Council of the
European Union

Brussels, 8 February 2017
(OR. en)

14583/1/16
REV 1 DCL 1

GENVAL 118
CYBER 131

DECLASSIFICATION

of document:	14583/1/16 REV 1 RESTREINT UE/EU RESTRICTED
dated:	31 January 2017
new status:	Public
Subject:	Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" - Report on Hungary

Delegations will find attached the declassified version of the above document.

The text of this document is identical to the previous version.

Council of the
European Union

Brussels, 31 January 2017
(OR. en)

14583/1/16
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 118
CYBER 131

REPORT

Subject:	Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" - Report on Hungary

ANNEX

1. EXECUTIVE SUMMARY

As a general remark the evaluation team would like to stress the courtesy and professionalism of the Hungarian authorities responsible for arranging the visit and their permanent willingness to improve support for the team and provide it with further information or clarifications.

The agenda for the on-site visits was well balanced and enabled the evaluation team to contact several of the most relevant players in the area of combating cybercrime.

The only downside to be mentioned was the absence of representatives from the banking sector, since it is likely that they would have relevant information to share regarding this sector's activity in preventing and countering cyber attacks and fraud through the internet.

Several presentations were made in order to inform the evaluation team about Hungary's experience in the area of fighting cybercrime, including an overview of the most relevant aspects of Hungarian substantive and procedural laws on cybercrime and the state of play of cyber security. The evaluation team also had the opportunity of listening to the perspective of both the law enforcement authorities and the judicial authorities regarding the obstacles and also the best practices and results achieved in this area.

As well as institutional contacts with the Hungarian authorities, two extremely interesting visits were organised to entities working in the area of awareness-raising on cyber matters:

- The first visit took place in a special institution for visually impaired children, where the evaluation team attended a project aimed at fostering teenagers' abilities to use the internet in the safest possible way;

- During the second visit – to Magic Valley (*Bűvösvölgy*) – the evaluation team had the opportunity to see Hungary's first media literacy and education centre.

Hungary appears to have made a genuine, proactive commitment to tackling the cyber threat as a priority over the last few years, with concrete efforts to update structures to bring them up to international standards.

The National Cyber Security Strategy is implemented by several actors: National Cyber Security Coordination Council, Cyber Security Forum (with private actors), cyber security working groups.

The governmental CERT (GovCERT) was created in 2013, and is operated 24/7 by 20 people. It deals with threat assessments, technical compliance, penetration testing, support for the development of reaction capacities and consultancies, for both the public and private sectors. It does not carry out traffic monitoring, intelligence activities, active defence or retaliation, or investigations.

Common statistical tools for all those involved in investigations exist at several levels (from the police forces, customs and financial services to the prosecution service). This effort is to be underlined as a good practice. The Hungarian authorities appear to be faced with weaknesses and shortcomings regarding the collection and presentation of statistical reports on cybercrime due to the fact that there is no designated authority to perform such tasks. During the evaluation, the police force presented its own statistics in the field of cybercrime.

The cooperation among different government authorities in the field of cybercrime is considered effective and the overall feedback is regarded as positive. However, the general impression given is that cooperation between the government and the public sector is in its early stages and further improvement is therefore needed.

There are no rules establishing specialised courts in cybercrime cases. District courts are, in general terms, competent to judge cybercrime cases, unless it is specified otherwise in the Code of Criminal Procedure.

The Hungarian prosecution service seems to have large capacities even in the field of investigations (investigation on its own, internal forensic support units). In 2014, the Hungarian justice authorities also developed a network of cyber magistrates for the Budapest area. The network, currently operating in the area of Budapest, works as a platform for continuous communication and consultation (via an email list), for sharing of information, expertise and good practices and for organising training sessions jointly with judges, police officers and tax and customs officers. This network is expected to be extended nationwide in the near future. Until then, the Hungarian justice authority plans to spread IT units (forensic support) all around the country.

The evaluation team considers that the setting up of a nationwide network of cybercrime prosecutors for the purposes of exchanging know-how and raising awareness in this area of criminality is a good practice that should be supported and fostered by the competent national authorities.

There are several forces and bodies dealing with law enforcement matters in Hungary. As a general rule, the law enforcement authorities dealing with investigations in the area of cybercrime come under the Ministry of the Interior (*BelügyMinisztérium*).

As to cybercrime, investigations are carried out, at a central level, by the NBI - National Bureau of Investigation, a High–Tech Crime Unit established in 2007 within the Riot Police (KR) of the Security Directorate.

The Hungarian legal framework in the area of cybercrime was established according to the principles and benchmarks laid down in the Council of Europe Convention on Cybercrime (the Budapest Convention) and Directive 2013/40/EU on attacks against information systems (the Cybercrime Directive (2013)). Hungary has transposed into national law Directive 2011/93/EU on combating sexual abuse and sexual exploitation of children and child pornography. However, Hungary has not yet ratified the additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

Regarding the investigation of child exploitation cases, the team noted that there is no dedicated database and/or specialised software to host, maintain and categorise material relating to child abuse. Moreover, the connection with the ICSE database was made very recently, and thus there is a need to ensure that more trained police officers can use the database. Furthermore, it was noted that there is a clear need for capacity improvement that will allow for a more effective proactive approach in the area of fighting child sexual abuse via the internet, such as the implementation of P2P monitoring software. Furthermore, it was noted that since they have recently been connected to the ICSE database, there is a need to improve and speed up the uploading to the database of material relating to child abuse in order to facilitate identification of the victims.

On the governmental level, public awareness actions seem to be effective. There is a specialised department within the governmental sector which is responsible for the policy related to cybercrime awareness and more specifically for the preparation of awareness material and its effective distribution. The establishment of such an institution could serve as an example to other Member States.

2. INTRODUCTION

Following the adoption of Joint Action 97/827/JHA of 5 December 1997[1], a mechanism was established for evaluating the application and implementation at national level of international undertakings in the fight against organised crime. In line with Article 2 of the Joint Action, the Working Party on General Matters including Evaluations (GENVAL) decided on 3 October 2013 that the seventh round of mutual evaluations should be devoted to the practical implementation and operation of the European police forces on preventing and combating cybercrime.

The choice of cybercrime as the subject for the Seventh Mutual Evaluation Round was welcomed by Member States. However, due to the broad range of offences which are covered by the term cybercrime, it was agreed that the evaluation would focus on those offences which Member States felt warranted particular attention. To this end, the evaluation covers three specific areas: cyber attacks, child sexual abuse/pornography online and online card fraud, and should provide a comprehensive examination of the legal and operational aspects of tackling cybercrime, cross-border cooperation and cooperation with relevant EU agencies. Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography[2] (transposition date 18 December 2013) and Directive 2013/40/EU[3] on attacks against information systems (transposition date 4 September 2015) are particularly relevant in this context.

1 Joint Action of 5 December 1997 (97/827/JHA), OJ L 344, 15.12.1997 pp. 7 - 9.
2 OJ L 335, 17.12.2011, p. 1.
3 OJ L 218, 14.8.2013, p. 8.

Moreover, the Council Conclusions of June 2013[4] on the EU Cybersecurity Strategy reiterate the objective of ratifying the Council of Europe Convention on Cybercrime (the Budapest Convention)[5] of 23 November 2001 as soon as possible and emphasise in their preamble that 'the EU does not call for the creation of new international legal instruments for cyber issues'. This Convention is supplemented by a Protocol on Xenophobia and Racism committed through computer systems.[6]

Experience from past evaluations shows that Member States will be at different stages of implementation of the relevant legal instruments, and the current process of evaluation could also provide useful input to Member States that may not have implemented all aspects of the various instruments. Nonetheless, the evaluation aims to be broad and interdisciplinary, focusing not only on the implementation of various instruments relating to fighting cybercrime but also on the operational aspects in the Member States.

Therefore, apart from cooperation with the prosecution services, it will also encompass how police authorities cooperate with Eurojust, ENISA and Europol/EC3 and how feedback from the given actors is channelled to the appropriate police and social services. The evaluation focuses on implementing national policies with regard to stopping cyber attacks and fraud as well as child pornography. The evaluation also covers operational practices in the Member States with regard to international cooperation and the support offered to those who fall victims of cybercrime.

The order of visits to the Member States was adopted by GENVAL on 1 April 2014. Hungary was the (nineteenth) Member State to be evaluated during this round of evaluations. In accordance with Article 3 of the Joint Action, the Presidency has drawn up a list of experts for the evaluations to be carried out. Member States have nominated experts with substantial practical knowledge in the field pursuant to a written request to delegations on 28 January 2014 made by the Chairman of GENVAL.

4 12109/13 POLGEN 138 JAI 612 TELECOM 194 PROCIV 88 CSC 69 CIS 14 RELEX 633 JAIEX 55 RECH 338 COMPET 554 IND 204 COTER 85 ENFOPOL 232 DROIPEN 87 CYBER 15 COPS 276 POLMIL 39 COSI 93 DATAPROTECT 94.

5 CETS No 185; opened for signature on 23 November 2001, entered into force on 1 July 2004.

6 CETS No 189; opened for signature on 28 January 2003, entered into force on 1 March 2006.

The evaluation teams consist of three national experts, supported by two staff from the General Secretariat of the Council and observers. For the seventh round of mutual evaluations, GENVAL agreed with the proposal from the Presidency that the European Commission, Eurojust, ENISA and Europol/EC3 should be invited as observers.

The experts charged with undertaking the evaluation of Hungary were Mr Andreas Anastasiades (Cyprus), Mr Emmanuel Kessler (France) and Mr Lyubomir Tulev (Bulgaria). One observer was also present: Mr José Eduardo Guerra (Eurojust), together with Ms Carmen Necula from the General Secretariat of the Council.

This report was prepared by the expert team with the assistance of the General Secretariat of the Council, based on findings arising from the evaluation visit that took place in Hungary between 7 and 11 March 2016, and on Hungary's detailed replies to the evaluation questionnaire together with its detailed answers to ensuing follow-up questions.

3. GENERAL MATTERS AND STRUCTURES

3.1. National cyber security strategy

The Hungarian Government adopted two strategic documents in 2012 and 2013:

- Government Decision No 1035/2012 (21 February) on Hungary's National Security Strategy (the full document can be found in Annex I in English);

- Government Decision No 1139/2013 (21 March) on Hungary's National Cyber Security Strategy (the full document can be found in Annex II).

Both documents were drafted bearing in mind the international examples and the importance of international involvement as well as the trends and challenges, so they provide a suitable strategic framework for domestic cooperation and coordination as well as for international cooperation (primarily within the framework of UN, NATO, EU, Council of Europe). These strategic documents attach great importance to the issue of cyber security and discuss the action to be taken against cybercrime, focusing on the tasks of guaranteeing a secure online environment.

Hungary's National Security Strategy describes cyber security as follows:

'The functioning of the state and society, our economy, public administration, and national defence as well as numerous other realms, is increasingly built on information technologies. Hungary will have to face increasingly pressing and intricate challenges in the physical and virtual space of IT and telecommunications networks and related critical infrastructure.

The unhindered proliferation of the results of scientific and technological development and their potential malicious use by state or non-state actors, and even terrorist groups, to interfere with the normal operation of IT and communications systems and core governmental networks constitutes an additional threat. It is often difficult to identify the origin of and motivation behind such attacks. Hungary must be ready to manage risks and threats related to national security, defence, the fight against crime, as well as disaster-prevention, which are gaining in prominence in cyberspace across the globe, as well as to guarantee an adequate level of cyber security, perform the tasks related to cyber defence, and secure the operation of critical national infrastructure.

a) It is a primary task to systematically identify and prioritise actual or potential threats and risks in cyberspace, to strengthen governmental coordination, to increase societal awareness, and to capitalise on opportunities provided by international cooperation.

b) In addition to strengthening the protection of the critical national information infrastructure, Hungary strives to enhance the security of information systems and to participate in the development of appropriate levels of cyber defence in cooperation with allies and fellow EU members.'

Hungary's **National Cyber Security Strategy** reflects the basic values enshrined in the Fundamental Law of Hungary, specifically freedom, security, rule of law, international and European cooperation, in a separate field within security and economic policy; it is a document of cyber security for national data assets as part of national assets, derived from Section 38 of the Fundamental Law, as well as for the related critical infrastructures.

In accordance with the Hungarian National Security Strategy, adopted by Government Decision No 1035/2012 (21 February), and based thereon, the Strategy elaborates the government efforts and responsibility laid down in Section 31 thereof. Its roots date back to the Budapest Convention adopted in 2001 ('Convention on Cybercrime'); an international agreement defining internationally recognised principles used as a reference. At the same time, the Strategy is in conformity with the recommendations of the European Parliament for the Member States included in Decision No 2012/2096 (INI) on cyber security and defence, adopted on 22 November 2012, and with the joint communication published by the European Commission and the High Representative of the Common Foreign and Security Policy of the European Union on 7 February 2013 under the title 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace'. Furthermore, the Strategy is in line with NATO's Strategic Concept adopted in November 2010, NATO's Cyber Security Policy adopted in June 2011 and its implementation plan, as well as the cyber protection principles and objectives set out in the documents of the NATO summits held on 19-20 November 2010 in Lisbon and on 20-21 May 2012 in Chicago.

Regarding good practices in combating cybercrime, attention should be drawn to the good cooperation with the civil and private sphere – a key factor in effective actions – which has led to a significant reduction in the volume of internet piracy and misuse of intellectual property. Due to the successful identification of perpetrators and the collection of internet data and evidence, many successful criminal cases have been conducted. These results received wide publicity, so the number of voluntary withdrawals has increased.

The evaluation team reached the following conclusions:

The Hungarian National Cyber Security Strategy is defined in two main documents:

– Government Decision No 1035/2012 (21 February) on Hungary's National Security Strategy;

and

– Government Decision No 1139/2013 (21 March) on Hungary's National Cyber Security Strategy.

According to this last document, the Hungarian cyber security strategy '*aims at developing a free and secure cyberspace and protecting national sovereignty in the national and international context, which has undergone a significant change due to the emergence of the cyberspace, a new medium which has become a key factor in the 21st century. Furthermore, it aims at protecting the activities and guaranteeing the security of national economy and society, securely adapting technological innovations to facilitate economic growth, and establishing international cooperation in this regard in line with Hungary's national interests.*'
(https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/HU_NCSS.pdf)

In the same Decision, the government instructs the state secretary heading the Prime Minister's Office '*to prepare a work and action plan for implementing the tasks defined in the National Cyber Security Strategy of Hungary.*' However, the whole government is involved in matters of cyber security, namely the Ministries of the Interior, Justice, Foreign Affairs and Trade, National Development, National Economy and Human Capacities.

Public authorities and experts work together in a complex network - the National Security System of Hungary - composed of the following entities and working groups:

- National Cyber Security Coordination Council, chaired by the Minister of the Interior. The Council has a Deputy Chair (Cyber Coordinator) and has among its members one delegate per ministry.
- Cyber Security Forum, devoted to cooperation with non-governmental actors (business, academia, NGOs);
- Cyber Security Working Groups (senior expert level, for instance, CERTs, e-Government, internal security)

a) incident management,

b) internal security,

c) electronic public administration,

d) energy,

e) child protection.

In addition to those bodies and public entities, whose role is more strategy-oriented, the National Cyber Security Centre is also involved, on an operational level, in ensuring the security of information systems.

The National Cyber Security Centre includes GovCERT and the NEISA (National Electronic Information Security Authority), a public body responsible for the supervision of security of information systems. Furthermore, the NEISA ensures the compliance of electronic information systems with the relevant security requirements.

– CERTs:

• There are several CERTs in Hungary:

  – the Government Incident Handling Centre (GovCERT-Hungary, operated by the National Cyber Security Centre, is a vulnerability assessment service for government agencies. It also provides security training for government IT staff)
  – CIP CERT (operated by the Directorate-General for National Catastrophe Management)
  – specialised CERTs, e.g. MilCERT (MoD) and IntCERT (Ministry of Justice), Media and Telecom Regulator

The cyber security system in Hungary seems to be complex and communication between the different actors with a role to play in this area is not always smooth and effective.

The flow of communication and the exchange of information between the CERTs and the law enforcement authorities could be improved in order to better prevent and fight cybercrime.

The Republic of Hungary has clearly defined its national priorities with regard to handling cybercrime and cyber security. The priorities are clearly described in the documents mentioned above and cover issues such as cyber defence, cyber security, cybercrime, awareness-raising and training. Moreover, the priorities of the police are clearly defined in a certain document and cover operational aspects, training needs, improvements on hardware and software, awareness and safety.

The Hungarian National CERT acts as the centralised point of coordination, cooperation, information sharing and statistical registration of cyber security incidents. The current structure of the CERT seems to work effectively and the general impression is positive. However, it seems that a more coordinated approach between the CERT and LEAs is needed in the field of information sharing between the two authorities. The team also noted that the governmental institutions do not have a legal obligation to report cyber attacks to the CERT.

The evaluation team considers that GovCERT should be encouraged to report as more as possible the relevant cyber incidents to law enforcement.

3.2. National priorities with regard to cybercrime

According to the National Cyber Security Strategy, Hungary's set of values, vision and objectives relating to cyber security are the following:

'6. The protection of Hungary's sovereignty in the Hungarian cyberspace is a national interest, too; a free, democratic and secure functioning of the Hungarian cyberspace based on the rule of law is regarded as a fundamental value and interest. In Hungary, the freedom and security of cyberspace is ensured through the close cooperation and coordinated activities between Government, academia, business sector and civil society based on their shared responsibility.

7. Hungary aims at establishing and maintaining trust-based cooperation with all public and private actors of the global cyberspace sharing the same set of values with Hungary, and endeavours to guarantee free and secure use of the global cyberspace through its allies and international relations, particularly the EU and the NATO, the Organization on Security and Cooperation in Europe (OSCE), the United Nations, the Council of Europe and other international organisations in which the country is a member. Being aware of the fact that threats and attacks emerging in cyberspace may escalate to the level requiring allied cooperation, Hungary considers it highly important that cybersecurity has become an issue for collective defence under Article 5 of the founding treaty of NATO. Hungary is interested in this allied international cooperation for the sake of its own security, too. Hungary regards the Central and Eastern European region with special attention, where cybersecurity can be further improved within the framework of regional cooperation

8. To address present and future challenges, Hungary lays down the requirement that the Hungarian cyberspace shall provide a secure and reliable environment:

a) for individuals and communities to ensure social development and integration through communication based on liberty, freedom from fear, and guaranteeing the protection of personal data,

b) for the business sector to develop efficient and innovative business solutions,

c) for future generations to ensure value-based learning and unharmed collection of experiences resulting in a sound mental development,

d) for electronic public administration, to promote innovative and cutting-edge development of public services.

9. In the interest of a free and secure use of cyberspace, Hungary lays downs the following objectives to be met by aligning the interests of national security, efficient crisis management and user protection:

a) to have efficient capabilities to prevent, detect, manage (react), respond to and recover any malicious cyber activity, threat, attack or emergency, as well as accidental information leakage,

b) to provide adequate protection for its national data assets, to ensure the operational safety of the parts of its critical infrastructures linked to cyberspace, and to have a rapid, efficient mitigating and recovery capability in case of a compromise, deployable also during a state of emergency,

c) to ensure that the quality of IT and communication products and services for the secure operation of the Hungarian cyberspace meet the requirements of international best practices, with special emphasis on compliance with international security certification standards,

d) to ensure that the quality of education, training as well as research and development meets the requirements of international best practices, thus contributing to the establishment of a world-class national knowledge pool,

e) to ensure that the establishment of a secure cyberspace for children and future generations meets the requirements of international best practices.'

3.3. Statistics on cybercrime

3.3.1. Main trends leading to cybercrime

The largest amount of damage is caused by crimes against intellectual property rights and cybercrimes relating to the financial sphere. Other typical crimes come under the category of 'Breach of Information System or Data' and 'Information System Fraud'.

3.3.2. Number of registered cases of cybercrime

As far as criminal statistics are concerned, the investigating authorities (police) and the public prosecutor's office collect data in a unified system; however, data collection by the courts is carried out separately from this system. These databases are not integrated, so the whole criminal procedure cannot be tracked in one single statistical system.

The **Unified System of Criminal Statistics of Investigating Authorities and of Public Prosecution (hereinafter referred to as 'ENYÜBS')** is a criminal justice database which is maintained effectively by the Ministry of the Interior, under the joint responsibility of the Ministry of the Interior and the Office of the Prosecutor General.

The ENYÜBS system contains data on criminal proceedings initiated and conducted by the police, the National Tax and Customs Administration (hereinafter 'the NTCA') and the public prosecution service, in addition to data collected during the prosecution phase of the proceedings. In line with this, the ENYÜBS system follows a given case from the reporting of the crime (i.e. making the complaint) until the prosecution (indictment) phase. However, it does not contain data about the court proceedings and the number of convictions.

The ENYÜBS system also includes the number of criminal reports (complaints), criminal offences and completed investigations, as well as the number of perpetrators, accused persons and victims. The latter data collection covers sex, age, citizenship, occupation, reference data on possible alcohol or drug influence and the type of relationship between the victim and the perpetrator. The ENYÜBS system is regulated by a ministerial decree (Decree No 12/2011 of the Minister of the Interior). There is a public website where the data can be seen (https://bsr.bm.hu/SitePages/Nyitolap.aspx); however, it is available only in Hungarian.

As part of the statistical activities of the courts, the grounds of these activities are regulated in Act XLVI of 1993 on statistics and in its implementing decree **(**Government Decree No 170/1993). In the framework of these activities the task of the courts is to provide a real, fair and objective picture on the caseload and workload of the courts (including the received, completed and pending cases) and, for this purpose, to collect data by statistical methods, as well as processing, storing, analysing, providing, disseminating and publishing them.

The National Office for the Judiciary collects the detailed statistics of criminal cases with final judgments in 'CdFk' pages/forms regarding the convicted persons from the courts of first and second instance where the final judgment was passed. The data are provided exclusively by the courts; other external bodies, institutions or the private sector do not participate in the data collection. These data are available for the public on the webpage of the National Office for the Judiciary (http://birosag.hu/kozerdeku-informaciok/statisztikai-adatok/orszagos-statisztikai-adatok). As mentioned above, they are separate from the statistics of law enforcement (investigating) authorities.

The collection of statistical data on cybercrimes is in accordance with the general rules as described above; there are no specific regulations thereon.

The private sector collects data exclusively about its own activities, and it can contribute to national data provision primarily in the area of cyber security.

CRIME STATISTICS	2013	2014	2015
Information System Fraud	249	1 389	2 175
Breach of Information System or Data	51	344	448
Compromising or Defrauding the Integrity of the Computer Protection System or Device	6	26	15
Illicit Access to Data	6	26	22
Criminal Conduct for Breaching Computer Systems and Computer Data (old)	769	200	64

TOOLS TO COMMIT CYBERCRIMES	2013-2015
Email	55
Internet	663
Malware	38
Decoder application	60
Hardware	258
Software	310

3.4. Domestic budget allocated to prevent and fight cybercrime, and support from EU funding

Allocations for the prevention of and fight against cybercrime appear in the budget of the concerned bodies and in the form of grants/subsidies, rather than dedicated sources in separate lines of the national budget. There are also EU funds currently contributing to the financing. However, the importance of the Internal Security Fund, especially for law enforcement activities, should be highlighted. The Hungarian national programme related to the Internal Security Fund reflects the emphasis on both the prevention of and fight against cybercrime, including the protection of critical infrastructures. The decision-makers allocated resources for the planned activities.

There is no dedicated budget within the police and/or government for raising awareness in the area of cybercrime and cyber security. However, there are funds available for this purpose within the general police budget. Moreover, it seems that no application was made for grants from EU funds for awareness-raising activities. The weaknesses in applying for EU funds in the field of cybercrime awareness are directly linked to the less effective cooperation between NGOs and the governmental sector.

It seems that there is a need for more regular cooperation between the private sector (telecommunications companies, banks and ISPs) and the governmental sector, mainly by organising and running prevention campaigns for small and medium companies regarding cyber security.

Moreover, the team noted that there is a lack of effective cooperation between NGOs and the governmental sector with regard to applying and granting European funds to raise awareness in the field of cybercrime and cyber security.

3.5. Conclusions

- According to European studies and national assessments, the threat level is felt to be fairly low. This perception is based on many different factors, such as the more recent development of the internet in Hungary (the equipment level in the population of 10 million is about 75 % for the internet and 50 % for Facebook.), the specificity of the language and also a loss of reports (confirmed by the National Cyber Security Centre and the banking sector).
- In spite of this, it seems clear that cyber threats have risen in the last few years, against companies which work closely with German companies and also against political authorities (anonymous groups in 2012, activists on migration issues).
- Since 2013, the Hungarian authorities have taken firmer action by reforming laws, developing structures (police forces) and tasking the Ministry of the Interior with a broad coordination role with a centralised approach.
- Hungary, which implements voluntary policies, currently enjoys real advantages, primarily through easier coordination of the various internet actors, mainly based in the capital which remains the laboratory of reforms.
- Hungary appears to have made a genuine, proactive commitment to tackling the cyber threat as a priority over the last few years, with concrete efforts to update structures to bring them up to many international standards.
- The National Cyber Security Strategy is implemented by all relevant actors: the National Cyber Security Coordination Council, the Cyber Security Forum (with private actors), Cyber Security Working Groups. The Hungarian Government has implemented two cybercrime strategies through two government decisions which cover the field of cyber security, cyber defence, cyber awareness, training issues and response to cyber attacks. For the time being this structure seems to be working efficiently. The cyberspace protection policy of the Republic of Hungary is the newest document in the field of cyber security and falls under the effective administration of the Ministry of the Interior. These strategic documents attach great importance to the issue of cyber security and discuss the action to be taken against cybercrime, focusing on the tasks of guaranteeing a secure online environment.

