed on the inadequacy of Article 134 in CPC (Search of computers, computer programs and transcripts, copying and provisional seizure).

Resource constraints

Prosecuting cybercrimes can be resource-intensive, requiring specialised skills, knowledge, and tools. Law enforcement agencies and prosecution offices may lack the necessary resources, training, and personnel to effectively investigate and prosecute cybercrimes. For example, when following the monies in crypto currency cases, it is widely recognised that the technology changes quite rapidly and is challenging to keep up with. This further underlines the importance of specialised training as set out in section 4c below.

Public awareness and victim reporting

Many victims of cybercrime may be unaware that they have been targeted or may be reluctant to report the crime due to embarrassment, fear, or a lack of trust in the authorities. This can make it difficult for prosecutors to build strong cases and bring cybercriminals to justice. For further discussion on this point see section 8b below.

Establishing intent and attribution

Proving criminal intent and attributing cybercrimes to specific individuals can be challenging due to the often anonymous nature of online activities. Prosecutors must gather sufficient evidence to demonstrate that the accused knowingly engaged in criminal activities and can be held accountable for their actions.

c. Importance of specialised training and resources for prosecutors

The workshops revealed that prosecutors dealing with cybercrime cases require specialised training beyond their traditional legal education. There should be regular review of training needs and ongoing in-service training efforts with regards to cybercrime. Cybercrime-related training should be an integral part of the standard pre-service training curriculum. There should be a comprehensive training strategy for prosecutors (and for judges and law enforcement officers).

Every prosecutor should be able to deal effectively with all evidential issues of cybercrime offences.

In order to allow prosecutors to apply their cybercrime knowledge such training programs should provide opportunities for practical application, such as mock trials.

To that end, Specialised Judicial Training on Electronic Evidence prepared within iProceeds-II project has been translated in Turkish and adopted to Turkish legal framework. It aims to be integrated into the training programmes of Justice Academy for both prosecutors and judges in the near future.

Some of the areas where it was identified that prosecutors may need additional training were:

1. Understanding of cybercrime laws: It's essential for prosecutors to thoroughly understand national and international cybercrime laws. This includes familiarity with specific national legislation, as well as broader international conventions like the Council of Europe's Budapest Convention on Cybercrime.

2. Technical knowledge: Prosecutors need to comprehend the technological aspects of cybercrime. This includes an understanding of digital forensics, networks, computer hardware, malware, ransomware, phishing, cryptocurrency and the dark web and other cybercrime tools and methods work.

3. Digital evidence handling: Training should cover the collection, preservation, and analysis of digital evidence. This includes understanding how to maintain the chain of custody for digital evidence, how to work with digital forensic experts, and how to present such evidence in court. This also includes handling and disclosing to the defence sensitive material.

4. Understanding cybercrime trends and tactics: Given the rapid evolution of technology, ongoing training should include updates on the latest cybercrime trends, tactics, and threats, as well as the tools and strategies used to combat them.

5.International and cross-jurisdictional issues: Because cybercrime often involves multiple jurisdictions, prosecutors need training on international laws and extradition agreements, and how to collaborate effectively with law enforcement agencies in other countries.

6. Victim support: Cybercrime can have a significant emotional and financial impact on victims. Prosecutors should be trained in how to provide effective support and resources to victims.

5. Judges

a. Role of judges in combating cybercrime

The role of judges relating to combating cybercrime is multifaceted and crucial in Türkiye. As a legal representative of the justice system, a judge is responsible for adjudicating about individuals suspected of committing cybercrimes in the long-term prosecution process.

It includes different stages, and the following sets out a good practice protocol for judges:

1. Investigation: Judges are the part of the investigation phase as well as prosecution phase. Within the investigation phase, prosecutors have ability to request measures of protection by judicial decision of judges on collecting evidence related to cybercriminals.

2. Indictment and decision of non-prosecution: Based on the evidence gathered during the investigation, prosecutors decide whether to bring formal charges against suspects. By this decision indictments are examined by judges about legal necessities. Judges can determine a demurrer to indictment by providing a more detailed investigation process or overcoming the deficiencies of indictments by prosecutors. On the other hand, prosecutors can determine to prepare decisions of non-prosecution with the thought that having insufficient evidence about cybercriminals committing a crime. Decisions of non-prosecution are also examined by judges in the direction of objection by any parties of that case.

3. Prosecution: Judges represent the state in court proceedings and are responsible for examining all allegations and pleas by parties and collecting missing and demanded evidence in collaboration with public and private entities. And their main role is to make a verdict aftermath of all these processes whereby rights of all parties are protected and respected fairly and lawfully.

4. Collaboration: Combating cybercrime often requires international cooperation, as cybercriminals may operate across borders. Judges must work with their counterparts in other jurisdictions to share information, coordinate prosecution, and conduct joint prosecutions when necessary.