- In 2012, coordination was strengthened, resulting in a broad strategy in 2013 (IT Security Law, Act 50/2013 for vital actors and administrations). The IT security law was reformed in 2015, with the Ministry of the Interior leading all the general organisation at strategic and operational levels with the governmental CERT.
- The governmental CERT (GovCERT) was created in 2013, and is operated 24/7 by 20 people. It deals with threat assessments, technical compliance, penetration testing, support for the development of reaction capacities, and consultancies, for both the public and private sectors. It does not carry out traffic monitoring, intelligence activities, active defence or retaliation, or investigations.
- In 2016, the objectives will be to implement the NIS Directive and develop an early warning system.
- Reporting of attacks to national authorities is compulsory, although implementation still needs to be maximised.
- Common statistical tools for all those involved in investigations exist at several levels (from the police forces, customs and financial services to the prosecution service). This effort is to be underlined as a good practice. The Hungarian authorities appear to be faced with weaknesses and shortcomings regarding the collection and presentation of statistical reports on cybercrime due to the fact that there is no single authority responsible for performing such tasks. During the evaluation, the police force presented its own statistics in the field of cybercrime. However, no statistical reports were presented from the police districts.
- Although there is no dedicated budget for preventing and fighting cybercrime, the Hungarian prosecution service spends EUR 891 000 each year on IT equipment (out of a global budget of EUR 123 million, for 8 426 civil servants working in this service).
- There is a need for more regular cooperation with the private sector (telecommunications companies, banks and ISPs), mainly by organising and running prevention campaigns for small and medium companies regarding cyber security.

4. NATIONAL STRUCTURES

4.1. Judiciary (prosecutions and courts)

4.1.1. Internal structure

Taking into account the result of the Hungarian EU Presidency in 2011 and the Conference on Cyberspace held in Budapest in 2012, government coordination of actions against cybercrime and cyber threats was significantly stepped up. The previous ad hoc structures were replaced by an institutional framework which sought to facilitate effective cooperation between sectors of different interests and functions by involving all concerned stakeholders. By now this structure has also gone through a notable transformation and it can be said that most related competences and responsibilities are concentrated at the Ministry of the Interior and its subordinate bodies; however, the basic institutional framework established by the Government Decree described in detail below has remained the same.

Government Decree No 484/2013 (XII. 17) on the rules on the establishment and operation of the **National Cyber Security Coordination Council**, the **Cyber Security Forum** and the **sectoral cyber security working groups**, and their related competences and responsibilities.

There is no specialised prosecution service or court in the Hungarian judicial system for cybercrime. When appointing the judges/prosecutors acting in a specific case, professionals with the most experience in the field of cybercrime are selected to pursue such cases.

The court is competent to decide on the question of criminal liability as well as on the status of property that was seized and any other measures that were taken during the criminal procedure.

Article 25 of the Fundamental Law declares that Hungary has a multi-level system of courts, which is further defined by Act No CLXI of 2011 on the system and administration of courts.

Article 16 of the latter act defines the list of acting courts as follows:

a) Curia

b) regional courts of appeal

c) regional courts

d) district courts

e) administrative and labour courts.

Neither the Fundamental Law nor Act No CLXI of 2011 on the system and administration of courts establishes specialised courts for acting in cybercrime cases. District courts may proceed in cybercrime cases, except for those listed in the CPA, which fall under the competency of the regional courts.

Criminal act	Referring rules of CC	CPA rule that refers crime to the competency of Regional Court
The information system fraud results in damage of particularly substantial value. Any person who causes damage by using a counterfeit or forged, or unlawfully obtained electronic payment instrument, or by accepting payment with such payment instrument.	CC Article 375 paragraph (4) point (a) and paragraph (5)	CPA Article 16 paragraph (1) point (r)
Acts of terrorism	CC Articles 314 - 316	CPA Article 16 paragraph (1) point (n)
Criminal Offences involving Classified Information	CC Article 265 paragraphs (2) and (3)	CPA Article 16 paragraph (1) point (i)
Criminal Offences Against Public Records and Registers Recognised as National Assets	CC Article 267 paragraphs (1) and (2)	CPA Article 16 paragraph (1) point (i)
If the infringement of copyright or certain rights related to copyright results in particularly substantial financial loss	CC Article 385 paragraph (4) point (c)	CPA Article 16 paragraph (1) point (s)

In Hungary, district courts may act in many cases of cybercrime. These are local courts operating in the place where the regional court has its seat.

According to Article 17 paragraph (6) of the CPA

Abuse of nuclear materials (Section 264 of the Penal Code), abuse of the operation of nuclear facilities (Section 264/A of the Penal Code), abuse of the application of nuclear energy (Section 264/B of the Penal Code) and economic crimes (Chapter XVII of the Penal Code) – not including the violation of accounting regulations (Section 289 of the Penal Code) and financial offences (Title III of Chapter XVII of the Penal Code) – shall fall under the jurisdiction of the local court located at the seat of the county court or within the geographical jurisdiction of the Metropolitan Court and the Pest Central District Court. The jurisdiction of these courts in respect of such criminal offences shall extend to the territory of the county or Budapest, respectively.

If the cybercrime committed does not fall under the jurisdiction of one of the courts specified above, the place where the crime was committed establishes the jurisdiction of the acting court and prosecution service according to the general rules.

Hungary has 20 regional courts.

Budapest is the seat of the regional court of Pest county (the county including Budapest), which is called the Budapest Environs Regional Court. There is also a central district court, namely the Buda Environs District Court located in Budapest. There is also one district court in the territory of each regional court, bearing the name of the place where they have their seat, e.g. District Court of Kaposvár.

Decisions made by the district courts may be appealed at regional courts as courts of second instance. If the decision of the second instance court contradicts that of the district court (e.g. when the accused was first acquitted by the district court then convicted by the regional court), there is a third instance to appeal to (Regional Court of Appeal).

In definite cases that are punishable with a longer term of imprisonment and in cases of more serious concern that are listed by the law, regional courts may act at first instance. Sentences handed down by the regional court as first instance judgments may be appealed at the regional court of appeal. An act adjudicated by a final judgement of a court may be subject to re-trial if new facts or circumstances emerge that were not examined before, while if the law was not applied properly by the court, a motion for review may be submitted to the Curia, which is the highest instance in the criminal procedure.

As judges assigned to the district courts located at the seat of the regional courts have exclusive competence to act in many types of cybercrime cases committed in the territory of the specific county, they obtain sufficient knowledge and experience of the approach to be taken to these cases and of how to consider electronic evidence.

According to Article 30 paragraph (1), the competence and jurisdiction of the prosecutor's office shall depend on the competence and jurisdiction of the court where it operates. The organisation of the prosecutor's office shall be determined by the Prosecutor General pursuant to the relevant law.

As the competence of the prosecution service matches that of the court, prosecutors assigned to the district prosecutor's office operating in the territory of a regional court also have exclusive competence in the listed cases involving cybercrime.

Both prosecution and judiciary services fall within the administration of the Ministry of Justice. There are no dedicated judges dealing exclusively with cybercrime cases. However, on a practical level, judges who are familiar with cybercrime issues are usually appointed to deal with cases of this type, at least as regards the serious cases. At the prosecution level, there are designated prosecutors in the Prosecutor General's service as well as coordinating prosecutors at regional level for cybercrime cases.

The prosecution service is well structured and works effectively in overseeing investigations and prosecuting cybercrime. They have a dedicated budget for training and equipment and within this framework many training sessions are organised that cover the training needs of prosecutors, judges and police officers.

4.1.2. Capacity for and obstacles to successful prosecution

District courts and prosecutors act solely in cybercrime cases. So far, these district courts and prosecutors' offices have not experienced any problems with the workload in cybercrime cases which would cause difficulties in the proceedings.

While strengthening capacities are the main task, it is also important to organise training courses to maintain an adequate level of knowledge and experience among staff to offset the changes in the staff of courts and prosecutors' offices.

Both the prosecutor’s offices and the courts organise such training courses in order to be able to recognise acts which constitute a criminal offence and to improve judicial practice and accelerate legal unification concerning the evaluation of electronic evidence.

The National Office for the Judiciary places particular emphasis on vocational training for judges and court clerks.

Usually there are no eye witnesses of the crimes committed using information systems, and the system does not keep any direct information which is enough on its own to pinpoint the identity of the perpetrator. When the system is being used by several persons, the identification of the perpetrator is difficult, and finding enough evidence that proves his or her guilt against a testimony where he or she denies the commission of the crime is also hard.

Wireless internet access (WiFi) has become a common method for getting onto the internet, which can be exploited by perpetrators, as they tend to use the internet access of others to hide their identity when committing a crime. As this is a real possibility, it is an easy excuse enabling a suspect to counter the suspicion of crime by announcing that perhaps an unknown person used their internet access, rather than the suspect themself being the person who committed the crime. This forces the investigating authority to try to find evidence to check this possibility. But sometimes this can cause difficulties on its own if it is impossible to rule out such an unknown and illegal access to the system.

If traces of the committed crime are stored on the system of a service provider outside the country, the information can be obtained only by sending a letter rogatory, which can prolong the procedure. Furthermore, sometimes the request is not even answered.

According to the Hungarian authorities even if service providers are cooperative, it is not always possible to obtain results, as the data on internet traffic can be overwritten very fast in the log files. This can render an international letter rogatory useless, as it is too slow from the beginning.

There are difficulties even when trying to request information from providers in other countries, especially from providers in the USA. This is usually in connection with cases of defamation and libel instituted by private accusers.

It is almost impossible to get information from Facebook, Twitter, Tumblr or Google, as these companies do not have any representatives in Hungary who are entitled to answer requests. Also, according to transparency reports, these companies do not give out information if the requesting party is not a government official.

Some pages (like Facebook) offer the possibility of filling out an online form to request data, but this mainly works with authorities in the USA (although authorities of other countries are not expressly excluded from this opportunity.)

Sometimes there are cases where a service provider can be reached via email. The problem with such cases lies in the identification of the requesting party, as it is not possible to prove the legality of the request with a Hungarian email address and phone number.

While filling out this questionnaire, the judges involved did not make any such requests, as they tried to find other pieces of evidence when the need arose.

When the perpetrators use methods to hide the originating IP address (with proxy server, TOR browser, IP-spoofing, etc.), difficulties arise in identifying the place where the crime was committed, the equipment which was used and the person who committed the crime.

Difficulties in identifying the perpetrator and proving their guilt with regard to a relevant case

Between June 2007 and 10 August 2007, an unknown perpetrator illegally accessed the CISCO 5300 AS type device of a Hungarian internet service provider on several occasions. The accesses were made with IP addresses originating from Venezuela and Mexico.

The company provided a VoIP service to its customers with the named device, which let them initiate phone calls via their internet access. In these cases the outgoing call to the network of the phone providers originated from the company's device.

The illegal access method was possible because of a security leak. The company had configured an H.323 protocol to prevent any illegal access, but they were not aware of the SYP protocol, which was a default factory configuration already present on the CISCO device. The company did not create any security measures to prevent illegal use through this protocol.

After the illegal accesses, the unknown perpetrator initiated 240 000 phone calls via the CISCO device. Most of the time they called phone numbers which were connected to a company situated in Lichtenstein, and were leased to seven other companies before the crime. The other companies were situated in Lichtenstein, Germany, Gibraltar, USA, Cyprus, the Seychelles and France.

These companies provided pay services on the phone numbers and also leased these numbers to other international companies in such a way that every company benefited from the price being paid for the calls. The method of these 'pay-by-phone' services was to give a specific password to the calling party after a time of waiting. A further rule was that the calling party could not know how long they were required to wait. In this system, the most popular call number gave the password after six minutes of waiting and repeated it after another seven minutes.

The victim company providing the possibility to call via its device received a phone bill of HUF 31 265 700 (about EUR 99 000) after the calls made by the perpetrator.

The passwords given on the called numbers could be used for services in English, Farsi, Arabic, Nepalese, German and Chinese. There was also a password to a called phone number which provided other services for customers of satellite channels in the region of North Africa and the Middle East.

The beneficiary companies of the calls – as was discovered following a data request sent via Interpol to Lichtenstein – were organised into a pyramid structure: two companies were located in Lichtenstein, another six were located in different countries (Germany, Gibraltar, USA, Cyprus, the Seychelles, France), and it was not known where the other 36 beneficiary companies were located.

There was no connection between the victim company and the perpetrator; it looked as if the perpetrator was running an automated search on the internet for possible victims vulnerable to this specific type of attack, and when one was found, the perpetrator exploited the leak to initiate the premium rate calls to benefit from the money paid for the bill which he or she had caused. Still, this suspicion could not be proven, as there was no hope of finding the perpetrator through the used IP addresses, and the letter rogatory was too slow to process with any hope of success.

One of the reasons for this was that the company reported the case only after the phone bill arrived.

The other problem was with the beneficiaries who were located in several countries, and without enough evidence it could not be proved that they had any connection to the fraudulent calls.

This case clearly shows that the methods used to hide the origin IP address, exploit known system vulnerabilities and organise a structure of smartly founded companies can result in an efficient model for committing a crime which is impossible to investigate from any of the countries involved. Also, a Joint Investigation Team containing 36 countries could cost a lot more than the damage caused by the original crime, and moreover would have a low probability of success.

4.2. Law enforcement authorities

In relation to cybercrimes there are shared responsibilities between the police and the National Tax and Customs Authority.

Since the Hungarian police has general jurisdiction for any kind of investigation, the central, county and local police departments also take part in the fight against cybercrime. In general, the local and county police forces carry out the investigations in simple cases, while in more important and/or international cases, possibly even involving organised crime, the specialised units of the Riot Police's National Bureau of Investigation carry out the criminal proceedings.

The Corruption and Economic Crime Unit of the National Police Headquarters coordinates the police's cybercrime investigations. The High-Tech Crime Unit in the Corruption and Economic Crime Division of the Riot Police's National Bureau of Investigation and the Money Forgery and Payment Card Fraud Unit in the Intelligence Division of the Riot Police's National Bureau of Investigation take an active part in this coordination.

The National Police Department Crime Prevention Unit coordinates the police's cybercrime prevention activity, in which the county police forces and the Budapest Police Department Crime Prevention Unit take an active part.

Several criminal offences falling within the competence of the NTCA, as defined in the law on Criminal Procedures, are in practice committed by means of the internet or IT systems.

The Department of Central Investigations of the NTCA's DG for Criminal Affairs conducts the investigation if the offence is committed in criminal association with accomplices and the committed value exceeds HUF 1 billion, and in cases which give cause for serious concern. The Department has different divisions dealing with special tasks, such as the Crime Analysis Division or the Information Technology Division (the latter is referred to hereinafter as 'the IT Division').

Of course, the regional criminal directorates are also involved in detecting and investigating activities related to criminal offences committed through the internet or IT systems which fall within their competence. The IT Division also regularly receives requests to provide IT support in such cases.

Within the organisation, the specialised unit for the fight against cybercrime is the High-Tech Crime Unit in the Corruption and Economic Crime Division of the Riot Police's National Bureau of Investigation. The Unit's activities extend to exploration and investigation of the more important and internationally related cybercrimes (e.g. offences against information systems, online payment fraud, internet fraud, international botnet networks, online child sexual exploitation, etc.).

Exclusive competence for named crimes belongs to the Riot Police's National Bureau of Investigation, and hence to the Unit: Act C of 2012 on Article 375 of the Hungarian Criminal Code (CC): the information system fraud involves a particularly considerable value and is committed in criminal association; Article 423 of the CC: a breach of information system or data offence is committed against works of public concern; and Article 424 of the CC: compromising or defrauding the integrity of the computer protection system or device is committed against works of public concern.

Furthermore, the Unit participates in some investigations which are conducted by the Riot Police's National Bureau of Investigation and other specialised units fighting international and organised crime (e.g. illegal migration, illegal immigrant smuggling, trafficking in human beings, drug trafficking, etc.). In such investigations, the Unit supports the actions at the scene. Thus, at the seizure and the data saving respectively, the Unit is exclusively responsible for performing the forensic saving and analysis of the seized electronic devices.

Some of the Unit’s regular police officers possess special knowledge certified by IACIS (International Association of Computer Investigative Specialists), such as Basic Computer Forensic Examiner.

The other specialised unit mentioned is the Money Forgery and Payment Card Fraud Unit in the Intelligence Division of the Riot Police's National Bureau of Investigation. The Unit's activities extend to more serious international cash-substitute payment instrument fraud (skimming, ATM hacking, card-present fraud, card-not-present fraud, phishing) and the Unit also participates in the fight against online bank fraud.

The Budapest Police Department has specialised units among the county police forces for the fight against cybercrime.

The Budapest Police Department's Computer Crime Subdivision is responsible for exploring and investigating important, often international, cybercrimes (e.g. offences against information systems, online banking fraud, internet fraud, cash-substitute payment instrument fraud) committed on the territory of the capital.

In addition to other non-cybercrime issues, the Child and Juvenile Protection Unit of the Budapest Police Department's Crime Division is responsible for investigating cases involving major online child sexual exploitation - often international in nature - committed on the territory of the capital.

The IT Division, operating at the request of the investigative authority (i.e. the Department of Central Investigations of the Directorate-General for Criminal Affairs at the National Tax and Customs Administration of Hungary), exposes and investigates computer- or internet-related criminal activities. The current main priority areas of the department are: exposing websites which infringe intellectual property rights, detecting perpetrators who share content illegally and prosecuting criminal investigations, as well as investigating the activities of web shops of national importance - and presumably combating tax avoidance - and initiating the necessary procedures or taking measures. The Unit against Internet Crime has been operating since 2011 and has exposed 27 special internet criminal cases and closed 86 other investigations. More than 50 000 intellectual properties were concerned in the cases exposed and the total committed value exceeds HUF 10 billion. Media coverage of the work of the IT Division in combating criminal activity has also affected the habits of Hungarian internet users.

There had been large numbers of openly operated pirate sites, which have now dwindled to a minimum. The phenomenon of peer-to-peer sharing cannot be stopped by criminal threat, and the purpose is not to criminalise average users, otherwise it is not permitted by the law. The purpose of the intelligence activities is to take action against those who release the content, who share protected work and cause significant damage, and to fight against illegal operators of websites and web shops whose operations generate illegal profits.

The IT Division carries out additional activities – based on requests from other departments – such as performing specific internet searches, securing evidence from the internet, making online inspections and making data backups with live forensic tools at crime scenes. The division is involved in international (EUROPOL, CCWP) and national (BSA, HENT, representative of copyright owners etc.) organisations. In addition to the above-mentioned activities, the unit carries out training sessions and presentations on experience in the field of cybercrime. These presentations are primarily intended for the judges, prosecutors (Hungarian Judicial Academy), students at the Law Enforcement Academy (National University of Public Service) and right holders (HENT, PROART, conferences, media appearances, etc.). The IT department has participated in several awareness campaigns (media appearances, conferences) and also helps the work of the investigators by creating written materials (for example, the Investigator`s IT Guide).

Computer forensic experts are appointed by the Director of the Institute of Expert Services (IES) of the Special Service for National Security (SSNS), based on the expert appointment request sent by the investigative authority. The IES has specific posts for computer forensic experts. The computer forensic experts it employs are not necessarily members of the Hungarian Chamber of Experts, since the IES is an organisation legally empowered to provide expert opinions regarding forensic and other technical questions, including in the area of computer forensics.

The main obstacles to investigations into cybercrime mentioned by the national authorities are as follows:

- The internet has no borders, while international law enforcement and judicial cooperation is slow and time-consuming.

- Most of the required information is held by the private sector, and the legal and technical difficulties regarding data and evidence collection makes life easier for perpetrators. Non-cooperative service providers (like Google) and some server holders do not register their clients and/or traffic data, thereby ensuring anonymity for perpetrators.

- When it comes to attacks against information systems, service providers are not interested in supporting a criminal procedure with aim of determining the criminal liability of the perpetrator. They are more interested in rebuilding the damage as soon as possible, as discreetly as possible, without damaging their reputation for reliability.

- With regard to child pornography, there is considerable latency, victim identification is very difficult and procedural obstacles make it difficult to prevent secondary victimisation.

- For financial, organisational and professional reasons, the investigating authorities find it more difficult to keep up with technology advances than the perpetrators. The perpetrators use encryption and self-covering methods or services (e.g. hyde, ip, proxy). As far as legal issues are concerned, the main problem is the bandwidth of data plans (e.g. IP address, traffic, subscriber data) as well as authority issues such as cloud storage (Google Drive, Dropbox, etc.) and accessing social pages like Facebook. Concerning cloud storage, the legal authority cannot be accurately defined, mostly because of the different territorial authorities. From a legal point of view, the data supplement is not unified, and there are many different legal regulations.

As regards the economic aspects, the most significant costs involve covering the licenses necessary for using forensic software, which can be expensive. The contiguous purchasing of the storage media needed for forensic acquisitions (e.g. hard disk, USB flash drive, CD, DVD, etc.) could also be problematic.

As regards the technical aspects, the most common problem is having to deal with the latest and ever more precise encrypting software - and of course unlocking it. There is also the question of analysing and processing the enormous amount of data.

The non-stop contact point, for the CoE 24/7 and also in the G8 24/7 contact point system, is the National Police Headquarters National Criminal Cooperation Centre (NEBEK). It receives requests and reports by phone, fax and email in English, German, French and Spanish. In each of these contact point lists, the High-Tech Crime Unit in the Corruption and Economic Crime Division of the Riot Police's National Bureau of Investigation constitutes a contact point that can receive requests and reports during working hours. If NEBEK cannot deal with a request, it immediately gets in touch with the Unit, which can react to urgent transcriptions during its standby duty.

The NBI has five regional departments geographically located in five different directions from the capital city. The officers who are part of these five regional departments deal with a large variety of crimes, which means that only the central level of the NBI has officers dealing specifically with cybercrime. This can sometimes cause problems, because the police officers from the central level are required to assist and give support to their regional departments. One proposal might be for the Cybercrime Department to appoint a specialised cyber officer in each of the five regional departments who would deal only with cybercrimes.

The Cybercrime Unit consists of 20 investigators, and there is an ongoing procedure to employ a further 19 persons. The main duties and responsibilities of the Cybercrime Unit include investigations into all types of cybercrimes (content-related, attacks on information systems, fraud via the internet and card frauds).

The Cybercrime Unit is not divided into any internal subgroups classified according to the different types of cybercrime, such as IPR group, CSE group, hacking/computer intrusions group, etc. For many reasons, international organisations such as Europol and the FBI (USA) designate a contact point person for each country as the contact point for a particular type of crime so that, if that country is requested to provide assistance, the counterpart body knows which officer should be contacted.

An example of good practice is the whole police investigation process. They can initiate a case, and start the investigation by analysing the information. They can ask an internet service provider for IP information directly, on their own initiative, which facilitates the investigation process.

Another good practice is that the Cybercrime Department is also responsible for carrying out forensic examinations of electronic devices seized during searches. This is recognised as being extremely useful, since the investigations are conducted by the same department.

However, the Cybercrime Department is not allowed to conduct undercover investigations, which could be extremely useful at times when dealing with special cases such as those involving child sexual exploitation. There is a need to develop national P2P monitoring tools to deal with international cases and to obtain information from sources other than international reports.

4.3. Other authorities/institutions/public-private partnership

National Cyber Security Centre

On 15 April 2013, the Parliament adopted Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies, and its implementing regulations, which identified the various information security organisations, roles and forms of cooperation.

On 16 July 2015, Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies was modified. As a result of the modification, the National Cyber Security Centre was established on 1 October 2015, by uniting GovCERT-Hungary, the National Electronic Information Security Authority and the Cyber Defence Management Authority (CDMA). The National Cyber Security Centre is more coordinated, and the implementation of tasks and the information flow are more effective in this united organisation.

Thanks to these measures, the National Cyber Security Centre can track and assist with the entire information security lifecycle and its evolution, including the planning phase, regulation, control and also incident-handling.

There are three organisational units, each with specific tasks, in the National Cyber Security Centre: the National Electronic Information Security Authority, GovCERT-Hungary and the unit that is responsible for security management and vulnerability assessment.

The tasks of the units are as follows:

- National Electronic Information Security Authority

- registering the customers and systems data
- control of the identified security classifications and security levels
- checking compliance with the requirements
- carrying out the vulnerability assessment
- suggestions for identifying a vital (information) system
- suggestions on designating a person responsible for the security of electronic information systems

- GovCERT-Hungary

- management of security incidents
- threat management
- duty service
- analysis / assessment
- cyber security exercise

  training, awareness-raising
- helping to identify the responsible person
- vulnerability assessment
- cooperation with the NISZ Ltd. in the event of having to manage security incidents
- to provide regular information for managers

- security management and vulnerability assessment unit

- vulnerability assessment
- investigation of security incidents
- performing tasks in connection with information security in the EMIR/FAIR systems

The National Cyber Security Centre makes use of previously established international relations, including GovCERT-Hungary's relations. It continues to build on existing professional relations, and to deepen the relationship with foreign cyber security organisations, CERTs and international cyber security organisations (European Network and Information Security Agency - ENISA, Forum of Incident Response and Security Teams - FIRST, Trusted Introducer - TI, International Watch and Warning Network - IWWN, European Government CERTs Group - EGC).

In 2015 GovCERT-Hungary was the president of the Central European Cyber Security Platform, the common platform for the cyber security organisations of the Visegrad Group plus Austria. Moreover, in 2015, GovCERT organised a cyber security exercise for IWWN community members.

Participation in the international cyber security exercises (2015):

At the Central European Cyber Security Platform (initiative of the Visegrad group and Austria) Hungary organised the 'CECSP Communication Exercise'.

To fulfil the duties of IWWN membership, GovCERT-Hungary successfully organised and managed an Alert Exercise (ALEX March 2015) on 25 March 2015.

In the course of 2015 Hungary took part in the NATO CMY crisis management international alert exercise.

GovCERT-Hungary took part in preparations for the Cyber Storm V (US CERT) exercise and the Cyber Europe 2016 exercise, organised by ENISA. It is also planning to take part in both these exercises in 2016.