5. Legal expertise: Judges must possess a deep understanding of the applicable laws and legal frameworks related to cybercrime, as well as stay up to date with emerging trends and technologies. This knowledge helps them to effectively apply the law and adapt to the ever-evolving landscape of cybercrime.

6. Prevention and deterrence: Judges contribute to deterring impunity in cybercrimes by prosecuting cybercrimes and adjudicating fairly for cybercriminals. They also raise public awareness of the legal consequences associated with cybercrime through their verdicts that are made on an equitable basis.

7. Advocacy and policy development: Judges play a role in advocating for stronger laws, policies, and resources to combat cybercrime. They can provide valuable input to legislators and policymakers based on their experience and insights from handling cybercrime cases. Additionally, supreme court judges especially play a role in the development of precedent, and they can provide a valuable legal opinion for all parties of the legal system in general. The precedent is also available and necessary for filling the legal gaps.

8. Capacity building: Judges, who usually speak with their decisions, are also involved in capacity-building efforts aimed at improving the effectiveness of law enforcement agencies, the judiciary, and other stakeholders in combating cybercrime. This can include training and education programs, sharing best practices, and developing relevant and appropriate guidelines and protocols.

b. Challenges faced by judges in adjudicating cybercrime cases

The coordination meetings were held across various geographical regions in Türkiye to indicate the challenges for judges. There were some common issues and some regional differences in how judges dealt with the investigation and prosecution of cybercrime. These meetings were well attended, and the main challenges were identified as follows:

Technical complexity

It was widely recognised and acknowledged that there was a shortage of skills and knowledge among judges when dealing with cybercrime cases. Cybercrimes often involve sophisticated technologies and methods, which are ever evolving and being insufficiently trained makes it difficult for judges to understand the underlying mechanisms and to present evidence in a clear and concise manner. In addition to this deficiency, was reported in the workshops that there was a lack of credible expert witnesses. Consequently, there is a need for specialisation for judges. The recent establishment of specialised courts for cybercrimes provides various benefits, such as speeding up judicial proceedings.

As such, training on all cybercrime offences including the handling of electronic evidence and other digital exhibits with regular updates is necessary for judges as well as prosecutors. Thus, that they can continue to improve their knowledge of cybercrime and electronic evidence to enhance prosecution. This need is derived from insufficient investigation process. It is stated in almost all the meetings that insufficient investigations require the fulfilment of investigation procedures such as evidence gathering activities in the prosecution phase by judges. Even if judges have relevant procedural power to substitute investigatory acts during the prosecution phase, it is rather a fruitless practice for cybercrime cases since digital evidence are volatile and usually stored for a short period of time.

Judges also discussed the scoring method of closing the cybercrime cases by their final verdict within the context of difficult challenges and the specialism of cybercrimes. These challenges result in extending the process, and judges who dealt with those cases suffer for not closing enough cases. It was thus recommended that cybercrime cases would be evaluated differently from other types of the cases within performance evaluations.

Having a single point of contact

Need of collaboration with public and private entities subsists in the prosecution phase too because of the factors explained above such as necessity of conducting investigatory procedures during the prosecution phase, and insufficient investigation situation. Therefore, prosecution is affected from the failure of response or insufficient response by private businesses, banks and service providers. This situation causes subsequent warrants to be sent to private actors, and that lingers the prosecution phase even further. As a result, it was suggested creating single point of contact to facilitate active contact and assistance between these parties.

Gathering and preserving digital evidence

As explained above, since digital evidence is often not entirely collected in the investigation phase, judges are obliged to collect digital evidence during the prosecution phase with their relevant powers. However, digital evidence is mostly deleted and eliminated completely until that stage which is after months or years from the date of crime committed.

Cross-jurisdictional issues

Cybercriminals often operate across international borders, which can create legal challenges related to jurisdiction and the enforcement of laws. Extradition, mutual legal assistance, and cooperation between different countries; law enforcement agencies can be slow and complicated.

In addition to this, it is observed that some international private entities do not response rogatory demands for depending on different reasons. For example, the act of defamation is regulated as a crime in Türkiye, however, that act is not regulated as a crime in some European countries. The lack of monotonous regulation among countries causes the malfunction of the process of international collaboration.

Rapidly evolving technology

The fast-paced evolution of technology means that laws and law enforcement techniques may struggle to keep up with new forms of cybercrime. Judges must stay up to date with emerging trends and adapt their strategies accordingly. They can achieve it with the appropriate training. Also, it was reported that in this fact following up on recent legal precedent of higher courts is important and crucial. Correspondingly, it was stated that it would be useful to prepare weekly or monthly bulletins that include current and relevant case law which can be viewed on the National Judiciary Informatics System (UYAP) screen.

Legal frameworks

Cybercrime laws vary across jurisdictions, and in some cases, existing laws may be outdated or insufficient to respond to new forms of cybercrime. Judges may face challenges in applying the law effectively, and there may be gaps in the legal framework that hinder successful prosecution. All agreed on the inadequacy of Article 134 in CPC (Search of computers, computer programs and transcripts, copying and provisional seizure).