National Crime Prevention Council

The National Crime Prevention Council was established on 13 April 2011 by Government Decree 1087/2011 in order to create a high level of public safety, combat crime and take steps to combat offenders and the factors leading to crime. The main aim of the Council is to operate the new models of crime prevention effectively and to coordinate the development and implementation of action plans. The Council consists of no more than 23 people, who are representatives of different organisations.

The main tasks of the Council are:

- to harmonise the implementation of the national crime prevention strategy, take part in the development of the action plans and monitor their implementation;
- to draw up proposals for the Government in order to disseminate and apply all the resources aimed at implementing crime prevention programmes and tasks;
- to initiate and encourage measures against the causes of committing crimes and processes that promote crime;
- to initiate the drafting of legislation in the field of crime prevention and to give its opinion thereon. After the legislation has entered into force, the Council helps to monitor its implementation;
- to harmonise the actions of the central public administration bodies and the law enforcement agencies in the field of crime prevention and to support the activities of the local crime prevention bodies;
- to cooperate with the foreign and international crime prevention organisations;

- to coordinate cooperation between the Hungarian public administration and law enforcement bodies, local crime prevention organisations and foreign and international organisations;
- to contribute to the creation of a coherent national crime prevention information system;
- to disseminate good practices in social and law enforcement crime prevention in Hungary and abroad and to help to put professional know-how to good use in law enforcement education and training;
- to participate in creating the Government's crime prevention programmes and in drawing up the evaluation report on social crime prevention and crimes committed during the previous year;
- to contribute to law enforcement crime prevention and victim support and to the crime prevention activities of scientific and educational institutions;
- to help to achieve the Government's goals in public security with efficacy and methodological studies;
- to contribute to the granting of subsidies from the available resources to crime prevention projects.

Counter Terrorism Centre

The NCTC is responsible for monitoring online materials with extremist ideologist content. However, the Centre is not entitled to open investigations; if it suspects that a crime has been committed, it must inform the police.

The National Media and Infocommunications Authority contributes to the prevention of computer crimes as follows:

Pursuant to Article 92/A and 159/B of the Electronic Communications Act, the NMHH organises and controls the implementation of temporary or permanent prevention of access to data published through the electronic communications network ordered in a criminal proceeding. Article 158/D). Ordering the prevention of access to such data creates an obligation for internet service providers to filter the specific illegal online content (e.g. child pornography) from internet traffic.

This action is taken if the court has ordered the removal of the specific online content at the initiative of the public prosecutor and the web hosting service provider has failed to comply with the order or (in the case of a foreign service provider) the request to the foreign authority to provide legal assistance concerning the removal of the electronic data produced no result within thirty days. In such cases, the NMHH is involved in the enforcement of the relevant court order as follows:

a) Operating KETHA – delivery of the relevant court order to the obligated electronic communications service provider:

The NMHH operates KETHA, the central electronic database of the decisions on rendering data inaccessible, which collects data on rulings and orders on making data inaccessible as submitted by the courts and forwards them to electronic communications service providers as well as search engines and caching service providers.

b) Communication of technical hindrances to the court

Pursuant to Article 159/B (5) of the Electronic Communications Act, the NMHH may notify the court if the implementation of the order on blocking by the electronic communications service providers could be questionable given the data content provided.

c) Technical assistance to service providers

Article 159/C (4) of the Electronic Communications Act stipulates the following: 'Upon the request of the access-providing electronic communications service providers/search and cache providers, the Authority, to the extent feasible with the available technical options, shall cooperate in the development of the technical environment necessary for the implementation of the judicial decisions.'

The NMHH complies with the above obligation by setting up and operating TSR, the technical assistance system, to which service providers can connect free of charge pursuant to the terms and conditions in the public administration contract. More information (in Hungarian): http://nmhh.hu/tart/index/1507/Elektronikus_adatok_hozzaferhetetlenne_tetele

4.4. Cooperation and coordination at national level

4.4.1. Legal or policy obligations

The National Cyber Security Coordination Council, the Cyber Security Forum and the sectoral cyber security working groups work on coordination activities in the field of cybercrime and cyber security at national level.

The level of protection of national information systems has been significantly developed in the past few years; however, in order to provide a comprehensive approach, there is still much work to be done in the future as well. A proper level of security cannot be established simply by reorganising the institutional framework and developing the operational and security systems used by those institutions. For systems with security shortcomings, the level of safety should be consistently increased in line with the law on information security. For new systems, particular attention should be paid to and sufficient financial support should be provided for establishing appropriate information security. Raising awareness at all levels must be increased – among leaders, system developers, users – since protecting those systems by technical tools alone would entail extremely high costs for the State.

Security-conscious behaviour and safety improvements are needed as well as appropriate institutional frameworks - including the National Cyber Defence Centre - in order to ensure a high level of cyber security.

Common rules on disaster management in a decree of the Ministry of the Interior lay down the rules for critical infrastructure protection as well. According to the decree (62/2011), the police, the Hungarian prison service, the Constitution Protection Office, the National Security Special Service and the Counter-Terrorism Centre are responsible for disaster management, coordinated by the National Directorate-General for Disaster Management at the Ministry of the Interior (NDGDM). They cooperate in building up the critical infrastructure protection system; they also take part in the identification procedure and provide data for these tasks.

Article 156[7] of Act C of 2003 on Electronic Communications regulates the obligations of service providers in the field of cyber security.

According to this provision, service providers shall take appropriate technical and organisational measures - jointly with other service providers if necessary - in order to safeguard the security of their services and for the protection of personal data of subscribers obtained in the process of supplying electronic communications services.

Breach of personal data of subscribers shall cover a breach of security leading to the accidental or unlawful use or processing of personal data, meaning, in particular, the destruction, loss, alteration and unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service.

In the event of a personal data breach, the provider of electronic communications services shall, without undue delay, notify the personal data breach to the Authority.

7 Established by: Article 51 of Act CVII of 2011. In force: as of 3 August 2011.

Electronic communications service providers shall maintain an inventory of personal data breaches comprising the material facts surrounding the breach, its effects and the remedial action taken by the electronic communications service provider. The inventory shall include all facts and circumstances, and any information deemed sufficient to enable the Authority to verify whether the electronic communications service provider has complied with the provisions of Subsection (5). Only the information necessary for this purpose shall be included in the inventory.

When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or other private individual, the provider of electronic communications services shall also notify the subscriber or private individual of the breach without undue delay. Notification of a personal data breach to a subscriber or private individual concerned shall not be required if the provider of electronic communications services has demonstrated to the satisfaction of the Authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

Without prejudice to the service provider's obligation to notify subscribers and private individuals concerned, if the service provider has not already notified the subscriber or private individual of the personal data breach, the Authority, having considered the likely adverse effects of the breach, may - following consultation with the *Nemzeti Adatvédelmi és Információszabadság Hatóság* (National Authority for Data Protection and Freedom of Information) - require the service provider to do so.

The notification to the subscriber or private individual shall, as a minimum, describe the nature of the personal data breach and the contact points where more information can be obtained by the subscriber, and shall recommend measures to mitigate the possible adverse effects of the personal data breach. The notification to the Authority shall, in addition, describe the consequences of the personal data breach and the measures proposed or taken by the provider of electronic communications services to address that breach.

The Authority may make recommendations as to the format of such notification and the manner in which the notification is to be made under this Section, and shall disseminate best practices among providers of publicly available electronic communications services concerning the level of security deemed appropriate for processing personal data.

The technical and organisational measures shall be sufficient - with regard to best practices and the costs of the proposed measures - to afford a level of security appropriate to the risk presented in connection with network integrity and the services provided.

In case of a particular risk of a breach of network integrity and security of services that may remain in spite of the technical and organisational measures taken, the service provider must inform the subscribers of such risk and the measures the subscribers may take to enhance the level of protection.

Should an event occur which affects or jeopardises network integrity or the security of services, and a previously unknown risk of a breach of security appears in consequence, the service provider shall - at least through its customer service and website - promptly inform the subscriber of that risk, the measures the subscriber may take to enhance the level of protection and the estimated costs involved. The service provider shall provide this information to the subscriber free of charge. The requirement to inform subscribers of particular security risks does not discharge the service provider from the obligation to take appropriate and immediate measures to restore the integrity of its network and the normal security level of the service.

Above and beyond the obligations of service providers conferred under this Act relating to the protection of personal data, the privacy of communications transmitted over the service provider's network and the security of services, the detailed regulations concerning the processing of personal data, the special requirements for the protection of privacy of communications and messages transmitted over public networks, and the conditions for the indication of identifiers and call forwarding are decreed by the President.

The High-Tech Crime Unit in the Corruption and Economic Crime Division of the Riot Police's National Bureau of Investigation works in close cooperation with the Hungarian Banking Association. In recent years, in order to combat fraud, they have published warnings and information for the public, in all major cases affecting large numbers of people, on attempts at illegal bank card data gathering via the internet. These warnings were published, with minor alterations, on the main online banking webpages of most Hungarian financial institutions.

Moreover, in more serious cases, the Hungarian Banking Association organised large-scale media campaigns to provide the quickest and most effective form of information for the public. In some cases, the Bank Security Units reported these abuses and new ways of committing offences to the High-Tech Crime Unit from the very moment the crime started to be committed ('zero day').

From a practical point of view, nearly all bank cards in Hungary are equipped with a chip, which forms the basis for card authorisations throughout the ATM and POS network. This means that cards issued in Hungary are not vulnerable to card fraud through the magnetic strip, either in Hungary or in the rest of the EU. Unfortunately, in countries outside the EMV zone there have been illegal cash withdrawals using bank card data copied in Hungary. This was possible because as yet none of the financial institutions in Hungary have introduced geo-blocking technology.

Each financial institution has a different level of authorisation for online transactions, and this varies widely. Some financial institutions require only a static password for using online banking and do not even require any dynamic password for internet purchases using bank card data. Bank card companies are trying, with varying degrees of success, to orientate these institutions towards more secure online bank card use.

Most domestic financial institutions expect internet traders to ensure that a dynamic password is also used to enable bank card authorisation (e.g. 3dsecure). There is a system - unique in the world - involving widespread use of text messages sent to customers after bank transactions in Hungary which helps to alert them to any attempted fraud.

Cooperation with the private sector takes place during the implementation of the 'Order to preserve data stored in an information system' in accordance with Article 158/A of the **CPA**, during 'Rendering electronic data temporarily inaccessible' in accordance with Articles 158/B-158/D of the CPA, and during the implementation of the 'Order to render electronic data permanently inaccessible performed by disabling access irrecoverably' in accordance with Article 596/A of the CPA.

The cooperation among different governmental authorities in the field of cybercrime is considered effective and the overall feedback is regarded as positive. However, the general impression given is that cooperation between the governmental and the public sector is in its early stages and therefore there is a need for further improvement.

Moreover, it was noted that there is a need to develop a platform for receiving a complaint or reporting information in relation to the commission of a possible cybercrime offence. The implementation of such an initiative in the field of cybercrime could help to develop both a proactive and a reactive approach to cybercrime.

4.4.2. Resources allocated to improve cooperation

The equipment and capacity of law enforcement agencies differ depending on the authority (investigating authorities, prosecutors or courts) to which they belong.

The National Tax and Customs Administration or the police are in charge of conducting investigations, but some cases come directly under the responsibility of the prosecutor's office.

The National Tax and Customs Administration and the police both have special cybercrime units that use adequate tools (hardware and software) and are properly trained.

If an official of an authority not working for the special unit encounters a problem related to the gathering or recording of e-evidence, then he or she does not have direct access to the equipment, software or know-how. However, the officials of the investigating agencies can ask for assistance at any time from the special unit of their authority. Alternatively, they can turn to external experts as well.

In the prosecution service, the investigating prosecutors and the IT personnel all receive proper training to prepare them to conducting investigations on their own. If necessary, the prosecutor's office can also ask for help from the specialised units of the investigating authorities.

In addition to the above-mentioned task of investigation, the main duty of the prosecution service in cybercrime cases is to supervise investigations and present the indictment in court. To fulfil this task, the prosecutor also has to handle e-evidence, but they receive it in a form which can be accessed and evaluated using the equipment available to the prosecutor's office.

There are several training courses within the prosecution service to prepare colleagues for handling cybercrime cases, and there is generally close and direct contact with the investigating authorities, which makes it easier for tasks to be carried out successfully. If prosecutors responsible for a case cannot fulfil their tasks because of their lack of specialised knowledge, they can ask for help from colleagues who have more experience with such cases.

For the court – as for the prosecutor's office – the main goal is to evaluate the available pieces of evidence in order to form a final decision on the matter. The IT equipment of the courts is adequate for this purpose. The judges also receive training to help them to handle e-evidence correctly.

Yet it has to be said that it is hard to muster sufficient proof for a conviction in most cybercrime cases; as a result, only a small amount of cases can come before the court and the judges. Judges therefore have fewer opportunities to gather experience in cybercrime cases. Despite this, there are no major issues that would be beyond the knowledge and skills of judges in this field.

The Money Forgery and Payment Card Fraud Unit in the Riot Police's National Bureau of Investigation does not have special technical equipment. The expert opinions are drawn up where necessary by the High-Tech Crime Unit in the Corruption and Economic Crime Division of the Riot Police's National Bureau of Investigation. With the help of the Bank Security Units and certain international training courses, an up-to-date information flow about new technologies and methods used by modern criminal organisations is guaranteed.

Conclusions

- Justice in Hungary is administered in a four-level system by the Supreme Court (Curia), the regional courts of appeal, the county courts (including the Metropolitan Court of Budapest) and the local (district) courts.

- There are no rules establishing specialised courts for cases of cybercrime. District courts are, in general terms, competent to judge cybercrime cases, unless it is specified otherwise in the Code of Criminal Procedure.

- This means that criminal offences such as mail fraud; misuse of personal data; misuse of public information; offences involving classified information; criminal offences against public records and registers recognised as national assets; forgery of administrative documents; use of a forged private document; child pornography; infringement of copyright and related rights; and compromising the integrity of a technical protection all fall under the competence of district courts.

- On the other hand, the jurisdiction of the local courts located at the seat of the counties extends to the territory of the county or to Budapest (within the geographical jurisdiction of the Metropolitan Court and the Pest Central District Court) in the following cases: information system fraud; illicit access to data; breach of information system or data; compromising or defrauding the integrity of the computer protection system or device. The competence of the prosecutor's office derives from the competence and jurisdiction of the court where it operates.

- Prosecutors are, in Hungary, the judicial body responsible for supervising investigations. According to the Hungarian Code of Criminal Procedure, when the investigating authority (Law Enforcement) conducts an investigation or certain investigative actions independently, the prosecutor shall determine whether the investigation complies with procedural law and shall ensure that the procedural rights of participants are respected.

- The Hungarian prosecution service seems to have large capacities, including in the field of investigations (investigations it conducts by itself, internal forensic support units). In 2014, the Hungarian authorities also developed a network of cyber prosecutors for the Budapest area. They now plan to roll out IT units (forensic support) all around the country. All these efforts should be particularly noted as good practices favouring greater cooperation between prosecutors. The evaluation team considers that the setting up of a nationwide network of cybercrime prosecutors for the purpose of exchanging expertise and raising awareness in this area of crime is a good practice that should be supported and fostered by the competent national authorities.

- The prosecutor may, therefore, set up an investigation, allocate it to an investigating authority and give instructions on how to perform specific investigative actions.

- In addition, the prosecutor may be present during the investigative actions, assess documents produced during the investigative actions, and amend or revoke decisions of the investigating authority.

- Last but not least, it is the prosecutor's duty to consider the complaints lodged against decisions or measures taken or ignored by the investigating authority, and they may take over the proceedings if necessary.

- At organisational level, the structure of the investigating prosecutor's offices is as follows:

  - The Central Investigating Chief Prosecutor's Office (5 regional offices in: Budapest, Debrecen, Győr, Kaposvár, Szolnok, with a total of 82 prosecutors);

  - Budapest Investigating Prosecutor's Office (Budapest);

  - Pest County Investigating Prosecutor's Office (Budapest);

  - Local investigating prosecutor's offices in the remaining 18 counties (merged into the central local prosecutor's offices at the seats of the county courts).

- There are several forces and bodies dealing with law enforcement matters in Hungary. As a general rule, the law enforcement authorities dealing with investigations in the area of cybercrime come under the Ministry of the Interior (*BelügyMinisztérium*).

- The Hungarian police (Hungarian Police Headquarters - ORFK) is the general law enforcement agency with the power to gather information and carry out criminal investigations into most types of crime. The ORFK is composed of several Directorates, namely the Criminal Directorate, the Economic Directorate, the Educational Directorate and the Security Directorate.

- As to cybercrime, investigations are carried out at central level by a High–Tech Crime Unit in the NBI (National Bureau of Investigation), established in 2007 within the Riot Police (KR) of the Security Directorate.

- At county level, the County Police Headquarters have criminal investigation units in Budapest and the other 18 counties. Local city police stations (in Budapest 22 district police stations) also have investigation units.

- The Cybercrime Unit of the NBI is divided into two sub-units: the Investigation Sub-unit and the Technical Support (Forensic) Sub-unit. The Unit currently has 20 staff members (out of a total of 39 planned posts) and its tasks are, in brief: information-gathering (including OSINT), conducting criminal investigations (including national and international cooperation at police level), performing forensic work and setting up awareness-raising and educational activities.

- Since 2007, this main investigation service has been responsible for international cooperation and has established contacts with INTERPOL (connected to the ICSE data base for one year) and EUROPOL/EMPACT, and has concluded bilateral cooperation agreements with the FBI, the Department of Homeland Security, NCMEC, NCA and BKA.

- Considering the highly demanding tasks assigned to the Unit, the evaluation team is of the opinion that it is crucial to provide it with adequate human resources and technical capacities. The allocation of financial means from the EU Security Fund might be a solution for overcoming possible budgetary constraints.

- As a point of contact for the Financial Intelligence Unit network, the National Tax Customs Administration performs 5 000 investigations each year. This service has an IT unit of 6 investigators, based in the Central Investigation Department. In recent years it claims to have had considerable success in curbing copyright offences involving intellectual or cultural goods.

- The Hungarian authorities claim to have had difficulties in receiving information from abroad because of limited data retention periods in some countries or cumbersome processes with foreign operators (namely, some American providers). Such cooperation should benefit from EU support, with a view to looking at how to simplify relations with American providers.

- The Hungarian authorities benefit from legislation which allows for one year of traffic data retention, which they deem useful and necessary for operational matters. The NBI has assessed that 25 % of its cases would not be solved without data retention.

- The Critical Infrastructures Protection Network Security Centre concentrates monitoring facilities and may be used to support coordination when faced with the consequences of large-scale cyber attacks against infrastructures.

- The national media and info communications service has been operating an internet hotline on illegal content since 2011. This authority concluded an agreement with the Hungarian police in 2013 and also cooperates with the Prevention Council.

- It checks reports to ensure that only relevant ones are sent: to date, they have issued 3 027 reports involving 2 797 substantive cases, 2 788 of which were successful. To help providers to disable access to illegal data, it can provide free technical support and inform them about good practices. It sends justice orders to providers, checks the implementation thereof, reports problems to courts and manages the KHETA databases (on illegal access).

- In Hungary, most of the digital security missions are concentrated under one authority (the Ministry of the Interior), which may then coordinate a large range of actions from cyber security to cybercrime issues. There seems to be a high level of centralisation in Hungary.

5. LEGAL ASPECTS

5.1. Substantive criminal law pertaining to cybercrime

5.1.1. Council of Europe Convention on Cybercrime

Hungary signed the Council of Europe Convention on Cybercrime on 23 November 2001 and ratified it on 4 December 2003. The Convention entered into force and was to be applied by Hungary with effect from 1 July 2004. (See Act LXXIX of 2004 on the promulgation of the Convention on Cybercrime signed in Budapest on 23 November 2001).

5.1.2. Description of national legislation

A. Council Framework Decision 2005/222/JHA on attacks against information systems and Directive 2013/40/EU on attacks against information systems

The implementation procedure was finalised by the summer of 2015 and the national authorities did not report any difficulties during the implementation phase. Due to the short period of time that has elapsed since implementation, the national authorities could not give any feedback on difficulties in relation to its enforcement.

B. Directive 2011/93/EU on combating sexual abuse and sexual exploitation of children and child pornography

The transposition (implementation) and related notification took place at the beginning of 2014. Having regard to the limited time that had elapsed since the transposition deadline, the national authorities did not experience any difficulties in implementation.

Regarding transposition, the national authorities reported difficulties related to the notion of 'grooming' in Hungarian law, considered literally not possible. The difficulty was that transposition could only be carried out to the extent necessary and limited to the strict minimum because 'grooming' seems to be an early preparation conduct. Given that this conduct is complex, the Hungarian Criminal Code complies with it through more relevant statutory provisions, depending on the circumstances of the case (treating it either as an 'attempt to persuade' or as a preparation conduct).

C. Online card fraud

If individuals become victims of bank card fraud, they primarily claim for compensation of damages, so they contact their financial institution. After that the financial institutions usually examine to what extent the customer is responsible for the committing of the offence due to his or her failure to take the reasonable steps essential for data security. If the financial institution does not hold the customer responsible for the losses, compensation will be paid. In such cases, individuals usually report the crime only if the financial institution makes this a requirement for compensation.

In order to protect their market position, financial institutions often decide to compensate the damage caused in spite of the customer's smaller failure, because an attack against a financial institution may result in the loss of customers, so it is more profitable to compensate the loss. If the financial institution does not compensate the loss, customers typically report the crime when the loss is considerable and they try to claim for damages through the criminal procedure.

In more serious cases, or whenever they have relevant information about the perpetrator which may result in the success of the investigation, the financial institutions report the crime themselves.

The Hungarian National Bank publishes quarterly data on abuse of bank cards (the statistics contain data for the period between 2010 and the first quarter of 2015):

http://www.mnb.hu/statisztika/statisztikai-adatok-informaciok/adatok-idosorok/xiv-penzforgalmi-adatok/penzforgalmi-tablakeszlet

The High-Tech Crime Unit in the Corruption and Economic Crime Division of the Riot Police's National Bureau of Investigation works in close cooperation with the Hungarian Banking Association. In recent years, in order to combat fraud, they have published warnings and information for the public, in all major cases affecting large numbers of people, on attempts at illegal bank card data gathering via the internet. These warnings were published, with minor alterations, on the main online banking webpages of most Hungarian financial institutions.

Moreover, in more serious cases, the Hungarian Banking Association organised large-scale media campaigns to provide the quickest and most effective form of information for the public. In some cases, the Bank Security Units reported these abuses and new ways of committing offences to the High-Tech Crime Unit as soon as the crime started to be committed ('day zero').

From a practical point of view, nearly all bank cards in Hungary are equipped with a chip, which forms the basis for card authorisations throughout the ATM and POS network. This means that cards issued in Hungary are not vulnerable to fraud through the magnetic strip, in either Hungary or the rest of the EU. Unfortunately, in countries outside the EMV zone there have been illegal cash withdrawals using bank card data copied in Hungary. This was possible because as yet none of the financial institutions in Hungary have introduced geo-blocking technology.

Each financial institution has a different level of authorisation for online transactions, and this varies widely. Some financial institutions require only a static password in order to use online banking and do not even require a dynamic password for internet purchases using bank card data. The bank card companies are trying, with varying degrees of success, to orientate these institutions towards more secure online bank card use.

Most domestic financial institutions expect internet traders to ensure that a dynamic password is also used for bank card authorisation (e.g. 3dsecure). There is a system - unique in the world - involving widespread use of text messages sent to customers after bank transactions in Hungary, which helps to alert them to any attempted fraud.

D. Other cybercrime phenomena

The equipment and capacity of law enforcement agencies differ depending on the authority (investigating authorities, prosecutors or courts) to which they belong.

The National Tax and Customs Administration or the police are in charge of conducting investigations, but some cases come directly under the responsibility of the prosecutor's office.

The National Tax and Customs Administration and the police both have special cybercrime units that use adequate tools (hardware and software) and are properly trained.

If an official of an authority not working for the special unit encounters a problem related to the gathering or recording of e-evidence, then they do not have direct access to the equipment, software or know-how. However, these officials of the investigating agencies can ask for assistance at any time from the special unit belonging to their authority. Alternatively, they can turn to external experts as well.

In the prosecution service, the investigating prosecutors and the IT personnel all receive proper training to prepare them to conduct investigations on their own. If necessary, the prosecutor's office can also ask for help from the specialised units of the investigating authorities.

In addition to the above-mentioned task of investigation, the main duty of the prosecution service in cybercrime cases is to supervise investigations and present the indictment in court. To fulfil this task, the prosecutor also has to handle e-evidence, but they receive it in a form that can be accessed and evaluated using the equipment available to the prosecutor's office.

There are several training courses within the prosecution service to prepare colleagues for handling cybercrime cases, and there is generally close and direct contact with the investigating authorities, which makes it easier for tasks to be carried out successfully. If prosecutors responsible for a case cannot fulfil their tasks because of their lack of specialised knowledge, they can ask for help from colleagues who have more experience with such cases.

For the court – as for the prosecution office – the main goal is to evaluate the available pieces of evidence in order to take a final decision on the matter. The IT equipment of the courts is adequate for this purpose. The judges also receive training to help them to handle e-evidence correctly.

However, it has to be said that it is difficult to muster sufficient proof for a conviction in most cybercrime cases; as a result, only a small number of cases can come before the court and the judges. Judges therefore have fewer opportunities to acquire experience in cybercrime cases. Despite this, there are no major issues that would be beyond the knowledge and skills of judges in this field.

The Division against Counterfeiting Money and Bank Cards in the Riot Police's National Bureau of Investigation does not have special technical equipment. The expert opinions are drawn up where necessary by the High-Tech Crime Unit in the Corruption and Economic Crime Division of the Riot Police's National Bureau of Investigation. With the help of the Bank Security Units and certain international training courses, an up-to-date information flow about new technologies and methods used by modern criminal organisations is guaranteed.

Hungary tries to overcome cross-border obstacles by placing great emphasis on direct information exchange and establishing professional networks. To this end, the national authorities have established and maintained direct contacts with most EU countries' central units responsible for investigations of bank card fraud cases (BG, RO, HR, SI, SK, CZ, PL, AT, DE, DK, FIN, SE, NL, FR, ES, PT, IT, EL, UK), and with the FBI and the US Secret Service (USSS). The contribution of liaison officers specialising in police cooperation in foreign countries (including Switzerland and Canada) is also a great support.

5.2. Procedural issues

5.2.1. Investigative techniques

Although the CC and CPA contain the basic rules, many other acts are concerned. During the investigative phase the most important task is to collect all evidence, which is manifested in cybercrime cases when securing data and devices, at least temporarily. There are different rules in place depending on whether an opened or a covert investigation is involved. Lawfulness, promptness and precision are important factors. The procedure is influenced by the certain fact of the case, but the rules are general. The CPA contains rules on investigation. As mentioned in the previous point, in addition to the rules on house searches and seizure, it includes basic guarantees that must also be taken into account.

The relevant national legislation is provided in Annex D.

5.2.2. Forensics and encryption

In Hungary, online examination of e-evidence is executed by the investigating authority. This examination generally follows the rules on inspections, which are conducted by investigators. It may take place in the presence of an official witness and usually includes the following actions:

Identification of web pages:

- first-hand information about web pages comes from internet databases which contain information when the web address or IP address is entered (e.g. www.centralops.net (domain dossier), www.robtex.com);

- further detailed information about the owner of the web page can be found in the 'who-is-who' databases of the various service providers (e.g. the www.domain.hu in the web pages ending with .hu);

- the trace-route service makes it possible to find the servers used to reach the target server. This can be done via the DOS prompt of the computer by giving the tracert <web page> order (example: tracert index.hu);

- the number of visitors to the web pages can be checked at the www.alexa.com web page.

Recording data from web pages:

- taking a screen capture of the opened web page (Alt+PrtScr);

- employing browser add-ons, which create a pdf file of the whole page (such as WP screenshot, screengrab etc.);

- creating an offline copy of the full web page (for example, using HTTrack Website Copier);
- performing trial downloads;
- finding deleted web pages which are archived (for example, the service of Wayback Machine on www.archive.org).

Searching the internet:

- using simple web search engines (such as google.hu) and giving further information in the detailed search to narrow down the number of hits;
- using special web search engines for deep searches (e.g. www.deeperweb.com);
- using special crawler software for a full search;
- using a special web-crawler application (such as Easy Web Extract, Outwit, Convextra) to download all information on a web page (for example, to export the questionnaires of the Vatera online auction site).

Methods and services to search for specified persons/companies:

- searching for information connected to the persons or companies concerned (such as email addresses, phone numbers, nicknames, addresses, etc.);
- combined searches for partial information found using the above method;

- special search services (such as www.pipl.com);
- searching social networking sites (like Facebook);
- sending a data request to international service providers.

Recording data from the internet as evidence:

During the online inspection the authority records every item of data, every circumstance and every piece of information which may be important in the procedure. The process of data-recording is documented via screen captures or screen capture videos, which are saved to a DVD disk together with the actual data, files and applications recorded during the inspection. The DVD is an attachment to the minutes created during the process. To ensure that these files are unchanged, it is necessary to create an image file from the downloaded data, and the HASH-key created from it must also be recorded in the minutes.

The examination of online evidence is carried out by the investigating authority, if necessary by employing a forensic advisor.

According to Article 182 (1) of the CPA, the prosecutor and the investigating authority may employ an advisor in investigatory actions, if special knowledge is required for uncovering, obtaining, collecting or recording means of evidence, or if the prosecutor or the investigating authority request information concerning a professional matter.

Points b) and g) of Article 103 (1) of the CPA state that a person may not act as an expert if he or she acts or has acted in the case as a judge, prosecutor or a member of the investigating authority, or is a relative of that person, or has been employed in the case as a forensic advisor.

It is possible to employ a member of the Chamber of Forensic Experts for uncovering, obtaining, collecting or recording evidence. It will no longer be possible to employ that person as a forensic expert in the same procedure, so they cannot be asked to examine and evaluate the evidence they uncovered.

When the e-evidence is secured, possibly using a forensic advisor, it may be given to a forensic expert for proper evaluation.

During the investigation, the simple data checking and information queries are recorded in official notes, and the investigator attaches the downloaded materials to them.

In Hungarian criminal procedure, an expert shall be employed if the establishment or evaluation of a fact to be proven requires special knowledge. The court, the prosecutor and the investigating authority has the right to assign a forensic expert. The order on the assignment of an expert shall state:

a) the subject to be examined by the expert and the issues to be answered by the expert,

b) the documents and objects to be handed over to the expert, or, if this is not possible, the place and time where the documents and objects may be inspected,

c) the deadline for submitting the expert opinion.

The court, the prosecutor and the investigating authority may assign a forensic expert listed as an expert in the register of experts, or a business association entitled to give expert opinion (hereinafter 'business association'), an experts' institute, or a government body, institute or organisation defined by separate laws (hereinafter 'organisation'), and if this is not possible, a person or institution (hereinafter 'ad hoc expert') possessing the necessary knowledge.

The expert shall be obliged to make a contribution to the case and to give an expert opinion. The expert shall give an opinion based on a professional examination. The expert shall conduct the examination by using the tools, procedures and methods available according to the present state of science and modern professional knowledge. The expert shall be obliged and entitled to become acquainted with all data required for the fulfilment of his or her task and for this purpose the expert may inspect the documents of the case, be present at the procedural actions, and may request information from the defendant, the victim, the witnesses and the other experts involved in the proceedings. If so required for the performance of the tasks, the expert may request further data, documents and information from the assigning authority.

In Hungary the forensic expert can only conduct such examinations as are necessary to answer the questions of the assigning authority. They can be present at investigating actions only to gather data to fulfil this purpose.

In the trial phase of the procedure, it is customary for judges to give the forensic expert a data storage containing only the relevant data which need to be examined in order to answer the questions.

The forensic experts, present during the measures taken on-site and at the (own or external) forensic units used by the investigative authority (as regards the rapid development of encryption technologies), use 'live forensic procedures' (this means that the computers, servers and other tools found on-site are examined during the operation). During the live forensic procedure, to ensure the protection of the evidence, a server is used which aims to prevent any modification of the data. As encryption technologies are constantly evolving, there is not possible to know which data in files, directories or drivers may became unavailable. The data are saved on the spot during the operation of the system in order to prevent them from being lost.

The most significant problem is the decryption itself. It requires a suitable hardware and software background. Decryption of encrypted devices is possible only by using extremely high capacities of servers and networks. During examination of seized IT devices, we have encountered, on numerous occasions, files protected with strong encryption (AES-256 encrypted archives) and whole disk encryption (TrueCrypt, BitLocker, FileVault2). Decryption of these files was very time-consuming and required a great amount of computing power. The competent authorities have succeeded in decrypting password-protected files (documents, spreadsheets, databases, etc.) and operating system user accounts on various occasions during the examination of seized IT devices.

The investigative authority may contribute significantly to the success of password cracking if it can provide information relevant to the password itself (possible passphrases, phrase fragments, character set, password length, etc.), and if it provides all digital evidence (storage devices) to the computer forensic expert. The computer forensic expert therefore always tries to collect all information relevant to the case, so that the requesting authority can gain access to the decrypted data and get proper answers to the questions asked of the expert.

In the case of mobile devices, the competent authorities have encountered certain applications that hide files and directories, but they managed to circumvent these by using physical data recovery methods. They have yet to encounter encrypted files or file systems on mobile devices. They do not possess decrypting devices, manufacturer support and proper methods to decrypt hardware-encrypted storage devices (AES-256 encrypted pen drives, hard drives protected by ATA Security, etc.). It is impossible to create forensic images of such devices without first bypassing the encryption.

Encrypted files (AES-256 encrypted archives) and whole disk encrypted drives (TrueCrypt, BitLocker, FileVault2) would require much greater computing power in order to decrease the time required for successful password cracking.

The NNI CSBEO encounters encrypted data carriers in cases involving sexual abuse of children and in economic crimes. The TrueCrypt encryption is typically used in cases involving exploitation, while Bitlocker encryption tends to be used in cases involving economic crime. In the case of password-protected documents and files, the AD PRTK/DNA application provides adequate assistance, but there are cases when access to these kinds of files is not possible.

Cooperation among the various bodies is based on previous consultations and on the rules laid down in the Code of Criminal Procedure (upon issuing an expert decision).

The application of different 'civilian' services could cause security risks, so for this reason only experts and expert institutes can be used.

5.2.3. e-Evidence

The definition of e-evidence has not been outlined until now; therefore, Hungary does not have specific rules for it. However, it does have rules and definitions which are connected to e-evidence:

- the definition of physical evidence
- the definition of information system
- the definition of data.

The rules concerning the pieces of evidence found in digital form are laid down in the general rules of the CPA.

Gathering and storage of e-evidence depend on several factors: what type of crime is being investigated; what kind of evidence can be found on the data storage device or information system they plan to examine; what kind of role the holder of these devices plays in the criminal procedure.

On-site data gathering falls into two possible categories: direct and indirect. In the direct approach, the competent authorities seize the actual device and there is no need to execute further measures to collect the data. The fundamental rule of data gathering is to make sure that the data is unchanged (with equipment preventing any writing action on the target device during the access of the data, and with the use of hash values and complete copies of the original data). It is also a fundamental rule that the evidence has to be protected from any physical harm caused in the storage device it is stored in, and it has to be identifiable (which can be solved with appropriate evidence bagging and tagging). A photo of the seized storage device is taken, including when a part is removed from a device (for example, the hard disk); a photo is taken before the part is taken out and afterwards a photo is taken to portray the whole device (laptop, computer, server, other hardware) and to show where the part was located.

The second category is the indirect approach, when a number of preparatory measures to seize the data are needed. Without mentioning all the possibilities, such measures can include backup/export of a database, decrypting of an encryption, or creating an image file of a folder.

Most of the time such measures are targeted at the companies' servers, but sometimes there is a need to apply them to individuals' information devices as well. These measures are photo-documented.

When the IT person of a company hands over some data voluntarily, this is recorded in a minute and a hash value of the data is created. In such cases 'known data' are seized. During the more usual direct method, 'unknown data' are seized. In such cases, the competent authorities continue with further examination work to find out what kind of data there are on the device and what can be proven with such information and how.

During seizure, because there is usually a lack of time, it is not always possible to copy the data from the data storage devices on-site. In such cases the device is seized as evidence, and the copying is carried out in the office of the authority, after the evidence bag is opened during a documented procedure, either in the presence of the suspect of the case or their representative. The data is copied on unused and empty storage devices or formerly used devices which are emptied with a method entailing several overwrites (wipe) to ensure that there are no more identifiable data fragments on the device.

After creating a bit-by-bit copy of the data on the seized device used as evidence, the whole bit-by-bit copy and the relevant data are sent to a separate storage device along with a report on the examination of the data.

Capturing evidence from the internet: in general, the relevant information is found and recorded by the investigator carrying out the online inspection. The procedure is documented in a minute or a report. The captured data is usually stored in an 'image-file' and identified with a hash-key, which is recorded on the storage device (the latter can be a CD/DVD/BR-disk or a hard disk).

During an on-site (live forensic) data recording: while it is running, the information system is examined by a forensic expert, by a representative of a special data recording organisation acting as a forensic advisor or by an experienced member of the investigating authority. The live examination of a working device cannot be avoided these days, because some of the data is often stored in the cloud, on outside network storage devices or on internet storage spaces, which can only be accessed on-site. The other reason why it is necessary to do live forensic is that encryption methods are developing very fast, and it is not possible to know which files, folders or drives will become inaccessible after the system is turned off.

The on-site data recording must be executed without the installation of any software on the system and without any change made to the relevant data of the system. Furthermore, it must be well documented. Under this method, data is also recorded by saving it onto image files on data storage devices with hash keys for verifying purposes.

Data recording from a seized device: the forensic expert or the member of the investigating authority copies the data from the seized computer, phone or other device and creates a report which includes a copy of the relevant data. Another storage device is used for the purpose of copying.

When responding to a data request, the service providers (telecommunication service providers, storage service providers, financial institutions or other authorities) send the data on storage devices, which can be attached to the other documents of the investigation.

5.3. Protection of human rights/fundamental freedoms

Fundamental rights and freedoms are generally protected in and by the Fundamental Law of Hungary, which is the highest level of legislation (the constitution) in Hungary. The relevant sectoral legislation also contains further guarantees and procedural legal elements for the protection and implementation of these rights.

There is no special criminal procedure in relation to cybercrimes; general rules on criminal procedure are applicable. Fundamental rights and freedoms can be derogated from where this is necessary and proportionate. However, a criminal procedure is the totality of guarantees, so these guarantees have also been built into the CPA in order to provide appropriate protection for fundamental rights and freedoms.

Derogations can be instituted in relation to collection of evidence, the imposition of coercive measures, the use of covert techniques, in connection with seizure and confiscation and also when rendering electronic data permanently/temporarily inaccessible.

The CPA determines the basic rules for ensuring enforcement of fundamental rights and freedoms (see section 1.7) However, Article 60 of the CPA also states that if the CPA allows a derogation from the fundamental rights and freedoms of a certain person, this can be executed only if the expected result cannot be achieved by another act that requires less restriction.

5.4. Jurisdiction

5.4.1. Principles applied to the investigation of cybercrime

The following principles are applied according to national law:

Temporal scope

Article 2 of the CC

(1) Subject to the exceptions set out in paragraphs (2) and (3), criminal offences shall be adjudicated under the criminal law in effect at the time when they were committed.

(2) Where an act is no longer treated as a criminal offence, or if it draws a more lenient penalty under the new criminal law in effect at the time when it is adjudicated, that new law shall apply.

(3) The new criminal law shall apply with retroactive effect in connection with acts which are punishable under universally acknowledged rules of international law, if such acts did not constitute a criminal offence under Hungarian criminal law at the time when they were committed.

Territorial and personal scope

Article 3 of the CC

(1) Hungarian criminal law shall apply:

a) if the criminal offence is committed in the territory of Hungary;

b) if the criminal offence is committed on board a Hungarian vessel or a Hungarian aircraft situated outside the territory of Hungary,

c) to any act committed by a Hungarian national abroad which is considered to be a criminal offence in accordance with Hungarian law.

(2) Hungarian criminal law shall, furthermore, apply:

a) to any act committed by a non-Hungarian national abroad, if:

aa) it is a criminal offence under Hungarian law and is also punishable in accordance with the law of the country where it was committed,

ab) it is a criminal offence against the State, excluding espionage against allied armed forces and espionage against the institutions of the European Union, regardless of whether or not it is punishable under the law of the country where it was committed,

ac) it is a criminal offence under Chapter XIII or XIV or any other criminal offence which is to be prosecuted under an international treaty proclaimed by an act of Parliament,

b) to any act committed by a non-Hungarian national abroad against a Hungarian national, a legal person and other legal entity without legal personality established under Hungarian law, which is punishable under Hungarian law.

(3) In the cases described in paragraph (2), the initiation of the criminal proceedings shall be ordered by the Prosecutor General.

I. The principles of the basis for criminal jurisdiction

The rules for determining the geographical and personal scope of the application of criminal law follow the principles of the basis for criminal jurisdiction (the principle of territoriality, the personal principle, the principle of national self-defence, the principle of unconditional punitive power). The Hungarian Criminal Code gives a general definition of the principle of territoriality and also defines an extensive active personality principle. Furthermore, the 'passive personality principle' can serve as a basis for the Hungarian jurisdiction.

1. The principle of territoriality in the Hungarian Criminal Code

According to the Criminal Code, the scope of the principle of territoriality covers the geographical territory of Hungary (point (a) of Article 3(1) of the Criminal Code) and criminal offences committed on commercial ships or vessels sailing, or aircraft flying, under the Hungarian flag outside the territory of Hungary regardless of their location (quasi-territorial principle).

Regarding the crime scene, the principle of unity of action is applicable in Hungary. According to this, the criminal offence is committed in Hungary if any element of it (according to the Hungarian Criminal Code) was committed in Hungary (be it the criminal behaviour or the result of it): in other words, the criminal offence was committed in Hungary even if elements of it were carried out abroad.

2. The personality principle in the Hungarian Criminal Code

In the case of a criminal offence committed by a Hungarian citizen abroad, the active personality principle of the Criminal Code is in force (principle of nationality): a Hungarian citizen is responsible for a criminal offence if this offence was committed in a country where it is not considered as a criminal act (point (c) of Article 3(1) of the Criminal Code).

3. The principle of *ne bis in idem*

According to point (d) of Article 6(3) of the Code of Criminal Procedure, no criminal proceedings may be initiated, and criminal proceedings in progress shall be terminated or a verdict of acquittal rendered, if a final court verdict has already been delivered on the action of the defendant; however, this provision does not apply to the procedures defined in Part Four and Titles II and III of Chapter XXIX.

Therefore, if final judgment has been passed on the act, the 'transnational *ne bis in idem* principle' applies. This principle relates to the decision of the Hungarian court acting in its criminal jurisdiction. If the decision was taken abroad, recognition of the validity of the foreign judgment is necessary to for it to be binding in the same way as a Hungarian judgment (Article 47(1) of Act XXXVIII of 1996 on international legal assistance in criminal matters). This means that, if there is recognition, it shall be deemed that the act has been subject to the final judgment of a Hungarian criminal court (Article 47(3) of Act XXXVIII of 1996 on international legal assistance in criminal matters). If the act of a person subject to Hungarian law has been judged by a foreign court but the judgment was not recognised by Hungary (meaning that the foreign judgment is not deemed to be equivalent to the judgment of a Hungarian court), there is no obstacle to starting a criminal procedure but in this case the permission of the Chief Prosecutor is required. However, in the latter case, enforced penalties involving deprivation of liberty and house arrest must be included in the sanctions imposed by the Hungarian court (Article 47(2) of Act XXXVIII of 1996 on international legal assistance in criminal matters).

We should refer here to paragraph 6 of Article XXVIII of the Fundamental Law of Hungary (25 April 2011): 'With the exception of extraordinary cases of legal remedy laid down in an Act, no one shall be prosecuted or convicted for a criminal offence for which he or she has already been finally acquitted or convicted in Hungary or, within the scope specified in an international treaty or a legal act of the European Union, in another State, as provided for by an Act.'

4. Accessibility rules based on the principle of universal jurisdiction, state self-defence, and passive personality.

a) Article 3(2) of the CC contains 'accessibility rules' in order to be able to use Hungarian criminal law as widely as possible. That is why principles of universal jurisdiction, state self-defence and passive personality have been recognised by the law.

An accessibility rule in relation to double criminality was incorporated into point (aa) of Article 3(2). It requires that the act should be a crime under the Hungarian CC from the Hungarian point of view, but from the point of view of the place where the act was committed the act should only be punishable, which is not necessarily the same thing. This means that, in order to apply the Hungarian CC, there should be no obstacles for punishing the act at the place of commission, while the secondary obstacles for punishment within the Hungarian CC are not relevant. (e.g. different rules on desuetude).

b) The principle of state self-defence in point (ab) of Article 3(2) does not require double criminality, with the exception of two crimes: Article 262 of the CC: Espionage Against Allied Armed Forces and Article 261/A of the CC: Espionage Against EU Institutes. The exemption in this case means that, if the crime is committed abroad by a foreigner, point (aa) of Article 3(23) cannot be applied in line with the content of Article 3(2).

c) Universal jurisdiction in point (ac) of Article 3(2) is about protecting universal values and it establishes the possibility for establishing Hungarian jurisdiction in relation to acts where personal or territorial connection is undetectable. Crimes against humanity are in a separate chapter and these rules refer to this (point (ac)), but it would also be possible to start a procedure in relation to these only – according to the Decision 53/1993 (X.13) of the Hungarian Constitutional Court - on the basis of international treaty or customary law. In case of other international crimes – because of the dualistic approach in the Hungarian system – a procedure can be started only if the international treaty has been incorporated into or implemented under national law.

5. Recognition of the passive personality principle in point (b) of Article 3(2) means that Hungarian jurisdiction can be established on the grounds that the insulted victim is a Hungarian citizen or a legal person established under Hungarian law or other entity without legal personality established in accordance with Hungarian law. Where this principle is used, dual criminality should not be examined. It therefore does not matter whether it is a crime in the other state or the perpetrator could be punished under the other law. The sole requirement is that the act should be punishable according to the Hungarian CC.

II. Principle of opportunity

In all cases where Article 3(2) could be used, the principle of opportunity is applied. The Chief Prosecutor is entitled to take the decision on prosecution. He or she can do this at any time within the desuetude period in accordance with Hungarian law.

5.4.2. Rules in the event of conflicts of jurisdiction and referral to Eurojust

Hungary has adopted provisions facilitating the implementation of Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings. The adopted provisions have been in force since 1 January 2013 [see Act CLXXX of 2012 on criminal cooperation in criminal matters between the Member States of the European Union, hereinafter referred to as 'the EU Act', Chapter VII]. As a result, if conflicts of jurisdiction arise, EU Member States may exchange information or may engage in consultations.

A proceeding was initiated in Hungary and in the United Kingdom regarding child pornography and the threat to public danger, the facts of which show a strong correlation with each other. Due to the risks of conflict of jurisdiction, the proceeding started at Eurojust (initiated by Hungary) and after this a coordination meeting was held with the participation of Hungary, the United Kingdom and the United States of America. During the coordination meeting and based on the evidence available, the territoriality of the offence committed was not yet decided (was it committed on the territory of Hungary or on the territory of the United Kingdom?). Regarding this, the representatives of the United Kingdom and Hungary initiated the establishment of a joint investigation team.

Based on the evidence available, these crimes were committed by illegally breaking into the computer system and cracking the passwords on a number of occasions. Communication between the United Kingdom and Hungary was performed through servers located in the United States of America. The Hungarian judicial authorities sent a request for legal assistance to the US Department of Justice in order to collect data – IP addresses - stored on the iCloud and on the Google drive, which are operated by Apple Inc. and Google Inc. The basis for the request for legal assistance was the Treaty on Mutual Assistance on Criminal Matters between Hungary and the United States of America.

5.4.3. Jurisdiction for acts of cybercrime committed in the 'cloud'

Some international internet provider companies (such as Facebook and Google) are not represented in Hungary and cannot be asked to provide data.

This is problematic because sometimes the Hungarian authorities do not get any reply to their request for international procedural legal assistance. It is therefore impossible in such cases to step forward and examine what IP address was used during the offence. Furthermore, the aforementioned companies do not answer every request. The lack of information can make it harder to identify the perpetrator, the time of the offence, the location of the offence and the instrument the offence was committed with.

These obstacles are compounded by the fact that Hungarian citizens make active use of the services offered by Facebook and Google Inc. and there is therefore an increasing amount of evidence to be found on their servers.

The solution:

There are further solutions for continuing the investigation should the internet providers concerned prove unwilling to provide data.

- If the offence was committed for the purpose of financial gain, it is possible to track the path of the money and to find the perpetrator.

- If the victims have access to the cloud-based service system, the competent authorities can check (with the consent of the victim) those data which are accessible for them. For example, the mailboxes of Google Inc. record the recent IP addresses that were logged in, which can be also checked by the users.

- As happens in ordinary criminal offences, in the cases of offences committed on the internet it may happen that the perpetrator and the victim know each other, for example if the offence is committed out of revenge. During the investigation the competent authorities can check whether there is anyone who was interested in committing the offence.

- If several similar offences were committed, they can be identified and merged based on the means of perpetration recorded in the databases of different authorities. This can be useful in identifying the perpetrator by comparison with the data that were managed separately in the past.

If international procedural legal assistance cannot be avoided, there is an option for getting the appropriate answer in particularly important cases with the assistance of Europol, Interpol and Eurojust.

These solutions cannot be used to solve all the problems mentioned above. Getting in touch with these companies, as mentioned in the legislation, and getting the appropriate answer could be the real solution. But this could only be done by a direct request to the companies concerned.

Cases where the accused person stores the data in a cloud can be problematic as well, because during a house search it is not possible to know which country the data are stored in.

Solution:

- If the suspect is prepared to cooperate, they can be asked to search for the relevant data and give the data to the authorities of their own free will. The suspect cannot be forced to cooperate, but if they are prepared to hand over the requested data, this act can be considered as a testimony which is a mitigating circumstance (the suspect must be informed about this).

- If somebody else is authorised to obtain those data, then that person may be asked to provide the data to the authorities.

- Sometimes the data can be obtained from the cloud with the help of the service provider, in the form of a request for international procedural legal assistance.

There are some developments that help electronic communications service providers (operated by the National Media and Info communications Authority) to make the unlawful content available with the support of the content delivery network of the Technical Support System. Further developments are expected by the end of the year.

5.4.4. Perception of Hungary with regard to the legal framework to combat cybercrime

The rules of the Hungarian CC on jurisdiction (theory of unity of action, universal jurisdiction) and the rules of the CPA on the obligations relating to data preservation and seizure provide an appropriate framework for prosecution. International cooperation can be established on the basis of the CoE Cybercrime Convention or with the EU MS on the basis of the rules contained in the EU Act and with other States on the basis of the Act on International Cooperation (Act XXX of 1996).

The investigating authorities try to cooperate with foreign law enforcement authorities in cases of cybercrime. All channels of communication are used for the purposes of cooperation. These channels can be personal contacts, or the network of attachés, EUROPOL and INTERPOL channels, the 24/7 contact point lists and requests for legal assistance.

When it comes to foreign data collection by the investigating authorities, the challenge lies in the fact that it is very time-consuming. There is no known information channel - i.e. one that involves contacting the provider without coercive measures - that can ensure data exchange (IP address, email address and other data of the user) in the expected timeframe. This means that it can take several days or even weeks in the case of cybercrime. A further problem is if the provider is located outside the EU. In Hungary criminals intentionally use services (e.g. Gmail, Hotmail) which are operated by providers who do not cooperate with European investigating authorities.