Also, it was stated that judicial authorities lack the authority to decide on various protection measures. It was also stated that a quick and adequate contact channel should be established, and awareness-raising activities should be carried out, especially regarding the freezing of transactions. In addition, an opinion was indicated that the judicial authorities are rather hesitant to make decisions on protective measures. It was also stated that a quicker method with adequate safeguards should be adopted in terms of freezing accounts and transactions.

Resource constraints

Prosecuting cybercrimes can be resource-intensive, requiring specialised skills, knowledge, and tools. Judges have lacked the necessary resources, training, and personnel in their court registry to effectively prosecute cybercrimes. For example, when tracking the money in crypto currency cases, it is widely recognised that the technology changes quite rapidly and is challenging to keep up with. Hence, some participants offered that technical personnels should be appointed in the courts and law enforcement agents.

Establishing intent and attribution

Proving criminal intent and attributing cybercrimes to specific individuals can be challenging due to the often-anonymous nature of online activities. In the event of an insufficient investigation where missing evidence exists, Judges must gather sufficient evidence to demonstrate that the accused knowingly engaged in criminal activities and can be held accountable for actions.

Unification of all Specialised Courts

It was frequently stated at the meetings that establishing specialised courts on cybercrime at first instances courts in every city of Türkiye definitely help the specialisation of judges. However, especially judges of Assize Courts also have other critical cases such as murder or drug related crimes, and these crimes often put so much burden on judges' shoulder that they cannot put the necessary effort on cybercrime cases. Therefore, it was suggested that all IT crimes that fall within the jurisdiction of the Criminal Courts of First Instance and the Assize Courts can be tried by a single specialised court, or it can be provided in big cities that Assize Courts specialised on cybercrime will only deal with cybercrime cases, thus eliminating the burden created by other crimes and ensuring a real specialisation.

c. Importance of specialized training and resources for judges

The workshops revealed that judges dealing with cybercrime cases require specialised training beyond their traditional legal education. There should be regular review of training needs and ongoing in-service training efforts with regards to cybercrime. Cybercrime-related training should be an integral part of the standard pre-service training curriculum. There should be a comprehensive training strategy for judges (and for prosecutors and law enforcement officers). Every judge should be able to deal effectively with all evidential issues of cybercrime offences.

In order to allow judges to apply their cybercrime knowledge such training programs should provide opportunities for practical application, such as mock trials.

To that end, Specialised Judicial Training on Electronic Evidence prepared within iProceeds-II project has been translated in Turkish and adopted to Turkish legal framework. It aims to be integrated into the training programmes of Justice Academy for both prosecutors and judges in the near future.

Some of the areas where it was identified that judges may need additional training were:

1. Understanding of cybercrime laws: It's essential for judges to thoroughly understand national and international cybercrime laws. This includes familiarity with specific national legislation, as well as broader international conventions like the Council of Europe's Budapest Convention on Cybercrime.

2. Technical knowledge: Judges need to comprehend the technological aspects of cybercrime. This includes an understanding of digital forensics, networks, computer hardware, malware, ransomware, phishing, cryptocurrency and the dark web and other cybercrime tools and methods work.

3. Digital evidence handling: Training should cover consideration of the legal requirement of collection, preservation, and analysis of digital evidence. This includes understanding how to maintain the chain of custody for digital evidence, how to work with digital forensic experts, and how to interpret such evidence in court. This also includes handling and disclosing to the defence sensitive material.

4. Understanding cybercrime trends and tactics: Given the rapid evolution of technology, ongoing training should include updates on the latest cybercrime trends, tactics, and threats, as well as the tools and strategies used to combat them.

5. International and cross-jurisdictional issues: Because cybercrime often involves multiple jurisdictions, judges need training on international laws and extradition agreements, and how to collaborate effectively with public authorities in other countries in the context of the rules of rogatory.

6. Victim support: Cybercrime can have a significant emotional and financial impact on victims. Judges should be trained in how to provide effective support and resources to victims. In addition, Judges should be trained to explain the basis of intervener rights to the victim, especially if the victim does not have a legal attorney.

6. Digital Forensic Specialists

a. Capabilities

Digital Forensic Science is a branch of forensic science that focuses upon identifying, acquiring, processing, analysing, and reporting on data stored on electronic devices. Electronic evidence is becoming a factor upon all criminal investigations and support for the law enforcement, prosecutors, and judiciary in Türkiye for criminal investigations.

As part of the Joint Project's Needs Assessment, visits of digital forensic laboratories took place. Additionally, experts from the digital forensic laboratories attended some of the workshops. Examination of the equipment, processes and reports shows that Türkiye has a professional and well-equipped set of digital forensic laboratories available to law enforcement and prosecutors. The analysists are well trained and there are plenty of them employed by the authorities in Türkiye.