Since direct requests for data do not work properly, a request for legal assistance is the only solution left, but it is very time-consuming. New international channels should therefore be initiated, to ensure that data can be swiftly requested directly from the service providers.

In order to facilitate the request for legal assistance, the rules of procedure should be refined: because the technical implementation is not sufficient, the procedures are very slow and in some cases the answer comes too late. Consideration should be given to using English as the common language of communication, because translation takes too long and staff with the appropriate knowledge must be selected within each body to accomplish these tasks. However, this will not be the final solution, since the problem of inappropriate communication with non-EU countries is still unsolved. Furthermore, the information regarding the offences is stored in countries far away which are not willing to cooperate properly.

It must be noted that according to the experiences of a judge in this field (working at a court with the highest number of cases), with the exception of one or two phishing or defacement attempts, serious cybercrime offences were not committed in Hungary. Most of the above-mentioned offences do not fall within the scope of Article 375 and Articles 423 - 424 of the CC since these are mostly cases of defamation committed on social media sites.

Hungary's regulations provide adequate options regarding the investigation and criminal procedure in cases where a cybercrime offence is committed outside Hungary. The biggest challenge is when further steps cannot be taken because no answer is given to the request for international procedural legal assistance sent to a third country (e.g. the USA), as mentioned earlier in section 2.C.3.

In the case of e-evidence, the data are stored (in most cases) on servers operated by companies with a head office based in the United States of America. Since the request for legal assistance sent to the United States of America must be based on facts which are beyond reasonable suspicion, submitting the appropriate request for legal assistance is sometimes impossible. In this connection it must be noted that a request for legal assistance regarding the collection of e-evidence is nearly always required during a phase of the investigation which is based on reasonable suspicion of a lower level.

Further problems occur in situations when the traffic data are collected directly from the owner of the server, but the owner (referring to their own rules of procedure) informs the subscriber (the offender) of this fact. This must be avoided from the point of view of the investigation. To avoid a situation of this kind, the Hungarian authorities must send a request for legal assistance to the United States of America and after this the concerned authorities of the USA can take out a federal court order to prohibit the sharing of information with the offender. To prevent the deletion of data, a data retention request can be made (in the event of an ongoing criminal offence) as part of police cooperation (for a period of 90 days, which can be extended for a further 90 days), but a request for legal assistance is needed in this case as well. During terrorist-related offences, hostage-taking situations and when life or physical integrity are at risk, a swift response can also be requested from the attachés of the Federal Bureau of Investigation.

According to the national authorities, it would be beneficial to initiate a direct dialogue with service providers, who in any case provide access to the data, but in order to achieve the desired results this must be done within a joint, EU framework and not by amending national law.

5.5. Conclusions

- The Hungarian legal framework in the area of cybercrime was established according to the principles and benchmarks laid down in the Council of Europe Convention on Cybercrime (the Budapest Convention) and Directive 2013/40/EU on attacks against information systems (the Cybercrime Directive 2013).

- Hungary has transposed into national law Directive 2011/93/EU on combating sexual abuse and sexual exploitation of children and child pornography.

- However, Hungary has not yet ratified the additional Protocol of the Council of Europe Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

- The Convention on Cybercrime entered into force on 1 July 2014 and gave rise to several changes in Hungarian national law. In a nutshell, the Hungarian Criminal Code (CC) was amended in order to criminalise new types of conduct, such as:

  the unlawful violation of a computer system or computer data; the bypassing of technical measures designed to protect a computer system. In the same context, several existing substantive provisions were clarified (for instance, unlawfully gaining access to private secrets or misuse of illegal pornographic material). However, the realistic representation of a minor engaged in sexually explicit conduct is not a criminal offence.

- In the same line, the Code of Criminal Proceedings was amended and new rules concerning preservation and gathering of e-evidence were introduced. From a procedural point of view, Hungarian law allows for the most important investigative techniques and measures specific to this area of criminality.

- Investigations benefit from a large range of procedural measures and investigation techniques such as urgent searches, easy identification of an IP address following a formal police request (answer provided within one hour), monitoring and wiretapping that seem to be effective for the investigation of cybercrime. However, these investigation techniques can only be used in certain serious cases, and the prosecutor and/or investigator have to provide due justification that this method of investigation was absolutely necessary in order to convince the court to confirm the measure.

- National law does not provide for specific rules regarding assessment of e-evidence. The absence of regulation on the methodology of collection and presentation of e-evidence before the court does not seem to hinder the effective prosecution of cybercrime cases, since the admissibility of e-evidence falls within the general evidence regulations.

- Hungary has quite extensive jurisdiction over criminal offences. In fact, besides the application of general principles governing jurisdiction, such as territoriality and nationality principles, Hungarian criminal law applies to any criminal offence to be prosecuted under an international treaty ratified by an act of parliament (universal jurisdiction principle).

- Moreover, the principles of both nationality and territoriality have quite wide formulations. Nationality extends to any act committed by a Hungarian national abroad which is considered to be a criminal offence under Hungarian law (even if the law of the *locus delicti* does not criminalise such act); territoriality, through the application of the theory of unity of action, extends to any criminal offences where any of the constitutive elements of such offences (criminal conduct, effect/result, etc.) take place in the territory of Hungary.

- Under those circumstances, potential conflicts of jurisdiction may arise and, in order to offer the appropriate legal solutions, Hungary has adopted provisions in line with Council Framework Decision 2009/948/JHA on the prevention and settlement of conflicts of jurisdiction in criminal proceedings.

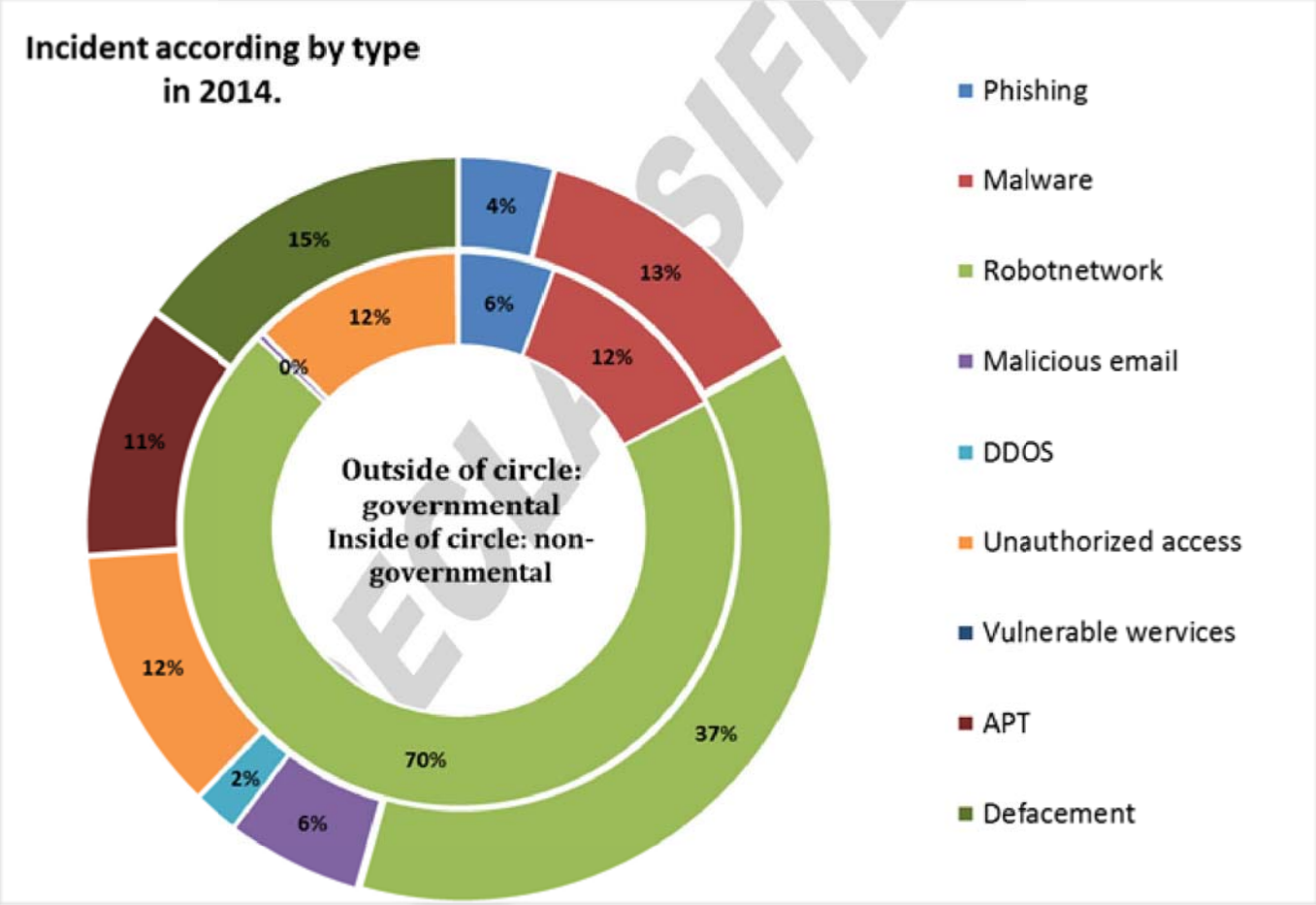
- Forensic activities are managed with a large range of partners in the private sector: specialised institutes, hackers academy, etc.

6. OPERATIONAL ASPECTS

6.1. Cyber attacks

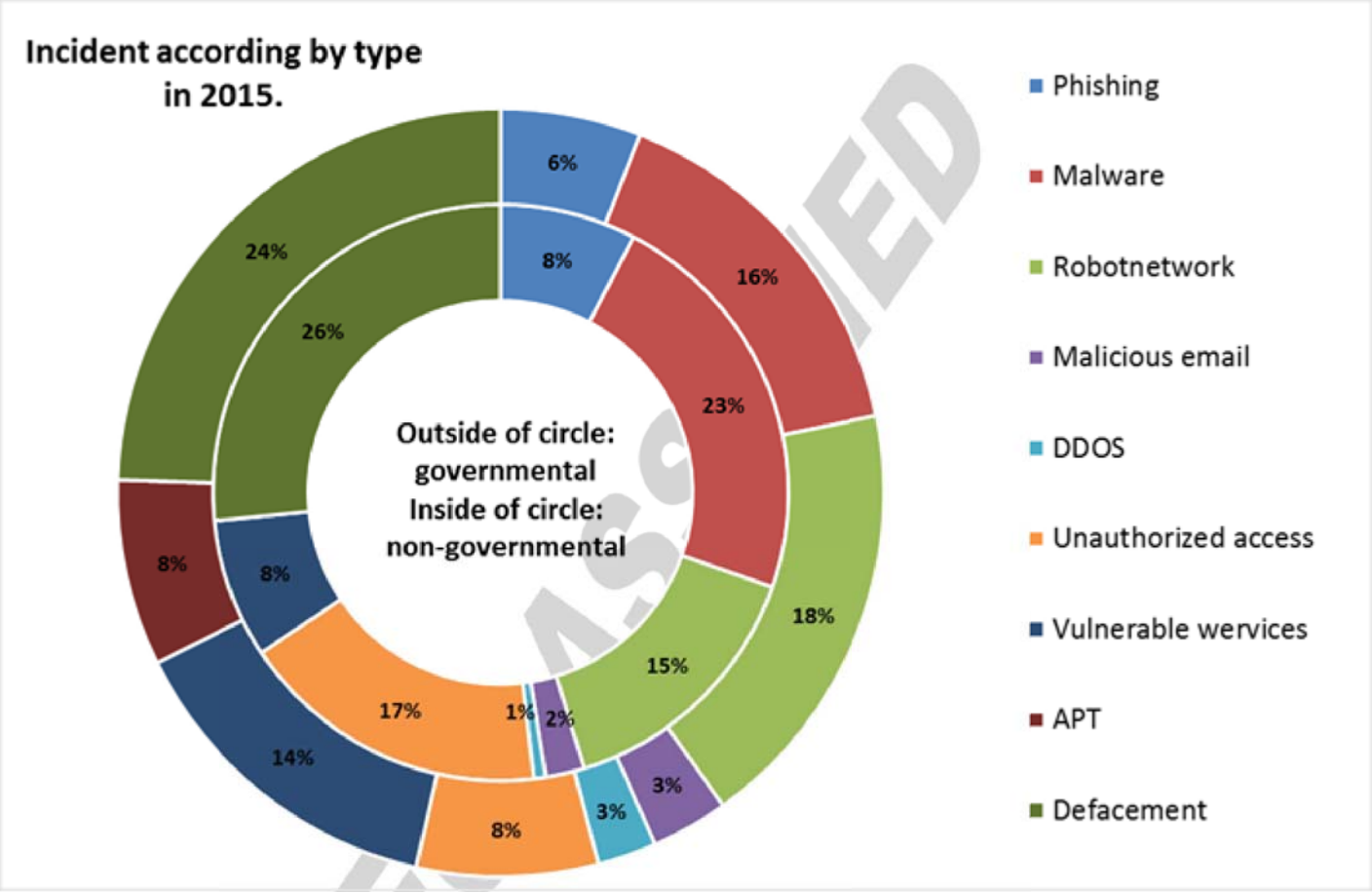
6.1.1. Nature of cyber attacks

As the diagram shows, in 2014 the GovCERT was aware of several incidents against both non-state and local governmental organisations. In both cases (governmental and non-governmental) the majority of incidents involved robot networks. Furthermore, in the governmental sector, there were several incidents of malware and defacement, while in the non-governmental sector the malware and the unauthorized access were usual.



The threats and incident notifications for GovCERT-Hungary in 2015 are shown in the diagram below.

In 2015 defacement was the most recent incident in both sectors. A significant percentage of incidents also involved the robot network and malware, in both the governmental and the non-governmental sector.



6.1.2. Mechanism to respond to cyber attacks

The level of protection of national information systems has been significantly developed in the past few years; however, in order to provide a comprehensive approach, there is still much work to be done in the future as well. A proper level of security cannot be established simply by reorganising the institutional framework and developing the operational and security systems used by those institutions. For systems with security shortcomings, the level of safety should be consistently increased in line with the law on information security. For new systems, particular attention should be paid to and sufficient financial support should be provided for establishing appropriate information security. Raising awareness at all levels must be increased – among leaders, system developers, users – since protecting those systems by technical tools alone would entail extremely high costs for the State.

Security-conscious behaviour and safety improvements are needed as well as appropriate institutional frameworks - including the National Cyber Defence Centre - in order to ensure a high level of cyber security.

Common rules on disaster management in a decree of the Ministry of the Interior lay down the rules for critical infrastructure protection as well. According to this decree (62/2011), the police, the Hungarian prison service, the Constitution Protection Office, the National Security Special Service and the Counter-Terrorism Centre are responsible for disaster management, coordinated by the National Directorate-General for Disaster Management at the Ministry of the Interior (NDGDM). They cooperate in building up the critical infrastructure protection system; they also take part in the identification procedure and provide data for these tasks.

In cases in which the perpetrator is identified as being foreign, mutual legal assistance will be used if this is expected to lead to further progress in the case and information cannot be obtained from Hungary. It is a principle that international procedural assistance will be requested during the investigation, if all the evidence is detected in Hungary and it is impossible to go forward without the result of legal assistance.

In cases in which the perpetrator is identified as being foreign and there is no, or if is Hungarian victim or the damage is not significant, Hungary may propose that the criminal proceedings be conducted in the country in which the perpetrator is living.

Hungary has never suffered any large-scale cyber attack, so fortunately there is no real experience of this. The legal background is well developed and possibilities for cooperation in the framework of mutual assistance in procedural or enforcement matters are ensured both at EU and international level.

6.2. Actions against child pornography and sexual abuse online

6.2.1. Software databases identifying victims and measures to avoid re-victimisation

The High-Tech Crime Unit in the Corruption and Economic Crime Division of the Riot Police's National Bureau of Investigation has access to the INTERPOL ICSE (International Child Sexual Exploitation image database) system. This image database is constantly used during the investigative work. The Unit plans in the long run to increase the number of colleagues who have access to INTERPOL ICSE. Cooperation and coordination is well-balanced and operates well with international partners. Hungary does not have a separate domestic image database, nor do we regard it as necessary.

The removal of photos and videos depicting the sexual exploitation of children in the framework of criminal proceedings is possible at the end of the proceedings as a criminal law measure, by which the court orders that the electronic data be rendered permanently inaccessible. During the proceedings the investigating judge – upon a motion by the prosecutor based on a proposal by the investigating authority – may issue an order to render electronic data temporarily inaccessible (requiring either the temporary removal of electronic data or the temporary prevention of access to electronic data).

It must be noted that cooperation between the police and the majority of domestic web hosting service providers is exceptionally good, and the web hosting providers often remove illegal content promptly and voluntarily on the basis of notification by the police.

In order to make photos and videos depicting the sexual exploitation of children inaccessible, a guide on how to apply the legal and technical possibilities of the INTERPOL 'Worst of' list (the collection of links containing child pornographic material) in Hungary has started to be compiled under the coordination of the National Media and Infocommunications Authority. The essence of this is to ‘block’ the links contained in the database at the level of the internet service providers.

6.2.2. Measures to address sexual exploitation/abuse online, sexting, cyber bullying

Sending images or videos containing sexual content with child pornography via the internet or mobile phone (sexting) is subject to criminal punishment based on Article 204 of the Hungarian Criminal Code. If such content describes adults, it is not a criminal offence.

As in other EU Member States, electronic harassment (cyber-bullying) is not a specific infringement (a separate criminal offence) in the Hungarian Criminal Code. Such acts are evaluated under the facts of harassment (Article 222 of the Hungarian Criminal Code). Under such facts the behaviour concerned is a regular, persistent harassment, i.e. it must be a repetitive or a permanent active behaviour. Bothering and harassing types of action may be displayed in various forms, collectively named as 'disturbance' in the law. Disturbance can be any kind of activity causing concern that can make one's everyday life more difficult or influence it negatively. The form of disturbance that takes place is irrelevant; thus, it may include harassment in person, by phone, in text messages or emails or even any threatening, defamatory or vituperative/insulting message over various social media or using other opportunities offered by the internet.

The facts of harassment are subsidiary, i.e. the perpetrator may be charged with this criminal offence if it is not combined with other more severe offences. It must be emphasised that, due to the personal nature of this offence, it is punishable only on the basis of a private motion, which means criminal proceedings may only be initiated if the authorised person reports the event to the police.

In an effort to improve legal regulations on actions against online threats to minors, the National Media and Infocommunications Authority (NMHH), in cooperation with the Ministry of Public Administration and Justice, developed Act CCXLV of 2013 on the Amendment of Specific Acts to Protect Children (Second Law Package for Child-friendly Justice).

In order to facilitate the growing popularity of child protection filtering software and parental supervision applications as well as child-friendly online content, the Act requires internet access and service providers, as of 1 July 2014, to provide free-to-download child protection filtering software and include information on the availability and use of filtering software in their general terms and conditions and compile information material relevant to filtering software.

In an effort to facilitate fast access to server hosts if any illegal online content is published, the Act requires service providers to display the contact information of the web hosting service provider on their website.

Based on the Act, any information that does not qualify as media content but can potentially harm minors' mental, spiritual, ethical or physical development, with a strong emphasis being placed on the direct and natural representation of violence or sexuality, may only be published with a warning sign and with such tags in the source code of the sub-page that clearly refers to the content category and is detectable to child protection filtering software. The Act, which came into effect on 1 March 2014, established the Internet Roundtable for Child Protection (hereinafter: Roundtable), an advisory, consulting and counselling body of the President of NMHH designed to facilitate compliance and enforcement of legislation on ensuring the healthy development of minors with regards to media content accessible via information society services and electronic communication services as well as information that does not qualify as media content based on Act CIV of 2010 on the Freedom of the Press and the Fundamental Rules of Media Content. The NMHH performs the tasks pertaining to setting up and operating this body. The Roundtable is not bestowed with powers to craft mandatory legislation. However, in the interest of promoting legal norms via self-regulation more effectively, it is authorised to issue statements and recommendations. Ever since it was founded, the body holds sessions bimonthly and discusses topics related to online child protection. The Roundtable issued its first recommendation on 23 April 2014 on the warning signs to be used for online content and services harmful to minors (age rating warnings) and child protection filtering software available for download at:

http://nmhh.hu/dokumentum/162986/szuroszoftver_ajanlas.pdf

By extending the rules of the 'notification-removal' procedure to cases involving privacy violations against minors, the Second Law Package for Child-friendly Justice created an opportunity for minors who are beneficiaries of privacy rights and those minors' legal representatives to take effective measures to protect minors' privacy even before or instead of any civil or criminal law proceedings. The beneficiary minors or their legal representatives may appeal to the Internet Roundtable for Child Protection if the service provider violates the rules of the notification-removal procedure or refuses to remove the online content due to insufficient grounds.

In order to protect minors, the Act requires that all computers with internet access located in public education institutions and public libraries be equipped with child protection filtering software.

Under the Act, distributors of computer games who had previously failed to join the Pan-European Game Information (PEGI) system are required to use an age rating warning sign on any game software with content potentially harmful for minors.

The National Media and Infocommunications Authority (NMHH) organises a lot of activities and campaigns dedicated to children, as they are the most vulnerable category:

a. Fliers and publications:

http://nmhh.hu/cikk/168141/Mediaertesfejleszto_oktatofilmek_es_szakkonyvek_az_NMHHtol

b. Equipment enabling technical filtering:

(see: http://internethotline.hu/tart/index/108/Szuroszoftverek)

Free-to-download filtering software in Hungarian: http://gyermekbarat.nmhh.hu

In order to facilitate more comprehensive online protection of children and implement proper protective mechanisms to fight online threats against children, the Hungarian Parliament passed the Internet Child Protection Act in December 2013 (Act CCXLV of 2013 on the Amendment of Specific Acts to Protect Children).

Among other things, the Internet Child Protection Act amended Act C of 2003 on Electronic Communications (Electronic Communications Act), Article 149/A (1) of which stipulates that, as of 1 July 2014, internet access service providers are required to offer some child protection filtering software on their websites that is free to download and use. The filtering software must be in Hungarian, easy to install and use, free to download from the website of the service provider and free to use. Thus, the persons - and parents - have no financial obligation whatsoever regarding the downloading and use of the software.

In addition to introducing the above obligation, the Internet Child Protection Act also established the Internet Roundtable for Child Protection (Roundtable) as the advisory, consulting and counselling body supporting the President of the National Media and Infocommunications Authority (NMHH) on issues pertaining to online child protection. The Roundtable issued its first recommendation on 23 April 2014 on the warning signs to be used for online content and services harmful to minors and child protection filtering software. The full text of the recommendation is available at the link below:

http://nmhh.hu/dokumentum/162986/szuroszoftver_ajanlas.pdf

The Roundtable believes that it is important that parents receive sufficient help in installing and configuring the filtering software. To that end, the Roundtable in its recommendation also pointed out that it expects service providers to offer installation guides and Hungarian language videos on their websites to enable even parents less skilled in information technology to install and configure the filtering software.

Based on the above, the download link of the filtering software will be available on the websites of internet access service providers. Henceforth, service providers are expected to make the guides and videos supporting the installation and use of filtering software available on their websites.

c. YouTube videos:

Where is Klaus? (Wo ist Klaus?)
https://www.youtube.com/watch?v=1HhD9P3qBCo

Facilitating media awareness among 6–9-year-olds:

New, Newer, Newest
https://www.youtube.com/watch?v=bfhIhQbkkgI

Click on, Burglars!
https://www.youtube.com/watch?v=No_gBnqP0z0

Heroes and Hotshots
https://www.youtube.com/watch?v=XmZy-UpJ0LQ

Who's the Coolest?
https://www.youtube.com/watch?v=rfWSsG8aIN0

Facilitating media awareness among 10–12-year-olds:

How can you live without it?
https://www.youtube.com/watch?v=DJMELEccylU

Mirror, mirror
https://www.youtube.com/watch?v=mcjaYJJEAgI

You're not cool, buddy!
https://www.youtube.com/watch?v=-y3dLmI_qII

Facilitating media awareness among 13–16-year-olds:

Flash or not to flash?
https://www.youtube.com/watch?v=t56c6fWDk24

The sharer
https://www.youtube.com/watch?v=wLUEoNKokFk

Beauty and the Beast
https://www.youtube.com/watch?v=l6pbjL3NdoU

Anti-Bullying Programme of the Public Foundation for a Responsible Society:

The aim of the Anti-Bullying Programme (*Megfélemlítés Elleni Program* - MEP) of the Public Foundation for a Responsible Society is to prevent and stop bullying and cyber-bullying in schools, kindergartens, at work and in relationships. The programme was developed in 2013 and it strives to educate the public on Responsible Digital Citizenship in order to prevent the victimisation of online users. It seeks to change attitudes and values in dealing with and witnessing bullying, cyber-bullying, workplace bullying and cybercrime. In addition to potential targets, communication efforts urge bystanders and witnesses to act and break their silence to create a crime-unfriendly environment. The colleagues of the National Crime Prevention Council also participated in the elaboration and implementation of the programme. The National Crime Prevention Council supported the re-printing of the programme handbook.

MEP is divided into two major strands: the Event Handling strand and the Institutional strand. The Event Handling strand includes prevention practices, education, training and information segments on how to prevent, recognise the effects of and handle bullying and cyber-bullying as well as the organisational segment on implementation. As well as preventive communication to the potential target, priority is also given to getting bystanders and witnesses to report bullying, cyber-bullying and cybercrime, thereby relieving the targets and victims of much of the responsibility. An application known as Anti Bullying Integrated Solutions (ABIS) aids online reporting, proof, documentation and monitoring.