An assessment of the challenges that are faced in digital forensics appears to be more of quantity of devices requiring analysis rather than the quality of the examination. Another area that was discussed was the standard of requests made to the digital forensic laboratory by prosecutors, who did not appear to understand the details that were needed for the examination and made too many requests that were not specific about what was being sought.

b. Exhibit handling

On many occasions, digital devices are submitted to laboratories contained in inappropriate packaging, which failed to prevent damage to the device, loss of data through heat, dampness, magnetism, or remote wiping. This meant devices were unable to be examined.

Whilst this failure is caused by the officers, prosecutors, and other officials involved in the investigation the solution is with the managers. Provision of the correct packaging is essential. This must be reinforced with directives that digital devices will not be accepted at the laboratories unless they are suitably packaged. Whilst this would initially start with some additional delays, after time everyone would be used to the system and follow the guidelines.

Other challenges include the submission of devices (mobile telephones) where the PIN code or pass phrase has not been obtained during the scene search or first stages of the case. This means that the analyst must break the code to acquire data (at an increased cost) and the prosecutors should consider this when managing scene searches and the submission of exhibits.

c. Exhibit submission

Digital forensic representatives at the coordination meetings explained other issues that occurred too frequently when digital devices are submitted to the laboratory;

• Often prosecutors submitted requests for digital forensic examination, where the scope of what was required was vague or not identified,

• Such requests often failed to include the basic description of the offence under investigation and the circumstances of the device seizure,

• Requests, which were described as vague or unclear, often resulted in large costs to be met by the relevant Prosecutors Office because of the time incurred where the instructions lacked clarity,

• Objective requests were often made, where the analyst was asked to make an interpretation if an image of an adult was indecent. These were subjective decisions outside the training of a digital forensic analyst.

The representatives from the Ministry of Justice Digital Forensic Laboratory explained that it would be useful for the laboratory to provide in house training to prosecutors and judges to deal with some of these submission failures. Digital forensics - A lot of the discussions dealt with the issues relating to Digital Forensics and were introduced by a participant from the Ministry of Justice Digital Forensic Laboratory. This suggestion is well received and is now a recommendation of this report.

The creation and mandatory use of a template that needs completion upon submission of exhibits to the Digital Forensic laboratory is recommended. The template, which will need to be drafted by the Ministry of Justice Digital Forensic Laboratory should stipulate details of the case, details of seizure, reference numbers, specific details that need to be undertaken at the laboratory including word searches. Other data, such as passwords, PIN codes, suspect and witness details should also be included. When sending work prosecutors and judiciary should add definitions such as "what constitutes an explicit image".

d. Analysis and reporting

In many of the workshops prosecutors and judges reported that they received digital forensic statements that they do not always understand, and they need to be simplified. Often the reports did not include a glossary of terms, which would have made reading them a simpler exercise.

The representatives from the digital forensic units accepted these comments and indicated that they would feed them back to staff. But they identified that with every report that they sent to the courts, a feedback form was attached. It appeared that it was extremely rare for these feedback forms to be completed and/or returned.

e. Child Sexual Abuse Material

During workshops, meaningful conversation took place about the examination of digital devices that contained Child Sexual Abuse Material (CSAM). Discussions identified that the material was handled in a similar way to other electronic evidence and no special procedures are in place in the handling of such material.

The number of copies of the CSAM should be kept to a minimum. For example, is there a requirement for the prosecutor to have the forensic image or copies of the videos or photos obtained in the analysis? Furthermore, is there a necessity for the defendant or defence solicitor to have the forensic image or copies of the videos or photos obtained in the analysis? International best practice seeks to avoid the sharing of such material and if the prosecutor or defence lawyer needs access to it, they can attend the digital forensic laboratory to view it in controlled ways.

Legislation currently exists in Türkiye that where a suspect's computer has been seized and imaged, he must have the computer returned to him as soon as that process is complete. This rare legal provision in Türkiye enables the return of the CSAM to the offender, which is bad practice when compared to how material should be handled. Türkiye is a signatory of the Council of Europe Lanzarote Convention on Protection of Children against Sexual Exploitation and Sexual Abuse[21]. This situation contradicts some of the important statements in the convention about protecting children from victimisation.

7. Public-Private Cooperation

a. Importance of collaboration between public and private entities in combating cybercrime

The workshops revealed that collaboration between judicial authorities and public/private entities has crucial importance to reach and explain objective elements of the offence in the cybercrimes, and several key elements has been identified as follows:

[21] https://www.coe.int/en/web/children/lanzarote-convention

1. Digitalisation and private ownership: Complex structure of Internet and digitalisation gives rise to a compulsory sectoral specialisation. Therefore, judicial authorities must reach different entities of various sectors to gather different type digital evidence. Plus, the private ownership of digital technologies hinders the direct access to personal data like IP address, bank account records, etc. by judicial authorities. To that end, information sharing and collaboration between judicial authorities and public/private entities becomes a necessity to prevent and combat cybercrime effectively.