Strong emphasis is placed on preventing introductory behaviours by teaching effective and aggression-free communication. As part of efforts to prevent the development of bullying and cyber-bullying, introductory behaviour such as school violence and aggression are also handled via mediation and conflict resolution. Restorative practices are applied to restore the initial (pre-aggression) state.

The Institutional strand, conducted in parallel with the Event Handling strand, focuses on raising public awareness, obtaining funding and lobbying the government in order to prioritise national roll-out and sustainability. Legislative lobbying takes place in order to amend the relevant laws and regulations and to introduce new anti-bullying and cyber-bullying laws.

The webpage of the programme provides help for persons in need:

http://www.megfelemlites.hu/#!help/ceam; www.interneteszaklatas.hu

The police can carry out most of the investigative measures, but victims under 14 years old must be heard only by prosecutors or judges (unless the hearing is a matter of urgency). In order to avoid re-victimisation, victims are only heard once during the whole proceedings. However, in exceptional circumstances, the judge may decide that a new testimony shall be given in court. If victims aged under 18 are to be present during the trial, they can refuse to stand face-to-face with the defendant. Several police stations in the country are equipped with child-friendly rooms in which to conduct hearings of victims. All interviews with children are video-recorded, which gives the option of playing the questioning session in court during the trial instead of interviewing the child victim over and over again. It is a really positive sign that Hungarian law enforcement officers are doing their best to protect children who have already become victims of crimes, to ensure that they are not interviewed several times over.

6.2.3. Preventive actions against sex tourism, child pornographic performance and others

There is operational information referring to some isolated cases but there is no information or notable experience about specific cases, or rather about the significant presence and activities of Hungarian citizens abroad or foreign people in Hungary for such purposes. Where they receive information on isolated cases, the police take all necessary steps to prevent such crimes and ensure that they do not get committed. Information from foreign law enforcement agencies is received and handled by the International Criminal Cooperation Centre (NEBEK) and in some cases by the High-Tech Crime Unit in the Corruption and Economic Crime Division of the Riot Police's National Bureau of Investigation. Moreover, they are often helped by local law enforcement agencies. The activities listed in Article 21 of Directive 2011/93/EU are also prosecuted under criminal law, i.e. the Hungarian Criminal Code incriminates these activities.

Article 2(3) of the Global Code of Ethics for Tourism of the UN World Tourism Organisation (UNWTO) states that 'The exploitation of human beings in any form, particularly sexual, especially when applied to children, conflicts with the fundamental aims of tourism and is the negation of tourism; as such, in accordance with international law, it should be energetically combatted with the cooperation of all the States concerned and penalized without concession by the national legislation of both the countries visited and the countries of the perpetrators of these acts, even when they are carried out abroad'.

The Code has been disseminated by the Ministry responsible for tourism and by national professional associations among tour organisers (e.g. translation into Hungarian, publication, website access). The Code is not binding, but encourages an ethical business attitude and envisages criminal sanctions which are in accordance with the provisions of the Hungarian CC.

Specific measures to counteract real-time web-based child pornographic performance do not exist because the national authorities do not really see how they can be implemented from a technological point of view.

This type of 'live stream' criminal activity can be punished under point (a) of Subsection (1) of Article 204 (’Child pornography’) of the Criminal Code (which states that 'Any person who… obtains…'). However, the national authorities have not yet experienced such cases in Hungary.

The following websites and applications are related to the specific preventive measures:

http://internethotline.hu/ - National Media and Infocommunications Authority (NMHH)

http://www.biztonsagosinternet.hu/ - National Infocommunication Services Ltd. and International Children's Safety Service (a Hungarian association)

Helpline - www.kek-vonal.hu (Kék Vonal Child Crisis Foundation)

HelpApp – Unicef Hungary

Based on the cooperation agreements signed between the Hungarian National Police Headquarters and the National Media and Infocommunications Authority (NMHH), as well as between the Hungarian National Police Headquarters and National Infocommunication Services Ltd., it is the High-Tech Crime Unit in the Corruption and Economic Crime Division of the Riot Police's National Bureau of Investigation which carries out the primary tasks with regard to public reports and notifications received by the two major Hungarian internet hotlines (http://internethotline.hu/; http://www.biztonsagosinternet.hu/). These tasks include evaluating the public report, ordering the investigation, determining competence and jurisdiction and, if appropriate, conducting the investigation.

Internet Hotline operated by the National Media and Infocommunications Authority (NMHH)

The NMHH has been operating the 'Internet Hotline' service since 22 September 2011.

The Internet Hotline (http://internethotline.hu) service is available to the public for reporting online content that is illegal or harmful to minors. Reports can be filed in the following case types:

- Content made accessible without permission
- Paedophile content
- Harassment
- Racist or xenophobic content
- Content portraying violence
- Content promoting drug use
- Content promoting, facilitating or inciting acts of terrorism
- Data phishing sites, content infected with viruses, spyware or worms
- Other content harmful to minors

Once a report is filed, it will be evaluated by the Internet Hotline personnel and if the reported content is found to be objectionable (i.e. either illegal or legal but harmful to minors), the operator of the online content or the affected server host is called upon to take the illegal content offline. The server owner (intermediary) removes the content either on the basis of Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services or based on the contract between the server owner and the person uploading the content: these service contracts usually stipulate that only materials and webpages that do not contain any illegal content may be uploaded to or hosted on the server.

In case of content that, while not illegal, is harmful or dangerous to minors, the Internet Hotline colleagues call on the operator of the website or the server host to clearly indicate on the website that it may be detrimental to minors.

It is important to stress that it is not the Internet Hotline's role to examine any online media content, such as online press, on-demand or other types of media content. If a report is filed on any infringing media content, it is the Media Council of the National Media and Infocommunications Authority which looks into the matter.

Achievements of the Internet Hotline

Over 3 000 reports have been received through the reporting interface of Internet Hotline since 2011. After being contacted by Internet Hotline, content and web hosting service providers have mostly ensured that often severely illegal content, such as child pornography recordings or other content violating the personal rights of minors, is made inaccessible.

In addition to reports on specific violations of the law, Internet Hotline has received a number of reports and inquiries regarding safe internet use. In such cases Hotline personnel inform the reporting party about the issues relevant to their questions, e.g. how to avoid online data theft, configure their privacy settings on social media websites, and protect themselves from online harassment, or about the available legal actions and remedies against online infringements.

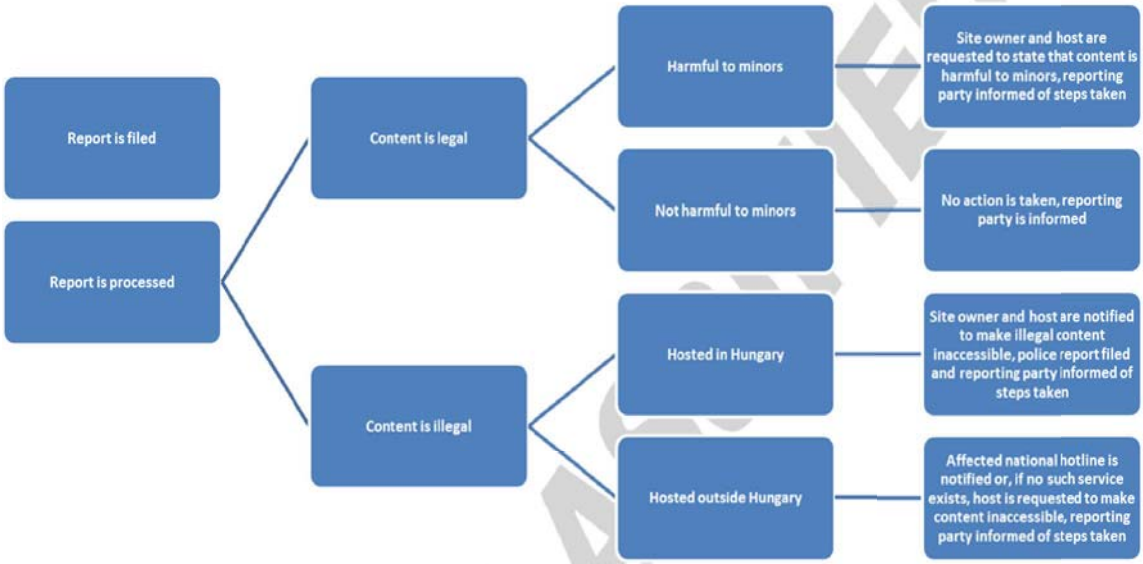
In the fight against illegal online content, the Internet Hotline continues to work closely with the Hungarian Police (with the National Police Headquarters).

The activities of the bodies receiving such reports are coordinated by the International Association of Internet Hotlines (INHOPE) at international level. This organisation ensures that paedophile content directed to Hungary but stored abroad can be removed from the internet. It is also notified if illegal content is stored on a Hungarian server. If the content is stored in the country of the reporting bodies, they call upon the web hosting service provider to remove the content and also communicate with the law enforcement authorities. The National Media and Infocommunications Authority joined INHOPE on 27 April 2012.

It is important to note that the experiences of Internet Hotline were put to use when drawing up legislation, e.g. in the law package on child-friendly online content at the end of 2013, and have been used ever since in the regulatory work and social responsibility activities in respect of online child protection.

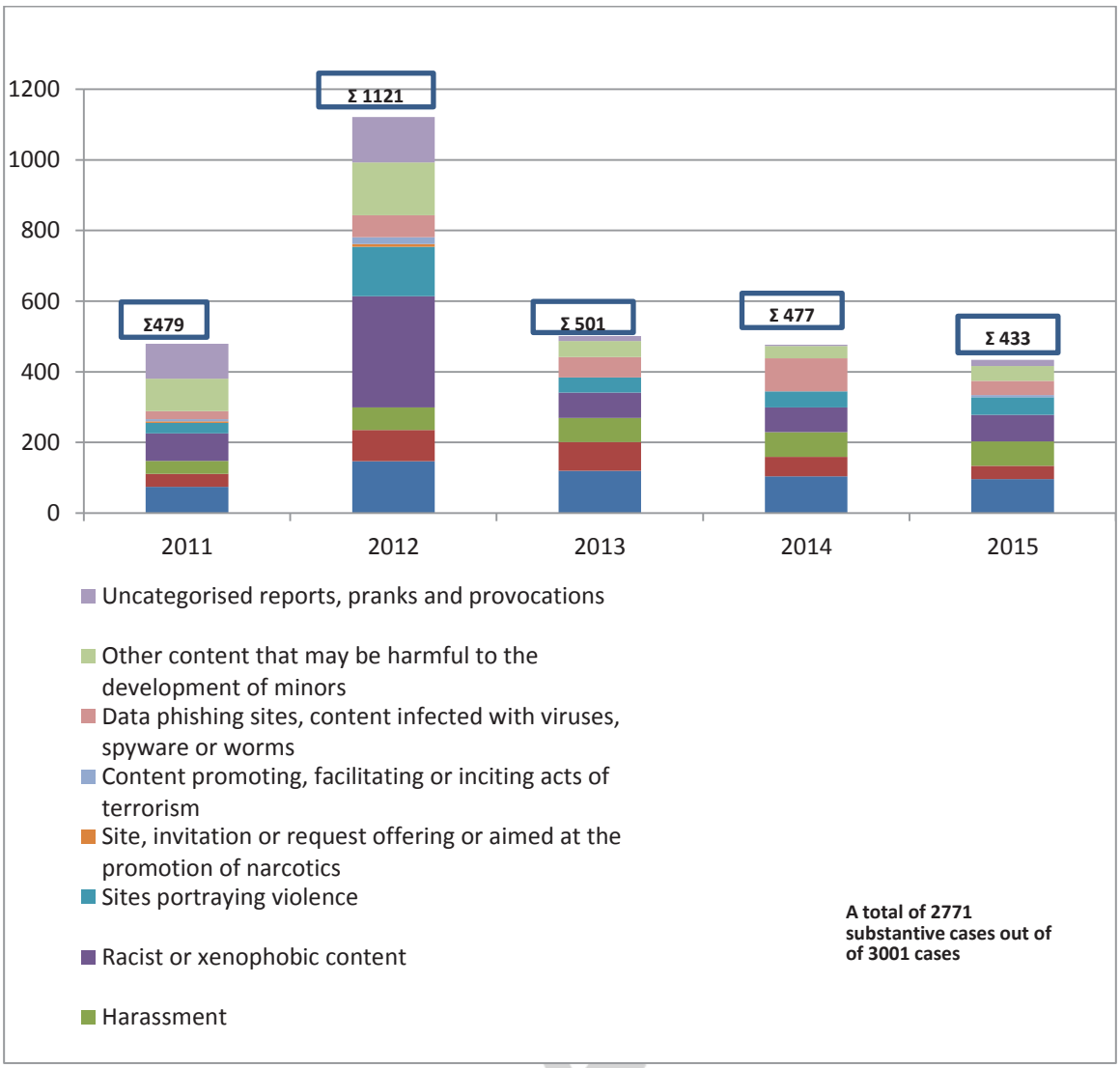
For more information on further child protection activities of the NMHH please visit http://gyermekbarat.nmhh.hu.

Hotline workflow, the process of managing incoming signals/reports:



Hotline statistics:

Number of reports since the launch of Internet Hotline (22.09.2011)



Overall, efforts to combat the sexual exploitation of children and minors and the fight against human trafficking are built on three pillars: victim support, law enforcement and prevention of victimisation. Protection of minors and children is a priority area of crime prevention. All children and minors can be potential victims, so awareness-raising and propaganda activities cannot be narrowed to certain groups of people. However, it can be said that the risks can be differentiated in a way which takes account of the fact that there are highly vulnerable minors and children. It is also important to emphasise that, in order to achieve the aims of awareness-raising activities, it is essential that training be provided for prevention professionals and members of the reporting system.

All this was taken into account when drawing up training plans, materials, and programmes targeting professionals as well as minors and children. Information and training for minors has been introduced at continuous, multiple levels, so children can participate in awareness-raising training courses from kindergarten until the end of secondary school. It focuses on developing skills and abilities that help minors to recognise emergency situations, reflect critically on the incidents and activate appropriate self-defence mechanisms. They will be able to recognise, decide, reject, avoid and ask for help in certain situations. When compiling the programmes, age characteristics are taken into account. The programmes are aimed at preventing all crimes against sexual freedom and sexual offences (sexual exploitation, sexual violence, sexual abuse, incest, pandering, living on earnings of prostitution, exploitation of child prostitution, child pornography, indecent exposure) in an indirect way.

The following programmes are available:

1. Elementary and high school police programme (a detailed description of the programme can be found under section 10.A.2)
2. The school advisory programme in crime prevention (IBT) was started in September 2013. The programme consists of preventive lectures and tasks and it gives immediate answers to the questions of teachers, children and minors. A direct professional relationship thereby helps to identify and handle the problems (e.g. endangerment). In the case of child prostitution, it is a very effective crime prevention tool because the advisors liaise with child protection bodies and civil organisations. They have the opportunity to get to know the parents, with whom they can recognise threats by building trust and confidence in each other. All the experts participating in the project were admitted to the programme after psychological pre-screening. All of them have higher education degrees, they are well-prepared, and highly motivated and have this type of personality that that helps to create a climate of confidence with teachers and minors and also with parents. Technical leaders (line-managers of regional police headquarters) help their work by publishing methodological assistance material such as the guide on 'Criminal procedure and police actions against minors and police measures to be applied in case of disappearances' produced by the Crime Prevention Department and Department of Children and Youth Protection of the Budapest Police Headquarters (BRFK).

3. Special crime prevention training programmes have been set up for teachers. The aim of the advanced training entitled 'Crime prevention in schools (competence-developing and methodological training)' is to prepare teachers to give lectures to children about crime prevention. The participants get to know crime prevention short movies and are taught to apply crime prevention multimedia materials. One of the crime prevention short movies shown to teachers is entitled 'Job advertisement' and was made in 2011. The detailed description of the programme can be found under section 10.A.2.
4. Children living in orphanages are more vulnerable to sexual exploitation and child prostitution, so special attention must be paid to them – bearing in mind that they usually come from a dysfunctional family, have behavioural or learning difficulties (ADHD syndrome) or suffer from other problems such as frustration, segregation or isolation. Dedicated coordinators of the regional police authorities maintain close contacts with these institutions.

The Hungarian National Crime Prevention Strategy (hereinafter known as 'the Strategy') deals with preventing and handling life situations endangering children (minor and child protection, preventing victimisation) including among others child prostitution. The implementing body of the Strategy is the National Crime Prevention Council, which also takes part in preparing the materials necessary for the work of the police officers as well as in training them.

There is a separate working group dealing with children's rights within the Hungarian National Authority for Data Protection and Freedom of Information (NAIH). In 2013 a free publication called 'Key to the internet world' (*Kulcs a net világához*) was created for parents, teachers and child protection specialists in order to help children's internet awareness. There is also a more colourful and simple version for young people. It is available online in Hungarian, English and French: http://naih.hu/adatvedelemr-l-fiataloknak--kulcs-a-net-vilagahoz--projekt.html

In 2014, a TV and radio campaign was launched through public interest advertisements, with the performance of a young pop singer.

As a project partner of the European ARCADES project, the NAIH drew up a training manual and a methodological manual on the topic of data protection in 2014-2016. These were shown to 200 teachers in a seminar held from 20 to 22 October 2015. In the framework of the project, teachers could present the 'best lesson about data protection' and win a study visit to Brussels together with their students.

http://naih.hu/arcades/dokumentumok.html

In November 2015, the Hungarian National Authority for Data Protection and Freedom of Information (NAIH) submitted a tender to the National Crime Prevention Council for the continuation of the 'Key to the internet world' programme, with the aim of compiling training material for police staff on the topic of data protection. It would also include training courses for police officers.

6.2.4. Actors and measures countering websites containing or disseminating child pornography

Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services (E-Commerce Act) allows for the removal of content violating a minor's privacy by calling on the intermediary to do so (Subsection (13) of Article 13).

In addition, under the e-Commerce Directive, the intermediary is held liable for the intermediated illegal content, including illegal content as defined by the Directive, if the service provider fails to take action to remove the content violating the minor's privacy rights. This provision indirectly contributes to the quick removal of such content (service providers usually remove such content shortly after being notified) (Articles 9–11).

As a whole, NMHH Decree No 19/2013 (X. 29) ensures compliance with Article 25 of the Directive by making online content with child pornography centrally inaccessible in a centrally coordinated system using the KEHTA database operated by the NMHH and its related functions.

I. Measures taken against illegal online content

- Rendering electronic data permanently inaccessible [Article 77 of the Criminal Code]
- Implementation of rendering electronic data permanently inaccessible [Article 324 of Act CCXL of 2013 on the implementation of penalties, measures, certain coercive measures and confinement due to infractions]
- Provision on the implementation of rendering electronic data permanently inaccessible by the permanent prevention of access [Article 596/A of the Criminal Proceedings Act]
- Rendering electronic data temporarily inaccessible [Articles 158/B-158/D of the Criminal Proceedings Act]
- Rendering electronic data permanently inaccessible and receiving its execution [Article 60/F–60/G of the Act on International Legal Assistance in Criminal Matters]
- Rendering electronic data permanently inaccessible and surrendering its execution [Article 60/F–60/G of the Act on International Legal Assistance in Criminal Matters]
- Procedural legal assistance [Chapter V of the Act on International Legal Assistance in Criminal Matters and Chapter IV of Act CLXXX of 2012 on criminal cooperation in criminal matters between the Member States of the European Union]

As of 2013, the Hungarian Criminal Code introduced rendering data published on the electronic communications network permanently inaccessible as a new type of criminal law measure (Article 77 of the Criminal Code). The reason for introducing this new category was that, even though the previous Criminal Code penalised offences committed by publication on the electronic communications network, i.e. on the internet (libel, defamation, harassment, preparation of terrorist acts, financing terrorism), nevertheless it did not provide for the inaccessibility of illegal content in cyberspace. This measure may be ordered if the data published on the electronic communications network constitutes a crime (it can be ordered for offences subject to both public and private prosecution), was used as a means to commit a crime or was created as a result of a crime committed.

In parallel with introducing the rendering of electronic data permanently inaccessible as a new criminal law measure, a new coercive measure was also necessary during the criminal proceedings targeting the prevention of continued online criminal activities and access to forbidden data content. This is how the Criminal Proceedings Act (Act XIX of 1998 on Criminal Proceedings) also incorporated provisions on rendering electronic data temporarily inaccessible (Articles 158/B–158/D of the Criminal Proceedings Act). The court has the power to render any data temporarily inaccessible, against which decision legal remedies may be sought. The court may order electronic data temporarily inaccessible only as a result of an offence of public prosecution, if any of the preconditions exist for ordering such data to be made permanently inaccessible, and this is required to prevent the crime from being continued.

Whether rendering the illegal online content permanently inaccessible in the final judgement or temporarily inaccessible as a coercive measure, the primary objective is to remove the electronic data from the web hosting server because it ensures that the illegal data content is removed. The court puts the web hosting service provider under an obligation to comply with such an order. First, the court calls upon the service provider to voluntarily comply with the order but, should they fail to comply, they will be coerced into doing so through the imposition of a large penalty of between HUF 100 000 and HUF 1 000 000.

If

- the Hungarian web hosting service provider cannot be coerced into complying even through the imposition of a fine, or

- the illegal content is at the disposal of a foreign service provider and the request for the removal of the illegal content within the context of international legal assistance in criminal matters yields no result within 30 days of the date of issue,

the court orders the prevention of access to content, i.e. the blocking of the data content, as a result of which the specific content would become inaccessible for Hungarian users in the course of internet service.

Blocking as a coercive measure as defined in the Criminal Proceedings Act may be ordered only for a limited group of crimes: drug trafficking, inciting substance abuse, aiding in the manufacture or production of narcotic drugs, criminal offences with drug precursors, illegal possession of new psychoactive substances, child pornography, crime against the state, terrorist act or financing of terrorism. According to the Criminal Code, rendering such content permanently inaccessible by blocking may be ordered in the case of any crime if there are certain additional preconditions.

Considering the globalisation of IT networks, the existing system of cross-border data transfer via the internet and the potentially broad access to data content made available over the World Wide Web, fast and reliable international cooperation is needed to prevent the abuse of IT systems, networks and data. Even identifying the location of the storage of the illegal data is often a difficult task and may require a consultant or expert or even criminal law cooperation.

In view of the above, and for the sake of smooth international cooperation, the Act on International Legal Assistance in Criminal Matters introduced certain amendments as of 1 July 2013 to enable the Hungarian authorities to use the procedural or enforcement legal assistance available to render electronic data temporarily or permanently inaccessible if the website is hosted by a foreign web hosting service provider, as well as to enable the Hungarian authorities to fulfil such foreign requests for legal assistance if the web hosting service provider is Hungarian.

II.

Subsection (13) of Article 13 of the E-Commerce Act (Article 30 (1) of Act CCXLV of 2013) and Articles 9–11 therein

Articles 1–5 of NMHH Decree No. 19/2013 (X. 29)

Among other things, the Internet Child Protection Act (Act CCXLV of 2013) stipulates that as of 1 July 2014, internet access service providers are obliged to offer some child protection filtering software on their websites that is free to download and use. The filtering software must be in Hungarian, easy to install and use, free to download from the website of the service provider and free to use. The filtering software in Hungarian can be easily customised and used on mobile phones, computers and tablets alike and is available free of charge at: www.gyermekbarat.nmhh.hu.

The removal of photos and videos depicting the sexual exploitation of children in the framework of criminal proceedings is possible at the end of the proceedings as a criminal law measure, by the court applying and ordering electronic data to be rendered permanently inaccessible. During the proceedings the investigating judge – upon a motion by the prosecutor based on a proposal by the investigating authority – may issue an order to render electronic data temporarily inaccessible (requiring either the temporary removal of electronic data or the temporary prevention of access to electronic data).

It should be noted that cooperation between the police and the majority of domestic web hosting service providers is exceptionally good, and the web hosting providers often remove illegal content promptly and voluntarily when notified by the police.

The next stage is to issue a court order to oblige web hosting service providers to remove such data. The procedural framework for this in urgent cases is defined in Articles 158/B–158/D of the Criminal Proceedings Act as a special coercive measure.

This is basically a two-stage procedure. First, the service provider is called upon to comply voluntarily. If that fails to happen, action for rendering data inaccessible (i.e. blocking through the NMHH) may only be taken if the criminal proceedings involve a severe criminal offence such as child pornography.

Quick reaction is facilitated by preliminary enforceability granted under Subsection (5) of Article 215 of the Criminal Proceedings Act.

In the case of 'normal' proceedings, the court may order the same in the final judgement, the enforcement of which occurs using the two-stage method described above.

If the police receive information about content stored by a foreign web hosting service provider, they use all available channels of international police cooperation to notify foreign peer authorities about illegal websites or content. In addition to direct channels, the police generally use EUROPOL and INTERPOL.

In this case, judicial authorities act in accordance with the procedure outlined in the Act on International Legal Assistance in Criminal Matters.

The activities of the bodies receiving reports on child pornography are coordinated by INHOPE (International Association of Internet Hotlines) at international level. This organisation ensures that paedophile content directed to Hungary but stored abroad can be removed from the internet and also that the organisation is notified if illegal content is stored on a Hungarian server. The Internet Hotline operated by the National Media and Infocommunications Authority joined INHOPE on 27 April 2012.

Within the police, the central unit specialised in fighting against cybercrime is the High-Tech Crime Unit in the Corruption and Economic Crime Division of the Riot Police's National Bureau of Investigation, whose activities focus in particular on reconnaissance and investigation of online sexual exploitation of children as well as international relations.

Among regional police authorities, the Children and Youth Protection Unit of the Criminal Division of the Budapest Police Headquarters (BRFK) handles the investigations of serious online child sexual exploitation cases committed in the capital but often containing international elements, as well as other crimes not linked to cybercrime.