2. Cross-border evidence gathering: Internet is a world-wide phenomenon that eliminates the physical borders without a centralized authority. Digital services that have millions of users can be provided by private actors located in different jurisdictions and cybercriminals use these services for their illegal activities with cross-border nature. Therefore, evidence gathering practices from foreign private actors become very crucial concerning the fight against cybercrime.

3. International and digital money transfer: Internet has changed traditional banking system and today a person can freely transfer him/his money to any branch of a bank regardless of national borders. Correspondingly, following cash-flow without bank records is almost impossible. Judicial authorities must send warrant to take records of bank account that belongs to cybercriminals in parallel to the "follow to money" principle in order to resolve their cases.

b. Examples of problems in public-private partnerships in Türkiye regarding cybercrime

Identified problems in public and private partnerships in Türkiye can be summarised as follows:

Rapid technological developments and the need for capacity building: Digital area has been developing rapidly and cybercriminals can use these new techniques for committing crimes and not all private actors can follow these developments closely and with an adequate technical capacity. Therefore, it is observed that the difference in technical and organisational capabilities in private actors hinder the possibility of a harmonised functioning regarding the fight against cybercrime. Even in a highly regulated sector such as banking sector, banks do not have a similar level of resources, tools or methods and that results in having differentiation between their success in preventing cybercrimes and their responses to the cooperation requests from judicial authorities.

Miscommunication and delays in data sharing: It is observed that there are regular delays and sometimes no response in relation to the judicial requests from private businesses and service providers. On the other hand, it was also stated this problem can be occurred due to the lack of knowledge of procedures of judicial authorities. In that regard, they often send requests to irrelevant parties or umbrella organisations such as the Banks Association of Türkiye and the BRSA (neither of them have legal power and authorisation to respond such request under current legal framework) instead of the banks, and this prolongs the investigations. In this context, even if an umbrella organisation cannot be established in every sector, the cooperation system between parties should be optimised with clear procedural rules and guidance.

It is also observed that social media platforms fail to quickly act upon deactivating and deleting accounts that are captured and used for fraudulent activities. It is also suggested that a direct communication system should be established between prosecutor's offices and representative offices of relevant social media companies.

Social media platforms: The fact that the big social media companies' headquarters are abroad, and the differences of substantial law between Türkiye and third-party countries that social media companies are located hinders the success level of the cooperation. Law numbered 5651 and its relevant provisions do not effectively provide the necessary enforcement over that companies. Using international legal cooperation mechanisms such as Budapest Convention more effectively, establishing better partnerships with this companies and regulating more effective legal framework in that regard are crucial to gather cross-border digital evidence.

Legislation on following and freezing proceeds of crime: It is also observed that the Article 61 of the Banking Law and the BRSA and its application lack efficiency and success in blocking fraudulent transactions and accounts. On one hand, foreigners can easily get mobile lines without sufficient legal checks or verification system. On the other hand, Turkish and foreigners are able to open up accounts in digital services such as e-money platforms, digital payment services, betting sites, and crypto trading platforms that help them transfer money easily, again without harmonised "know your customer" (KYC) requirements. Parallel to these, "potato lines" and "money mules" prevent judiciary to reach essential digital evidence as well as actual cybercriminals. It was suggested that the conditions for issuing mobile lines to foreigners should be made more difficult, and that effective identity validation systems should also be used for digital finance services and other related digital services (i.e. e-commerce companies, online betting sites, etc.)

8. Victims of Cybercrime

a. Overview of the impact of cybercrime on victims

In this modern era, technology and the Internet have become an integral part of our lives. Along with the advancement of technology and Internet usage, cybercrime is emerging as a serious cause for concern as it touches on every aspect of our lives. Cybercrime is a complex phenomenon where criminal activity is conducted using technology and the internet. Cybercrime operates in a virtual space, which makes regulating and policing it quite difficult. The impact on victims due to cybercrime can be both long lasting and distressful.

The impact of cybercrimes and cyber-enabled crimes can be far-reaching, often resulting in devastating consequences for victims. Listed are some of the impacts of cybercrime and cyber-enabled crimes on victims:

Emotional damage: Victims may be profoundly impacted emotionally by cybercrime.

Cybercriminals may steal the private information of victims, and this may leave them feeling helpless and violated. It is essential that victims are aware of the damage that a cyber-attack can inflict on them and that they are able to take steps to prevent cybercrime.

Reputational damage: Victims may face damage to their reputation due to cybercrime. This damage is usually long-lasting in the lives of victims and can make it difficult to recover from it quickly.

Financial loss: Cybercriminals often steal the private and financial information of a person and use it in such a way to cause them financial loss. Victims of such crimes can become reluctant to trust any online financial activity in the future.

Physiological impact: Cybercrime (s) can affect the mental health and well-being of a victim.