Given that the police are the general investigating authority, the local, regional and central bodies of the police all take part in the fight against online sexual exploitation of children. Normally, and in easier cases, the investigative units of local and regional police headquarters take action; however, in prioritised, organised crime and/or international cases, it is the High-Tech Crime Unit in the Corruption and Economic Crime Division of the Riot Police's National Bureau of Investigation which carries out investigations.

There are two internet hotlines in Hungary. Both of them are members of INHOPE and both of them report cases of internet violation to the Cybercrime Department. They are also both advertised as an internet hotline. The evaluation team recommends that the national authorities develop or create a new hotline specifically dedicated to gathering reports from the public, without any obligation to disclose personal data.

A case management system could be useful to deal with all forwarded cases. The hotline should also be seriously involved in most awareness-raising campaigns, along with the police.

6.3. Online card fraud

6.3.1. Online reporting

If individuals become victims of bank card fraud, they primarily claim for compensation of damages, so they contact their financial institution. After that the financial institutions usually examine to what extent the customer is responsible for the committing of the offence due to his or her failure to take the reasonable steps essential for data security. If the financial institution does not hold the customer responsible for the losses, compensation will be paid. In such cases the individuals usually report the crime only if the financial institution imposes this as a requirement for compensation.

In order to protect their market position, the financial institutions often decide to compensate the damage caused because an attack against a financial institution may result in the loss of customers, so it is more profitable to compensate the loss. If the financial institution does not compensate the loss, customers typically report the crime when the loss is considerable and they try to claim for damages through the criminal procedure.

In more serious cases or whenever they have relevant information about the perpetrator which may result in the success of the investigation, the financial institutions report the crime themselves.

The Hungarian National Bank publishes data quarterly on abuse of bank cards (the statistics contain data between 2010 and the first quarter of 2015):

http://www.mnb.hu/statisztika/statisztikai-adatok-informaciok/adatok-idosorok/xiv-penzforgalmi-adatok/penzforgalmi-tablakeszlet

6.3.2. Role of the private sector

The High-Tech Crime Unit in the Corruption and Economic Crime Division of the Riot Police's National Bureau of Investigation works in close cooperation with the Hungarian Banking Association. In recent years, in order to combat fraud, they have published warnings and information for the public, in all major cases affecting a large number of people, on attempts at illegal bank card data gathering through the internet. These warnings were published, with minor alterations, on the main online banking webpages of most Hungarian financial institutions.

Moreover, in more serious cases, the Hungarian Banking Association organised large-scale media campaigns to provide the quickest and most effective information for the public. In some cases, the Bank Security Units reported these abuses and new ways of committing offences to the High-Tech Crime Unit as soon as the crime started to be committed ('day zero').

In practice, nearly all bank cards in Hungary are equipped with a chip, which forms the basis for card authorisation throughout the ATM and POS network. This means that cards issued in Hungary are not vulnerable to fraud through the magnet strip, in either Hungary or the EU. Unfortunately, in countries outside the EMV zone, there have been illegal cash withdrawals using bank card data copied in Hungary. This was possible because as yet none of the financial institutions in Hungary have introduced geo-blocking technology.

Each financial institution has a different level of authorisation for online transactions, and this varies widely. Some financial institutions require only a static password in order to use online banking and do not even require a dynamic password for purchases through the internet using bank card data. The bank card companies are trying, with varying degrees of success, to orientate these institutions towards more secure online bank card use.

Most domestic financial institutions expect internet traders to ensure that a dynamic password is also used for bank card authorisation (e.g. 3dsecure). There is a system - unique in the world - involving widespread use of text messages sent to customers after bank transactions in Hungary, which helps to alert them to any attempted fraud.

6.4. Other cybercrime phenomena

The equipment and capacity of law enforcement agencies differ depending on the authority (investigating authorities, prosecutors or courts) to which they belong.

The National Tax and Customs Administration and the police are in charge of conducting investigations, but some cases come directly under the responsibility of the prosecutor's office.

The National Tax and Customs Administration and the police both have special cybercrime units that use adequate tools (hardware and software) and are properly trained.

If an official of an authority not working for the special unit encounters a problem related to the gathering or recording of e-evidence, then they do not have direct access to equipment, software and know-how. However, these officials of the investigating agencies can ask for assistance at any time from the special unit belonging to their authority. Alternatively, they can turn to external experts as well.

In the prosecution service the investigating prosecutors and the IT personnel all receive proper training to prepare them to conduct the investigation on their own. If necessary, the prosecutor's office can also ask for help from the specialised units of the investigating authorities.

In addition to the above-mentioned task of investigation, the main duty of the prosecution service in cybercrime cases is to supervise investigations and present the indictment in court. To fulfil this task, the prosecutor also has to handle e-evidence, but they receive it in a form which can be accessed and evaluated using the equipment available to the prosecutor's office.

There are several training courses within the prosecution service to prepare colleagues for handling cybercrime cases, and there is generally close and direct contact with the investigating authorities, which makes it easier for tasks to be carried out successfully. If prosecutors responsible for a case cannot fulfil their tasks because of their lack of specialised knowledge, they can ask for help from colleagues who have more experience with such cases.

For the court – as for the prosecutor's office – the main goal is to evaluate the available pieces of evidence in order to take a final decision on the matter. The IT equipment of the courts is adequate for this purpose. The judges also receive training to help them to handle e-evidence correctly.

However, it has to be said that it is difficult to muster sufficient proof for a conviction in most cybercrime cases; as a result, only a small number of cases can come before the court and the judges. Judges therefore have fewer opportunities to acquire experience in cybercrime cases. Despite this, there are no major issues that would be beyond the knowledge and skills of judges in this field.

The Division against Counterfeiting Money and Bank Cards of the Riot Police's National Bureau of Investigation does not have special technical equipment. The expert opinions are drawn up where necessary by the High-Tech Crime Unit of the Corruption and Economic Crime Division of the Riot Police's National Bureau of Investigation. With the help of the Bank Security Units and certain international training courses, an up-to-date information flow on new technologies and methods used by modern criminal organisations is guaranteed.

6.5. Conclusions

- Regarding the investigation of child exploitation cases, it was noted that there is no dedicated database and/or specialised software to host, maintain and categorise material relating to child abuse. Moreover, the connection with the ICSE database was made very recently, and thus there is a need to ensure that more trained police officers are given access to the database. Furthermore, it was noted that there is a clear need for capacity improvement that will allow for a more effective proactive approach in the area of fighting child sexual abuse via the internet, such as the implementation of P2P monitoring software. It was also noted that, since they have recently been connected to the ICSE database, there is a need to improve and speed up the uploading to the database of material relating to child abuse in order to facilitate victim identification.

- Despite having such authority, the police do not seem to have managed to develop information sources with regard to cyber attacks. The only available source of information for the police seems to be the complainant's reports. As mentioned earlier, it seems that institutions and organisations are not obliged to report a cyber attack incident to the police; instead, they are only under an obligation to confirm the incident when requested. Overall, the general impression given is that there are few mechanisms in place to handle cyber-attacks.
- The national authorities use Child Protection Systems for the identification of suspects via P2P software. However, it was noted that they do not use specialised software for the identification and categorisation of material relating to child abuse, in spite of its great importance. The lack of such specialised software is due to the fact that, during the importing and categorisation of images and videos, a database is created which leads to the reduction of the investigators' time.
- Since 2012, Hungary has been struck by new cyber threats: cyber activism (ANONYMOUS) in 2012 and 2013 (53 sites were attacked).

- Operational services (police, CERT) reported a number of new trends as of 2015: several botnet cases, phishing cases involving banks and APT against German companies. Moreover, 3 000 sites (including 36 government sites) were attacked (defacements) by activists (Morocco, Tunisia) during the migrant crisis.

- In their threat assessment, the Hungarian police forces said that over the last three years they had seen a significant rise in the number of cases, and that their forces had been reinforced at the same time: for example, info system frauds rose from 249 cases (2013) to 2 175 (2015), and the number of breaches from 3 to 74.
- Many victims of such fraud are international companies from Asia and Germany. In these criminal transfers, Hungary is only a transit country where Hungarian mules are used by organised crime groups from Nigeria, Ukraine and Russia. Most money laundering takes place in Budapest.

- The Hungarian police have said that they do not get enough answers from international partners concerning cyber attacks.

- The cyber security centre is developing relations with universities (except on classified issues). This centre will also develop its Public Private Partnership in the framework of the implementation of the NIS Directive. The Hungarian national CERT also takes part in conferences on hacking which are organised in Hungary.

- The coexistence of the investigators and the forensic laboratory can be considered as a positive approach towards the effective investigation of cybercrime. However, it was noted that there is a need for further capacity-building improvement when it comes to both software and hardware equipment. This could be achieved via EU funding.

7. INTERNATIONAL COOPERATION

7.1. Cooperation with EU agencies

7.1.1. Formal requirements to cooperate with Europol/EC3, Eurojust, ENISA

Article 36 (5) of the CPA provides that ’When the conditions specified in the relevant act apply, the investigating authorities may, with the permission of the Prosecutor General, form or take part in a joint investigation team acting in one specific case or groups of specific cases with the participation of investigating authorities from the Member States of the European Union or of the European Police Office (EUROPOL).’

Article 167 of Act CLXXX of 2012 on criminal cooperation in criminal matters between the Member States of the European Union provides that ‘(1) In Hungary NEBEK is in charge of the tasks related to the relations and information exchange with Europol. The competent authority of Hungary can keep direct contact with Europol. The head of the competent authority appoints the person authorized to keep direct contact with Europol and informs NEBEK by providing this person’s name, post, place of employment and contact details.’

According to Article 177 of Act CLXXX of 2012, **‘**The information exchange between Eurojust and the Hungarian judicial authority shall take place through the Hungarian national member.’

Hungary implemented Council Decision 2002/187/IB on the establishment of Eurojust, and Council Decision 2009/426/IB on the reinforcement of Eurojust and on the amendment of Decision 2002/187/IB (Eurojust Decision).

The Hungarian national member of Eurojust is the prosecutor appointed by the Prosecutor General. Order No 2/2014 (I.31) of the Prosecutor General of Hungary regulates the prosecutor's activities in connection with Eurojust and the European Judicial Network. Section 22 of the Order mentions those cases in which prosecutors have reporting obligations towards Eurojust, including cybercrime-related cases.

Obligation to report to Eurojust

Article 22 of Order No 2/2014 of the Prosecutor General.

(1) By completing an online Eurojust template published in the internal information technology system of the Prosecution Service (Intranet/Structural Units/Department for International and European Affairs/Eurojust) and with respect to the information contained in the template, the prosecutor acting in a specific case shall immediately report on:

a) the setting up and activities of a joint investigation team,

b) cases where conflicts of jurisdiction have arisen or are likely to,

c) repeated difficulties or refusals regarding the execution of requests for or decisions on judicial cooperation,

d) cases directly affecting at least three Member States and where requests for or decisions on judicial cooperation have been forwarded to at least two Member States provided that

da) the offence involved shall be punishable with imprisonment of up to five years at least and shall be included in the list of criminal offences referred to in point (a) of Article 13(6) of the Eurojust Decision, specified below:

daa) trafficking in human beings

dab) sexual exploitation of children and child pornography

dac) drug trafficking

dad) trafficking in firearms, their parts and components and ammunition;

dae) corruption

daf) fraud affecting the financial interests of the European Communities

dag) counterfeiting of the euro

dah) money laundering

dai) attacks against information systems; or

db) a criminal organisation is involved in the commission of the offence; or

dc) the offence may have a serious cross-border dimension or repercussions at European Union level, or it might affect Member States other than those directly involved.

(2) The prosecutor shall fulfil their obligation by forwarding the completed Eurojust template to the following email address: eurojust.jelentés@mku.hu and neuf@mku.hu.

(3) The reporting obligation may not jeopardise or harm the safety of individuals or Hungary's national security interests. The reporting obligation shall not apply to classified data.

According to Article 107 of Act CLXXX of 2012, the consultation procedure which has been established to avoid parallel criminal proceedings provides an opportunity for the Chief Public Prosecutor to contact Eurojust to have the matter decided in the absence of agreement between Member States.

(Article 107(1) - If the parties have failed to reach an agreement on which of the Member States is to continue the criminal proceedings referred to in Article 106, the Chief Public Prosecutor may contact Eurojust to have the matter decided, provided that Eurojust has jurisdiction over the specific case. The Prosecutor General shall inform the Member State's authority that they have contacted Eurojust.)

If Eurojust becomes aware that there is a pending parallel criminal procedure for the same offence in another Member State at the same time as the criminal proceedings pending in Hungary, before the Chief Public Prosecutor contacts Eurojust to have the matter decided, the agreement on the transfer of proceedings in criminal matters can be also attempted with the assistance of Eurojust in order to avoid a conflict of jurisdiction. The above-mentioned procedure is less formal and less time-consuming; moreover, it is a useful and well-established practical solution.

Communications between the National Media and Infocommunications Authority (NMHH) and ENISA are regulated by 'NMHH Decree No 4/2012 (I.24) on the rules on data protection and confidentiality obligations associated with public electronic communications services, the special conditions of data protection and confidentiality, the safety and integrity of networks and services, the management of traffic and billing information, the display of identification data and call diversion' as follows:

‘Article 6(1) - Service providers shall be required to notify the Duty Service without delay in the case of any network security breach (for the purposes of this regulation: network security incident) that has had a significant impact on the operation of networks or services.

(2) The Duty Service shall, where appropriate, inform the national regulatory authority of the other Member States and the European Union Agency for Network and Information Security (hereinafter referred to as ENISA) via the Authority.

(3) The Authority may inform the public on its website or may decide that service providers shall be required to provide information to the public, where it deems that failure to disclose the network security incident may be in conflict with or jeopardise public interests.

(4) Information provided by the service providers referred to in paragraph (3) shall include:

a) time and date of the network security incident;

b) number of subscribers or other private individuals concerned;

c) all contact details where subscribers can request further information related to the network security incident;

d) possible consequences of the network security incident;

e) measures envisaged in order to mitigate the negative consequences of the network security incident;

f) the time, date and way in which the public has been informed if the public has been informed at the time of the notification to the Authority.

(5) Once a year, the Authority shall submit a summary report to the Commission and ENISA on the notifications received and the action taken by the Duty Service.

(6) According to the rules and procedure regulated by Article 47 of Act 100 of 2003 on Electronic Communications, the Authority may decide, in the event of non-compliance, that service providers shall be required to provide data, including their written security strategy, in order to determine the security and integrity level of their networks.

(7) The Authority may decide that service providers shall be required to undergo a network security audit carried out by an independent and security-classified organisation defined by the decision. Service providers shall bear the cost of the audit.

(8) During the procedure according to this Article, the Authority shall consider the network-security-related technical guidelines of ENISA.'

7.1.2. Assessment of the cooperation with Europol/EC3, Eurojust, ENISA

In relation to the settlement of conflicts of jurisdiction, the competent Hungarian prosecutor's office requested assistance from Eurojust to promote the execution of letters rogatory – aimed at obtaining cyber evidence – sent to the USA in child pornography and other crime-related proceedings. Simultaneously, the competent Hungarian authority issued a letter rogatory to the UK, on the basis of which Eurojust revealed that other procedures were under way in the United Kingdom in connection with the crimes forming the subject of the procedure. This required consultation between the representatives of the Hungarian and British law enforcement and judicial authorities. With the assistance of Eurojust the consultation took place on 5 October 2015, and the representatives of the Member States concerned decided to establish a joint investigation team. The Hungarian national member of Eurojust is also a member of the joint investigation team, thus it can count on financial support from Eurojust. The draft agreement on the establishment of the joint investigation team has been finalised, and now awaits signature.

The Europol EC3 'Europol Platform for Experts' provides a great opportunity for sharing experience and conducting informal consultations for those prosecutors and police officers who have already registered on the platform.

Currently, as part of the fight against sexual exploitation of children, there are 10 Hungarian members, amongst them police officers from the National Bureau of Investigation and the Budapest Police Headquarters as well as prosecutors, while in the section on copyright infringement there are 20 Hungarian members, including representatives of the National Bureau of Investigation, the National Tax and Customs Administration, the Special Service for National Security and several prosecutors.

In the framework of national and international cooperation, the specialised units of the National Bureau of Investigation closely cooperate with EUROPOL EC3. Hungary is a member of FP CYBORG (Focal point on cybercrimes), FP TWINS (Focal point on sexual exploitation of children) and FP TERMINAL (Focal point on non-cash means of payment abuses).

The High-Tech Crime Unit in the Corruption and Economic Crime Division of the Riot Police's National Bureau of Investigation took part inter alia in the following actions linked to EUROPOL EC3: 'OPERATION HAVEN', 'OPERATION DEPLETION', 'OPERATION DAYLIGHT', 'OPERATION OMNYMUS', 'OPERATION FALLING STARS', 'OPERATION ARCHIMEDES' and 'OPERATION SHYLOCK'.

The Money Forgery and Payment Card Fraud Unit in the Intelligence Division of the National Bureau of Investigation took part inter alia in the following actions linked to EUROPOL EC3: 'FIRST AIRLINE ACTION DAY' and 'OPERATION PANDORA-STORM'.

Through the focal points and joint actions the units contributed to some useful data collection, surveys and the creation of guides, and received information and several reports promoting the investigations.

In the case of the National Tax and Customs Administration, the application of the international mutual assistance in criminal matters took place via Eurojust in several specific cases. The experiences are positive; the requests arrived within 2-4 months, which is much faster compared to 'classic' legal assistance.

Aspects of cooperation with EUROPOL:

- Participation in the EUROPOL COPY IOS (Operation In Our Sites) action, the aim of which is the analysis and closure of websites marketing fake products. The experiences are positive.

- Participation in the EUROPOL EPE platform. Sharing and integrating useful experiences and applications into the activity of the National Tax and Customs Administration.

- Use of the mobile lab provided by EUROPOL, with very good experiences.

EUROPOL EC3 plays a prominent role in the field of international law enforcement information exchange. The strategic documents and guidelines produced by EC3 provide up-to-date information about the trends, problems and difficulties of cybercrime. Its cross-match reports on operational cooperation contain lots of useful information which can support the national investigations. The Europol training course on Combating the Online Sexual Exploitation of Children on the Internet (COSEC), organised on a yearly basis, is attended by one prosecutor and one law enforcement investigator from Hungary. This high-quality training course and the training materials help to develop best practices at national level in the field of combating child pornography. The use of the Europol Platform for Experts (EPE) provides an opportunity for further discussion or consultation and strengthening knowledge.

The Centre and its experts also carry out outstanding work in all fields of the EMPACT CYBERCRIME priority. As co-drivers, they help to coordinate the tasks related to the sub-priority areas and take a leading role in the implementation of more actions.

The National Cyber Defence Institute (NCDI) is actively involved in the activities of ENISA - for example, the National Liaison Officer (HU) of ENISA is delegated from the Hungarian NCDI. Furthermore, the NCDI plays a significant role in situational practice tests led by ENISA and also takes part in a number of working groups. ENISA is basically a body providing expertise and advice: in order to ensure information security, it reviews the significant issues, collects best practices, drafts recommendations, organises awareness-raising campaigns and training courses, etc.

Hungary welcomes these advisory, training and preventive activities of ENISA, which are significant and useful in the field of cyber security. The NCDI therefore aims to take part in the above-mentioned actions in as many areas as possible.

The Internet Unit of the Directorate General for Criminal Affairs of the National Tax and Customs Administration of Hungary (NTCA) is also a member of the Europol Platform for Experts (EPE). This unit also works in cooperation with EUROPOL's COPY working group and takes part in the actions of IOS (Operation In Our Sites) aimed at the elimination of websites related to online sale of counterfeit goods (including intellectual property (IP) trademark infringements) and online piracy (IP copyright infringements). Information to support criminal investigations and information material to ensure the expansion of the knowledge base are also regularly provided by EUROPOL.

In relation to cybercrime, Europol/EC3, Eurojust and ENISA could have a more important role in coordinating data acquisition in investigating cybercrimes. The aim could be to form an accelerated data acquisition procedure without legal obstacles in such cases.

Eurojust could be used for streamlining direct requests addressed to foreign providers and for collecting best practices.

In an informal consultation on 7 December 2015 on behalf of the European Parliament and the Council, the Luxembourgish Presidency concluded an informal agreement on the Directive on Network and Information Security. The provisions of the Directive define a number of tasks with regard to ENISA, which are welcomed by Hungary. In line with the rules incorporated into the Directive, ENISA plays a greater role in providing security and raising awareness, and gives guidance to the Member States in a number of areas of cooperation. It will also assume the role of Secretary of the CSIRT Network established by the Directive.

The Deputy Head of the High-Tech Crime Unit in the Corruption and Economic Crime Division of the Riot Police's National Bureau of Investigation represents Hungary in the meetings of the EUCTF (European Cybercrime Task Force), which operates with the support of EUROPOL, is composed of the heads of European specialised units and performs strategic planning, analysis and advisory tasks.

The IT Division (ITO) - a special unit of the National Tax and Customs Administration (NTCA) - participates in the 3rd action of the 7th action plan of the Customs Cooperation Working Party (CCWP), aimed at exchanging experiences and improving cooperation between the IT units of national customs authorities in the EU. The IT Division (ITO) exploits the information exchange facilities provided by the Europol Platform for Experts (EPE). In recent years, the IT Division (ITO) has regularly participated in the IOS (Operation In Our Site) operations organised by EUROPOL AWF 'SOC' Focal Point 'COPY'. These operations are aimed at investigating and closing down websites marketing counterfeit goods. The criminal specialty of the NTCA does not currently participate in other relevant international cooperation (e.g. cyber patrols).

7.1.3. Operational performance of JITs and cyber patrols

Hungary has no experience in JITS and cyber patrols.

7.2. Cooperation between the Hungarian authorities and Interpol

The High-Tech Crime Unit in the Corruption and Economic Crime Division of the Riot Police's National Bureau of Investigation has access to the INTERPOL ICSE (International Child Sexual Exploitation image database). Currently they only have one year's experience of using the system, but the use of the database is improving. The Unit plans inter alia to increase the number of colleagues who have access to the INTERPOL ICSE system and to organise national training courses focusing on national use of the system and the opportunities it offers.

Telenor Hungary Ltd., the National Police Headquarters (ORFK) and the National Media and Infocommunications Authority (NMHH) signed a Memorandum of Understanding on 1 December 2011 in order to establish the safe use of the internet for children and to prevent distribution of paedophile content on the internet. According to the Memorandum, Telenor Ltd. makes inaccessible from its network all websites which contain child pornographic content as compiled and constantly updated by the International Criminal Police Organisation (INTERPOL) on its 'Worst of' list. Telenor Hungary Ltd. receives this list (of websites containing prohibited content) from INTERPOL through its parent company. The NMHH contributes to the cooperation via its Internet Hotline which enables the reporting of illegal online content. The Internet Hotline helps to remove illegal content and regularly informs the ORFK about reported illegal content of a serious nature, particularly paedophile content. INTERPOL sends this list of prohibited content to its partner internet service providers operating in its member states. According to their agreement with INTERPOL, the service providers ensure that the websites containing this child pornographic content are made inaccessible in their networks.

Telenor Hungary Ltd., the NMHH and the police launched this initiative in 2012 in the expectation that, in time, the majority of significant internet service providers would join. However, this did not happen - no other service providers have joined the cooperation so far, INTERPOL's 'Worst of' list is not blocked by domestic internet service providers other than Telenor and no service provider has indicated that they intend to enter into an agreement with INTERPOL to block the list. According to the service providers which do not block the list, it is not legal to block the websites concerned without any clear statutory obligation or orders from courts or other authorities to do so. Those service providers therefore refuse to undertake such blocking on a voluntary basis until clear legal conditions are settled regarding this matter.

7.3. Cooperation with third states

Hungary aims to ensure close cooperation with third countries in the field of combating cybercrime. During the investigations all the available channels are usually used, e.g. personal contacts, the attaché network, EUROPOL and INTERPOL channels or requests for judicial assistance. Cooperation is based on the application of the existing legal framework; however, there is currently little cooperation with third countries.

The law enforcement information exchange is significantly easier with Australia, USA, Canada, Norway and Switzerland owing to the participation of EC3 and EUROPOL's liaison bureaux.

The transmission of NCMEC reports can be underlined as a best practice in the field of improvement of cooperation: the NCMEC (National Centre for Missing & Exploited Children) reports related to online sexual exploitation of children are provided to Hungary through the EUROPOL channel by the USA. These reports are forwarded quickly and easily in digital format, in a systematic manner month by month, with the assistance of Europol.

7.4. Cooperation with the private sector

If a given private company has a branch in Hungary, the authorities contact this branch in the vast majority of cases. During the data collection before answering this questionnaire, Hungary found examples of requests addressed to Sony, Microsoft and UPC.

According to the general rules, private companies may be subject to house searches; this generally does happen during the investigations.

As quick information exchange is of the utmost importance in online bank card fraud cases, great emphasis is placed on direct information exchange and establishing professional networks. To this end, national authorities have established and maintained direct links with the central units responsible for investigating bank card fraud cases in most EU countries, as well as with the FBI and the USSS. The contribution of liaison officers specialising in police cooperation in foreign countries (including Switzerland and Canada) is also a great support.

7.5. Tools of international cooperation

7.5.1. Mutual Legal Assistance

As there is no *lex specialis* regarding mutual legal assistance in connection with cybercrime, the general rules apply, namely:

- Act XXXVIII of 1996 on international legal assistance in criminal matters: Articles 1-10, 60/F-60/H, Chapter V.

- Act CLXXX of 2012 on criminal cooperation in criminal matters between the Member States of the European Union: Chapter IV.

- Act CXVI of 2005 on the Promulgation of the Convention of 29 May 2000 on Mutual Legal Assistance in Criminal Matters between the Member States of the European Union and its Additional Protocol of 16 October 2001.

As there is no *lex specialis* regarding mutual legal assistance in connection with cybercrime, the general rules apply for sending and receiving requests.