Victims of cybercrime can feel anxious, depressed, and violated. And in some situations, can also feel embarrassed and ashamed about the crime that happened to them.

Safety issue: Due to cybercrime (s), victims can experience safety issues as well. A victim's physical location can be accessed by cybercriminals by stealing his private data and information. This can lead to distress and mental pressure in the victim's life.

Privacy threat: Victims are exposed to significant privacy threats due to cybercrime, as a result of which victims may feel insecure about privacy, violated, and depressed.

b. Importance of providing support and resources to victims of cybercrime

Cybercrime has become a growing concern in recent times. This crime has the capacity to affect millions of Internet users. Due to cybercrime and cyber-enabled crimes, a victim can suffer emotional damage, safety issues, privacy threat, psychological impact, and legal consequences. In such situations, the victims need reliable support and appropriate resources to support them. Cybercriminals are tech-savvy and know the loopholes in the digital space and use it to harm innocent digital users.

Cybercrime can be curbed using the right strategies, government-supportive steps, education, and effective resources. Support and resources should be made available to cyber victims to help them cope with such adverse situations. It is equally important for individuals to take proactive steps to protect themselves from such cyber threats. Resources should be provided by the government which an individual or small/medium business can utilise to keep safe and secure from such crimes.

Several issues were raised during workshops ranging from failure to report cybercrime cases and the way in which victims were treated upon reporting a case.

Failure to report: In respect of failure to report cybercrimes it was noted that internationally, the issue of underreporting of cybercrime is significant. With less than 1% of cybercrime incidents being reported to law enforcement agencies, and of these, less than 1% resulting in a criminal justice verdict, the proportion of cybercrime leading to convictions is notably small. It's imperative that this is addressed and improved, or the criminal justice response risks becoming inconsequential in the face of this type of crime.

It was suggested that the low number of cybercrimes reported had to do with the shame of being scammed; a lack of trust in the criminal justice system; the length of time it takes for the case to come to court and the length of time it takes to reach a conclusion. It was also recognised that victims were often treated with a lack of sensitivity upon reporting cybercrimes.

It was also suggested that victims may not know the correct place to report cybercrime and cyber enabled crime. This was because insufficient information was often placed in readily available information systems (such as websites). This often meant that victims reported cybercrime and cyber enabled crime to the wrong institution or department, causing delays and the loss of electronic evidence. It was suggested that public information should be improved and that the reporting of cybercrime should be facilitated through the creation of an online cybercrime reporting system.

Non-jurisdiction: This is where a victim reports the offence and then the prosecutor indicates that it would not be investigated further because the offence occurred outside of that prosecutor's jurisdiction. Victims could then find themselves being passed on to different prosecutors' offices. It was mentioned that legislation was recently bought in to deal with this issue and that the offence will now be investigated in the area where the person resides.

Awareness and prevention campaigns: In relation to money mules, it was felt that public information campaigns would be useful. Many mules were duped into receiving criminal funds through their own accounts after answering online advertisements. This was because many were naïve and public information awareness campaigns publicising how such scams are perpetrated would go some way in preventing their involvement in such crimes. It the UK it was noted that students were being caught up in this scam, which led to an awareness campaign being held on university campuses.

The effect of data protection : The number of cyber frauds committed is increasing day by day according to published Interpol statistics. The widespread use of cloud computing tools and services bring major problems with regard to obtaining and dissemination of personal data unlawfully. Victims usually have a lack of awareness about the importance of their personal information and how it should be protected in this technological age. It was suggested during the meetings that there should be education programs in schools to inform and teach young people and adolescents how to safeguard their personal data and themselves online.

For example, The Government of the United Kingdom has many online resources and guidance on cybercrime which is readily available to the public. By utilising these resources an individual can access the right information and get the desired help to stay safe online. This includes the following:

National Cyber Security Centre: National Cyber Security Centre is an agency of the United Kingdom government that provides support and guidance for cyber security. This agency aims to prevent cybercrime and provide much needed help to victims (www.ncsc.gov.uk).

Cyber Aware: Cyber Aware is a campaign of the United Kingdom Government. This campaign provides guidance on how an individual can stay safe in digital space and protect himself from cybercrimes (www.ncsc.gov.uk).

Action Fraud: Action Fraud is the United Kingdom's national reporting centre for cybercrime. Cybercrime can be reported here at any time of the day or night. The service of Action Fraud enables a victim to both report cybercrime and access help and support. (https://www.actionfraud.police.uk)

Victim Support: Victim Support is a charitable initiative by the government of United Kingdom. This charity provides support to victims of cybercrime. They also provide needed support and guidance to the victims of cybercrime (https://www.victimsupport.org.uk).

C. CONCLUSIONS AND RECOMMENDATIONS

As a result of the discussions in the workshop and the input from the international experts, the following conclusions and recommendations are made;

1. Law Enforcement

1. There remains a need to encourage Turkish National Police and the Gendarmerie units dealing with cybercrime to share their experience in this field;

2. To create a National Cyber Crime Unit to align with other national entities and coordinate the cybercrime response in Türkiye at local, regional and international levels (see paragraph 3a);

3. To create a National Unit dedicated to leading the response to online abuse against children and coordinate the online response to child abuse and child sexual abuse images in Türkiye at local, regional and international levels (see paragraph 3b);

4. To create a dedicated central reporting system fulfilling the role of an online national reporting centre for cybercrime (see paragraph 3c);

5. Law enforcement agencies create and implement a dedicated training strategy for investigating of cybercrime and dealing with electronic evidence. (see paragraph 3d);

6. To reduce the workload of law enforcement agencies and prosecutors through streamlining investigative processes. Investigators and prosecutors should focus resources upon investigations that are likely to succeed rather than undertake investigations upon cases that are bound to fail in the collection of evidence and/or the attribution of offending (see paragraph 3e)

7. Urgent improvement is needed in the areas of inter-agency cooperation. It is recommended that as many of the recommendations as possible, that are detailed in the Interagency Cooperation Protocol discussed with the Council of Europe and Türkiye are reviewed and implemented (see paragraph 3f);

8. To create dedicated resources in Türkiye to undertake online covert investigation measures such as surveillance, test purchase and undercover operations. Ideally such a unit would be placed in a National Cyber Crime Unit, but the creation of such a body would take time. These resources are required in the short term (see paragraph 3g);

9. For law enforcement to implement coordinated and meaningful crime prevention plan with a variety of awareness activities related to cybercrime across Türkiye. This is in line with the requirements of the current Turkish National Cyber-Security Strategy (see paragraph 3h);

10. To create a dedicated law enforcement unit whose role is to concentrate on the crime prevention plan within Türkiye. Ideally such a unit would be placed in a National Cyber Crime Unit, but the creation of such a body would take time. These resources are required in the short term (see paragraph 3h);

11. For the 24/7 SPOC within the TNP or similarly trained officers to deliver training and awareness for the prosecutors and judiciary throughout Türkiye about how electronic evidence from social media companies and multi-national service providers can be preserved and obtained for use in evidence. Such training should include awareness about reciprocity and explanations as to the futility of requesting material for some defamation cases (see paragraph 3g)

12. There needs to be specially trained police to deal sensitively with victims of cybercrime. At times this may also need to be gender specific.

2. Prosecutors & Judges

13. There remains a need for consideration to be given to establishing a centralised file system for investigations concerned with cybercrimes in different jurisdictions within the country;

14. There remains a need to implement guidelines and templates in order to enable faster communication between services, including requests for international exchanges from the Ministry of Justice to prosecutors;

15. Creating (career-related) incentives for Prosecutors & Judges to invest their time and energy on complex cybercrime cases and to ensure a lower turn-over of specialism.

16. Instead of using the number of completed cases as a measure for deciding on the promotion of Prosecutors & Judges, other criteria should be adopted in respect of cybercrime cases. Due to the complexity of cybercrime cases they should be rated or scored higher than other cases.

17. There should be regular review of training needs and ongoing in-service training efforts with regards to cybercrime. Cybercrime-related training should be an integral part of the standard pre-service training curriculum. There should be a comprehensive training strategy for Prosecutors & Judges. Every judiciary should be able to deal effectively with the evidential issues of cybercrime offences.

18. There should be a template for prosecutors to send evidence to the digital forensic specialists. The Ministry of Justice are in the process of developing such a template.

19. A weekly or monthly bulletin should be prepared that includes current and relevant case law which can be viewed on the National Judiciary Informatics System (UYAP) screen.

20. Mentorship initiatives (peer-to-peer) should be encouraged, especially in the context of high staff turn-over as this helps new members of staff.

21. There is a need to collect cybercrime statistics, there should be access to comprehensive statistics on not only cybercrime offending but also statistics on training.

22. All IT crimes that fall within the jurisdiction of the Criminal Courts of First Instance and the Assize Courts be tried by a single specialised court, or it can be provided in big cities that Assize Courts specialised on cybercrime will only deal with cybercrime cases thus eliminating the burden created by other crimes and ensuring a real specialisation.

23. There is a lack of knowledge on international cooperation in cybercrimes. For example, some Prosecutors and Judges are not aware of Budapest Convention mechanisms. Thus, trainings should be organised about the 24/7 points of contact.

24. Meetings similar to the coordination meetings should be held regularly to develop and support best practice. Prosecutors, judges, law enforcement officers, other relevant agencies and representatives from the private sector should be invited to attend.

3. Public and Private Cooperation

25. Sectoral capacity building efforts should be enchanced and harmonised regarding the fight against cybercrime at directly related sectors such as banking, telecomunication, digital services. Establishing and using umbrella organisations that can cooperate with judicial authorities should be considered if possible, and having clear and effective rules and guidelines on public-private cooperation must be provided on a sectoral basis

26. The electronic document management and Registered E-mail (Kayıtlı Elektronik Posta, KEP) application system should be used more effectively in correspondence between institutions. The GSM company representatives and private banks should be included in this system.

27. Article 61 of the Banking Law and the BRSA and its application should be re-evaluated for ensuring efficiency and success in blocking fraudulent transactions and accounts. Prosecutor's offices and banks should be able to act more rapidly with procedural safeguards.

28. IBAN and account information of the suspects should be made available to law enforcement, prosecution offices and/or courts through UYAP with adequate safeguards,

29. The conditions for issuing lines to foreigners at GSM operators should be made more difficult, and that effective identity validation systems should also be used for all digital finance services (e-money, digital payment etc.), cryptocurrency services, and other related digital services (i.e. e-commerce companies, online betting sites, etc.).

30. Using international legal cooperation mechanisms such as Budapest Convention more effectively, establishing better partnerships with social media companies and regulating more effective legal framework are crucial to gather cross-border digital evidence. Relevant hard law and soft law mechanisms should be re-evaluated with a multistakeholder perspective.

4. Digital Forensic Specialists & Legislation

31. There should be special procedures for the handling and disclosure of Child Sexual Abuse Material (CSAM). This will mean that the present legal requirement that where a suspect's computer has been seized and imaged, he must have the computer returned to him as soon as that process is complete, should not be applied in CSAM cases.

32. There is a need to amend the Criminal Procedure Code for making it much more comprehensive. A regulation that meets current problems such as searches in the cloud, while at the same time enabling evidence to be obtained from emerging technologies with a techno-neutral approach, should be introduced in a way that also includes all necessary procedural safeguards.

33. Article 134 of the Code of Criminal Procedure should be amended, especially with regard to the delivery of files containing images of child sexual abuse material to the suspect or defendant. This also impacts upon other matters such as where files containing cryptocurrency wallets, compromised data and much more are returned to the suspects as a requirement of this article.

34. Article 12/6 of the Code of Criminal Procedure should be clarified with an amendment to end jurisdictional conflicts between judicial authorities.

35. That legal regulations and an umbrella cybersecurity legislation should be prepared to require the reporting of cyber incidents in the public and private sectors.

36. There is a need to increase the legal basis for combating cybercrime in a manner that respects fundamental rights by regulating the legislation on the processing of personal data in public and law enforcement activities.

37. The use of ransomware should be defined as a newly introduced cybercrime.

38. Child online grooming (cyber servitude / online abuse) should be defined as a newly introduced cybercrimes.

39. An umbrella cybersecurity legislation should be regulated to require the reporting of cyber incidents in the public and private sectors.

40. A complete regulation that provides the legal basis for combating cybercrime in a manner that respects fundamental rights by regulating the legislation on the processing of personal data in public and law enforcement activities, is needed.

41. Protocol 2 of the Council of Europe Convention on Cybercrime (Budapest Convention) should be signed and transposed into domestic law.

5. Victims of Cybercrime

42. The need for Government led initiatives to raise public awareness of cybercrimes and how to safeguard oneself on the internet and other digital forums to avoid becoming a victim.

43. There should be awareness campaigns led by the Ministry of Education to educate children and young people on not falling prey to cybercrime activities. Children should also be taught about cyber-ethics. Prevention and awareness campaigns should be held in schools to build awareness of and prevent bullying, cyber-bullying, sextortion, and the repercussions of the circulation of child sexual abuse material.

44. The public must be aware of where and to whom cybercrimes should be reported; consider having a one-stop shop for reporting cybercrime.

45. Safeguarding the rights of victims and witness during court procedures, by allowing the use of screens where necessary and / or videoing the victims' evidence. This can include reporting restrictions and /or anonymity orders.

46. Formulating best practice in interacting with victims and witnesses from the investigation stage to its conclusion, such as keeping the victim informed throughout the journey of the case.

This Project is co-funded by the European Union and the Council of Europe.
Bu proje, Avrupa Birliği ve Avrupa Konseyi tarafından birlikte finanse edilmektedir.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

This Report was prepared under the scope of the European Union and the Council of Europe Joint Project on "Strengthening the Criminal Justice System and the Capacity of Justice Professionals on Prevention of the European Convention on Human Rights Violations in Türkiye".

This Project is co-funded by the European Union and the Council of Europe and implemented by the Council of Europe. The beneficiary institutions of the Project are the Ministry of Justice of the Republic of Türkiye and the Justice Academy of Türkiye. The contracting authority for this Project is Central Finance and Contracts Unit.

The Council of Europe is the continent's leading human right organisation. It includes 46 member states. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

T.C. HAZİNE VE MALİYE BAKANLIĞI CFCU MERKEZİ FİNANS ve İHALE BİRİMİ

TÜRKİYE CUMHURİYETİ ADALET BAKANLIĞI

TÜRKİYE ADALET AKADEMİSİ