Pursuant to the Convention of 29 May 2000 on Mutual Legal Assistance in Criminal Matters between the Member States of the European Union, promulgated by Act CXVI of 2005 in Hungary, competent judicial authorities (courts and prosecution offices) of EU Member States which have ratified the Convention may directly submit and receive MLA requests.

MLA requests are also made directly between the judicial authorities of Hungary and those of Italy, Luxembourg, Greece, the Swiss Confederation, the Principality of Liechtenstein, the Republic of Iceland and Norway.

MLA requests are made to or received from third States via the central authorities (Minister of Justice, Prosecutor General).

With respect to MLA requests submitted or received after criminal proceedings are instituted, the Office of the Prosecutor General is designated as the central authority in accordance with Article 27(2)(a) of the Council of Europe Convention on Cybercrime signed in Budapest on 23 November 2001.

Pursuant to Article 38(1) of Act CLXXX of 2012 on criminal cooperation in criminal matters between the Member States of the European Union, a request (for legal assistance) shall be made in writing or, if necessary, by any other manner or means suitable for verifying the identity of the requesting party, including, in particular, telefax or IT systems. Requests presented in such ways shall be deemed compliant.

Article 39(1) of the same Act stipulates that if the request cannot, or cannot fully, be executed in accordance with the requirements set out in the request, the Hungarian judicial authority shall immediately inform the Member State's judicial authority and indicate the data that is needed to execute the request. If necessary, the Hungarian judicial authority shall notify the Member State's judicial authority directly using shortcuts to communicate the necessary data.

Statistics on the number of MLA requests sent/received are not available.

The majority of MLA requests within the EU are made with regard to information system fraud (online banking fraud) and related money laundering. Most such requests are sent by Germany, and the majority of the requests seek data and turnover of recipient Hungarian bank accounts which receive money (transferred or ordered to be transferred and diverted without the knowledge of the bank account holder and by the use of bank account data or bank card data obtained by various fraudulent means) obtained by fraudulent use of information systems, or they seek interviews with the bank account holders concerned (this varies depending on whether the request involves interviewing the person concerned as a suspect or as a witness with respect to the predicate crime/money laundering).

In most cases European conventions on mutual assistance in criminal matters are referred to as the legal bases for execution of the MLA requests. The Budapest Convention on Cybercrime is rarely referred to as a legal basis.

The same conditions apply for execution of these MLA requests as for MLA requests made with respect to other criminal offences.

Among third states or non-EU countries, it is primarily the United States that seeks legal assistance in criminal matters involving cybercrime. What such requests have in common is that they involve criminal investigations into serious, international and organised criminal acts (operating botnets, ensuring or providing online payment instruments for illegal trade activities) committed by criminal organisations created with the specific aim of committing cybercrimes, and they usually request the interception, seizure or data saving of internet traffic of a main server located in Hungary.

Judicial requests for legal assistance are typically preceded by requests for expedited preservation of stored computer data provided for by Article 29 of the Convention on Cybercrime and made via the 24/7 Network. Such MLA requests are received and dealt with by the ORFK BFI NEBEK (*National Police Headquarters – Criminal Directorate – International Criminal Cooperation Centre*) and by the High-Tech Crime Unit in the Corruption and Economic Crime Division of the Riot Police's National Bureau of Investigation. The exchange of information and the provision of assistance via the 24/7 Network is immediate and is carried out as soon as possible (within hours or days at the most).

Judicial MLA requests sent with urgency or considered to be priority with regard to the requested actions are handled without delay, and the time of execution of the request depends on the nature of the requested action or on whether any organised, international actions need to be taken - to seize a server, for example - and whether members of the requesting authority would like to be involved in those actions. It has been possible for requests received until now to be executed within weeks. It must be noted, however, that the dates of the procedural acts are often set by the requesting party.

A special procedure or condition generally contained in US requests is that the interception of a server, for example, should be carried out in accordance with Hungarian national law. Real-time interception of information systems and data collection can only be carried out in Hungary within the constraints of covert data gathering. As a result, actions sought by such requests – provided the Hungarian equivalents of the requested actions comply with the requirements of covert data gathering – are subject to a judicial order.

All measures provided for in the Budapest Convention can be requested in a mutual legal assistance request:

- expedited preservation of stored computer data
- expedited preservation and partial disclosure of traffic data (even without a formal legal assistance request, as a temporary measure through the 24/7 Network)
- search and seizure of stored computer data
- rendering inaccessible or removal of computer data
- real-time collection of traffic data
- interception of content data.

Pursuant to Hungarian Criminal Procedural Law, real-time collection of traffic data and interception of content data can only be carried out within the constraint of covert data gathering, and shall be subject to judicial permit. Real-time collection of traffic data and interception of content data is carried out by the Hungarian National Security Service depending on its capacities.

There have been cases in which the judicial authorities informally consulted each other before they resorted to requesting legal assistance, but this tool has primarily been used by the investigation authorities via the 24/7 Network. The prosecution service may also resort to informal consultation through Eurojust.

Before sending out an MLA request, investigation authorities try to consult the law enforcement bodies of the requested party so that their request as suitable as possible. Apart from personal relations and bilateral channels, the most commonly used channels are EUROPOL and INTERPOL.

Although Hungary does not have statistical data in this respect, we can state that Act XXXVIII of 1996 on International Mutual Assistance in Criminal Matters provides the legal basis for the widest measure of legal assistance in criminal matters with third States.

Article 5 of Act XXXVIII of 1996 – as a general rule - stipulates that '…requests for mutual assistance shall be executed or made where a) the act is punishable under both the law of Hungary and the law of the foreign state; b) the mutual assistance request does not involve a political offence or an offence connected with a political offence or military offence.'

In principal, mutual legal assistance may be provided on the basis of multilateral treaties, bilateral agreements or reciprocity. Where there are no reciprocity arrangements, a decision on the execution of requests for mutual assistance shall be made by the Minister of Justice or the Prosecutor General, in agreement with the Foreign Minister.

Mutual legal assistance is generally provided on the basis of the existing bilateral agreements between Hungary and the requesting/requested third State. This rule applies to requests made with regard to criminal matters involving cybercrime. Among non-EU countries, it is mainly the United States which seeks legal assistance in criminal matters involving cybercrime. Similarly, Hungary seeks such legal assistance primarily from the United States. In these cases legal assistance is requested pursuant to the 1994 Hungary-US Mutual Legal Assistance Agreement Treaty, as supplemented by the 2005 Protocol to the Treaty, and the Council of Europe Convention on Cybercrime.

The Hungarian authorities do their utmost to execute legal assistance requests as soon as possible. As already mentioned in section 2.C.3, most of the legal assistance requests sent to the US have not been executed even though the utmost importance of the case and the need for the evidence being sought were emphasised in the requests. Obtaining disclosure from an ISP (located in the US) on connection logs, subscriber information and similar information on websites can ordinarily be accomplished by submitting a formal request for assistance providing a precise description of the data to be disclosed, and providing a detailed explanation of how obtaining this data would be useful to the investigation.

Pursuant to the relevant US law on searching for a location or obtaining email data and any content from a communication stored with an ISP, a court order known as a 'search warrant' is required. The amount of proof required to obtain a search warrant is known as 'probable cause'. This means that, in relation to an MLA request for obtaining disclosure of stored communication content from an ISP, the US authorities will require supplementary information in order to decide whether they can satisfy the requirements of the relevant law. This procedure is very time-consuming, and in the majority of cases will not lead to the execution of the MLA request.

In one specific case national authorities submitted an MLA request to the US authorities for obtaining disclosure on subscriber information and connection logs in March 2014. As requested by the US authorities national authorities provided supplementary information in July, and in September 2014 they were informed that the request would be executed. They asked for status updates several times on the execution of the request, but no answer was received. In the end, in December 2015, the US authorities asked for additional information in order to be able to execute the Hungarian request.

The First Amendment to the US Constitution guarantees freedom of expression by prohibiting Congress from restricting the press or the rights of individuals to speak freely. Freedom of expression applies to the content of websites as well. The US authorities are therefore unable to execute court decisions to remove insulting content or render it inaccessible, as this would be contrary to US law.

In October 2015, the US authorities in their MLA request sought an image of a server managed by an ISP located in Budapest, Hungary, a one-day capture of traffic data for that server prior to being imaged, and all records relating to that server. Pursuant to Hungarian Criminal Procedural Law, real-time collection of traffic data can only be carried out within the limits of covert data gathering, and shall be subject to a judicial order. In order for the Office of the Prosecutor General to decide whether the requirements for obtaining a judicial order for the covert data collection had been fulfilled, national authorities asked the US authorities to provide additional information.

In those cases in which the perpetrator is identified as being foreign, mutual legal assistance will be used if this is expected to lead to further progress in the case and information cannot be obtained from Hungary. In principle, an international procedural assistance request will be sent during the investigation if all the evidence is detected in Hungary and it is impossible to go forward without the result of the legal assistance.

Hungary has never suffered any large-scale cyber attack, so fortunately there is no real experience of this. The legal background is well developed, and possibilities for cooperation in the framework of mutual assistance in procedural or enforcement matters are ensured at both EU and international level.

7.5.2. Mutual recognition instruments

The mutual recognition instruments for the recognition and execution of confiscation orders, the mutual recognition of financial penalties, and the execution of orders freezing property or evidence have been implemented by Act CXXX of 2003 on judicial cooperation in criminal matters with the Member States of the European Union. The mutual recognition instruments for the European protection order, supervision measures and, finally, the custodial sentences and measures involving deprivation of liberty have been implemented by Act CLXXX of 2012. The instruments listed above are applicable as of 1 January 2013, but Hungary cannot provide statistical data on the requests that have been made on the basis of those instruments.

With effect from 1 January 2015, legal assistance on the enforcement of the European protection order was introduced as a new legal instrument whose detailed rules are stipulated in Articles 163/A - 163/S of Act CLXXX of 2012 implementing Directive 2011/99/EU of the European Parliament and of the Council.

Article 22 of the Directive makes it incumbent on Member States to communicate relevant data related to the application of such legal assistance, which is carried out by the courts in Hungary through direct data collection.

According to the information gained from the courts, between 1 January 2015 and 18 November 2015 no request for legal assistance on the enforcement of the European protection order had been received by any district courts operating at the seats of the general courts, and similarly, no such request was sent by Hungarian courts abroad.

There is no data collection obligation for the courts stipulated by law regarding other mutual recognition instruments. The National Office for the Judiciary therefore examined anonymised final judgments in order to answer this question and found examples of mutual recognition as follows:

1.

The court recognised the foreign judgment imposing a one-year prison sentence – suspended for one year – for committing fraud with the use of information systems, as defined in Subsection (5) of Article 375 of the Criminal Code and punishable according to Subsection (1) thereof.

2.

The court recognised the foreign judgment, in the case of the first convicted person, imposing a 12-year prison sentence, to run concurrently and to be served behind bars, for committing cash-substitute payment instrument fraud as defined in Subsection (1) b) and Subsection (3) (a) of Article 313/C of Act IV of 1978 on the previous Criminal Code, on two counts of abetting such fraud – once as an attempt – in addition to other criminal offences. In the case of the second convicted person, the court recognised the foreign judgment imposing a prison sentence of eight years and six months, to run concurrently and to be served behind bars, on two counts – once as an attempt – of fraud committed with the use of information systems, as defined in Subsection (1) and (5) of Article 375 of the Criminal Code, in addition to other criminal offences.

3.

The court recognised the foreign judgment, in the case of the first convicted person, imposing a prison sentence of one year and six months, to run concurrently – and suspended for three years – for committing fraud with the use of information systems, as defined in Subsection (5) and (2) (b) of Article 375 of the Criminal Code, cumulatively, in complicity and in addition to other criminal offences. In case of the second convicted person, the court recognised the foreign judgment imposing a prison sentence of two years and eight months, to run concurrently, for committing fraud committed with the use of information systems, as defined in Subsection (5) and (2) b) of Article 375 of the Criminal Code, cumulatively, in complicity and in addition to other criminal offences.

7.5.3. Surrender/Extradition

In the case of an offence on the list of categories provided by the EAW Framework Decision, the authority of the executing State decides on the execution of the EAW without examining double criminality. Annex 1 of Act CLXXX of 2012 contains the offences which correspond to the list of categories. Should the offence not correspond to the list of categories laid down in the EAW Framework Decision, surrender may be granted, but the executing authority will also examine the matter of double criminality.

As there is no *lex specialis* regarding extradition for cybercrime offences, the general rules apply for all cybercrime cases.

7.6. Conclusions

- Eurojust's role in this particular area is very well known to the Hungarian judicial authorities and its assistance is generally requested in cases where conflicts of jurisdiction have arisen or are likely to arise.

- Hungarian prosecutors have formal reporting obligations towards Eurojust in cases where conflicts of jurisdiction have occurred (or may occur), including, obviously, cybercrime-related cases.

- Reports are made by filling in a form provided by Eurojust (the 'Article 13 form') and published in the internal IT system of the prosecution service.

- The police forces of the Republic of Hungary work in close cooperation with Europol/EC3 and participate in the policy cycle through membership of EMPACT Child Sexual Exploitation, EMPACT Cyber Attacks and EMPACT Card Fraud.

- The MLA procedure request is used in order to obtain electronic evidence from other Member States and third countries. The average timeframe for answering a request varies between one and three months. Although the MLA procedure appears to be the most effective means of obtaining electronic evidence for prosecution purposes, at times the slow pace of this procedure is a negative factor for the conduct of investigations.

- EUROPOL is the favoured and appreciated channel for the Hungarian investigation services, for operational matters (by the NBI) or by using the EPE (Hungarian customs). Hungarian partners are involved in the EMPACT actions and actively took part in EUROPOL operations. Operational units should have direct access to SIENA.

- Developing cooperation with foreign private sector players remains a major challenge in operational cooperation. The Hungarian investigation forces are attempting to develop contacts with international providers (mainly from the US). Relations are assessed as being good with some of them (Facebook, for example), but need to be developed further with others (Google). Hungarian partners rely on the EU and EUROPOL to support such partnerships.

- The majority of MLA requests are received from Germany (online banking fraud) or from the US (botnets, payments for illegal trade activities). On reciprocity, most of the MLA requests sent to the USA are not implemented because of a legal gap (probable cause) with US law. For this reason, Hungarian partners prefer to avoid MLA requests with the USA.

- The Hungarian authorities are attempting to develop cooperation with American providers without damaging their cooperation agreement with the US judiciary, but this is quite difficult.

8. TRAINING, AWARENESS-RAISING AND PREVENTION

8.1. Specific training

Both the National Office for the Judiciary and the Chief Prosecutor's Office consider the professional training of judges, prosecutors and judicial staff to be a priority. Some of the training offered by the Prosecutor's Office and the courts of justice has been described in section 3.A.2 above.

1) Ministry of the Interior, International Training Centre (http://www.nokitc.hu/nokeng/news.php):

• ILEA (International Law Enforcement Academy):

The services required for the operation of the ILEA are provided by the International Training Centre of the Ministry of the Interior (BM NOK). The Director-General of BM NOK and the Director of ILEA cooperate pursuant to an Agreement (Government Decree No 165/1996 (XI. 20) Korm.) between the governments of the Republic of Hungary and the United States of America concerning the establishment of the International Law Enforcement Academy, and the Agreement aimed at implementing that Agreement, and the amendments thereto which came into effect on 11 December 1998 and 13 September 2000 respectively.

ILEA stages one- and seven-week training courses on the above subject which are financed and also advertised by the US Department of State. The one-week courses discuss a single issue, while the seven-week courses are a complex event with a number of subjects on their agendas.

Presenters come from US federal law enforcement agencies.

The fight against cybercrime is the subject of two one-week courses conducted by special agents of the US Secret Service. These courses discuss ways of obtaining and analysing information from standalone computers and computer networks, at beginner and advanced levels. Such courses are held for law enforcement specialists twice a year and last one week.

In addition to the above, during the FBI's one-week programme on fighting child pornography, lecturers discuss the modalities of using computer software and online surfaces in investigations given that the crime in question typically involves using computers and the internet. That training is staged once a year, and takes one week.

The seven-week training course has two sections that focus on cybercrime. Week 3 on Immigration and Customs Enforcement touches upon the issue of child pornography, and in the initial parts of Week 4 a discussion of the Secret Service includes a short presentation on the basics of accessing and analysing information from computers and networks. That course is conducted four times a year.

- BM NOK CEPOL Hungarian National Office (CEPOL MNI):

BM NOK is the Hungarian partner institution of the European Police Academy (CEPOL) in addition to the National University of Public Service. The competent department of BM NOK, CEPOL MNI, helps Hungarian officials to participate in training events offered by the agency and to get involved in its exchange programmes and other activities, and it independently organises some of the training events.

The following training was provided to Hungarian professionals over the past three years (code of the courses in the working programme, name of the training course, number of participants, and the department they work for):

2013:

a) 13/2013 Investigating cybercrime and charging criminals – 22-26 April – one person from the Chief Prosecutor's Office, one person from the National Police Headquarters

b) 14/2013 Child exploitation on the internet – 1-4 October – one person from the National Police Headquarters

c) 15/2015 Cybercrime - cyber security – 14-17 October – one person from the National Security Service

2014:

a) 12/2014 Children's exploitation over computer networks – 8-11 April – one person from the National Police Headquarters

b) 14/2014 Member States' and EU capacities to detect, investigate and fight cybercrime – 7-10 October – one person from the Chief Prosecutor's Office, one person from the National Security Service

c) 13/2014 Cybercrime vs. Cyber security – 27-31 October – one person from the Counter-Terrorism Centre

d) 11/2014 Forensic, and digital evidence in cybercrime – 17-20 November – one person from the National Security Service, one person from the National Police Headquarters

2015:

a) 17/2015 Cybercrime-strategy – 25-27 March – one person from the Counter-Terrorism Centre, one person from the National Police Headquarters

b) 15/2015 Training trainers to help fight children's online exploitation – 22-26 June – one person from the National Council for the Prevention of Crime

c) 16/2015 Forensic crime scene investigation (cybercrime-scene investigation) – 8-12 June – one person from the National Security Service, one person from the National Police Headquarters

d) 14/2015 Children's online exploitation – 30 November - 3 December – one person from the National Police Headquarters

• A BM NOK CEPA Hungarian National Office

A BM NOK is an institution cooperating with CEPA. The competent department of BM NOK (KERA MNI) provides Hungarian officials with the opportunity of attending training events arranged by CEPA countries in this framework, and enables them to participate in the exchange programme and other activities. It also organises some of the training independently.

Training events offered to Hungarian experts over the past three years (title and subject of course, number of participants)

2013

a) Internet crime – certain crimes committed online – special seminar, 11 Hungarian participants, of whom four gave presentations

b) International cybercrime – special seminar, five Hungarian participants

c) Follow-up seminar for alumni of 2004, 2005 and 2009. 10 Hungarian participants

d) Investigating international online crimes with special attention to child pornography – case study, one session lasting 45 minutes

e) MEPA criminal investigation course – fight against and prevention of international crime, four Hungarian participants. Subjects:

Evidence extractable from digital data storage devices – tools used to fight online crime – with special attention to child pornography, three sessions lasting 45 minutes

Fight against and prevention of crime committed with standalone computers and networks – Cybercrime, four sessions lasting 45 minutes,

Online fraud – 'Online Casino', one session lasting 45 minutes

2014

a) International cybercrime – special seminar, three Hungarian participants

b) Cybercrime - Evidence extractable from mobile data storage devices, 4 Hungarian participants

c) Follow-up seminar for alumni of the criminal investigation course of 1993, 2006, 2007 and 2010, eight Hungarian participants, of whom three gave presentations. Cybercrime-related subject:

Darknet, one session lasting 45 minutes

2015

a) MEPA course on criminal investigation - fight against and prevention of international crime, four Hungarian participants. Subjects:

Child pornography on the internet – case study, one session lasting 45 minutes

Evidence extractable from digital data storage devices, tools used to fight online crime – with special attention to child pornography, three sessions lasting 45 minutes

Attacks on the electronic banking system, one session lasting 45 minutes

b) MEPA's course on criminal investigation - fight against and prevention of international crime, four Hungarian participants. Subjects:

Child pornography on the internet – case study

Evidence extractable from digital data storage devices – tools used to fight online crime with special attention to child pornography, three sessions lasting 45 minutes

c) OC-Course, Fighting organised crime, course given in English, four Hungarian participants. Subjects:

Child pornography on the internet – case study, one session lasting 45 minutes

Phishing, two sessions lasting 45 minutes

Attacks against online banking systems – Darknet, one session lasting 45 minutes

2) National University for Public Administration (http://en.uni-nke.hu)

The Law Enforcement Faculty of the National University for Public Service (NKE RTK) offers three BA courses (Criminal Administration, Law Enforcement Administration and Disaster Prevention) for law enforcement officers as well as MA courses in Law Enforcement Administration (law enforcement theory, crowd control, analytical evaluation and combating organised crime).

The general BA training for police officers includes the sharing of information related to the classification of cybercrimes under penal law, their criminalistic features, the procedural properties of computer crime cases listed in Table 2, the data that can be extracted from info-communication tools, and sharing the criminology of the crimes grouped under this heading.

This area is discussed under several subject headings, and taught to criminal and financial investigators in a total of 16-20 lessons. These subjects come up in the other educational branches of law enforcement and financial investigation, but those courses involve fewer lessons. Currently two 30-lesson elective courses are being added in the BA section *Professional skills courses* focusing on the same subject. In addition to the above, the issue of international cooperation related to the protection of vital IT technology systems elements will be introduced as an elective *professional knowledge* course in the MA section. The university offers no regular, recurrent courses to investigative authorities or judicial bodies; it only stages occasional further training courses for staff of police agencies in tandem with the national police headquarters (the ORFK). There is no available training to judicial authorities other than those listed under the educational branches provided by the law enforcement faculty (RTK: police, financial investigator). The purpose of the BA training is to enable students to recognise instances of online crime and to conduct the related investigations. The objective of the further training offered in cooperation with the national police headquarters is to ensure that the most recent knowledge is being taught to assist the relevant investigative work.

3) Agencies established to perform general police tasks (the ORFK and its subordinate agencies)

The High-Tech Crime Unit in the Corruption and Economic Crime Division of the Riot Police's National Bureau of Investigation (KR NNI) regularly delegates a lecturer to the training events of the full-time section (’day course’) and the part-time section (’correspondence course’) of the Law Enforcement Faculty of the National University of Public Service (NKE) to present topics including ’Introduction to cybercrime’, ’Online sexual exploitation of children’ ’Cyber attacks’, ’Darknet’ ’International criminal cooperation in the area of cybercrime’ and ’Forensic knowledge’ for the 'Criminalistics' and 'Criminal Investigation' courses. The Money Forgery and Payment Card Fraud Unit in the KR NNI’s Intelligence Division held presentations entitled ’Introduction to bank card crime’.

At national level there is currently no institutionalised educational module specifically for forensic experts and investigators of computer crime.

Training courses for forensic experts are organised by the Chamber of Forensic Experts. This situation will change once the Department of IT experts also starts operating within the Institute of Criminal Experts and Research (BSZKI). Training of IT experts currently takes place mostly through Hungarian private enterprises specialising in IT safety training and consulting. (*Kürt Zrt., NetAcademia Oktatóközpont Kft*.), European Digital Forensic Training courses staged by OLAF, and Dublin University's MA course (UCD) entitled Forensic Computing & Cybercrime Investigations.

The National Bureau of Investigation provides basic one-week training for computer crime investigators. Members of the investigative authorities acquire their knowledge beyond the basics either on a self-training basis or at ethical hacker courses or training events provided by international organisations (CEPOL, EUROPOL, OLAF, etc.). See section 10.B.1 for an overview of international training events available to computer crime investigators.

A) The National University of Public Service provides training opportunities in these areas pursuant to Decree No 2/2013 (I. 30) BM of the Minister of the Interior on the *Further training and management training system of commissioned members of law enforcement agencies under the direction of the Minister of the Interior, and on the staff replacement and management data bank of the law enforcement system,* as described in section 10.B.1, integrated into the BA and MA curricula, taking into account the options offered in the annual programmes of the international partner academies as well as demand by members of the profession.

B) Several members of the BRFK's Cybercrime unit have attended courses since 2010 offered by the ECTEG (Forensic Scripting Using BASH, Malware Analysis and Investigations, Vista and Windows 7 Forensics). In 2014, the High-Tech Crime Unit in the Corruption and Economic Crime Division of the KR NNI delegated one person, and in 2015 two people, to EUROPOL's *Training Course on Combating the Sexual Exploitation of Children on the Internet*. The KR NNI's Money Forgery and Payment Card Fraud Unit in the Intelligence Division delegated two people to the training course entitled *Elimination of websites selling illegal payment card information* arranged by EUROPOL. Apart from the above, the members of the special units of the KR NNI make every effort to attend all conferences, seminars, and working group meetings on the subject in an attempt to familiarise themselves with the most recent trends and best practice. International experience is also integrated into the presentations held at various training/further training courses by the members of those departments. Internationally provided opportunities for training and for expanding professional knowledge enable the investigators of the relevant Hungarian agencies to keep abreast of new trends and challenges and to acquire the most recent methods/techniques of investigation and evidence gathering. Such opportunities also encourage them to make good use of networking and to play their part in effective international cooperation.

Educational institutions and training organisations do not have an earmarked annual budget to offer this type of training - in other words, this function forms part of the institution's overall budget. Staging the training events required to ensure the professional competences necessary in modern law enforcement practice is an essential task of educational institutions. The general budget of the respective agencies therefore provides resources to meet professional training demand, which is supplemented by resources from international partners (e.g. CEPOL, ILEA). The complex financial environment for funding and arranging training does not allow to specify an approximate annual figure.

Regular training to refresh current knowledge is certainly required, on account of technological advances and other factors. The target group extends from the law enforcement staff of local agencies to specialists, depending on the area of competence, and there is also a distinction by subject (e.g. crimes related to cardless payment (CLP**),** sexual exploitation of children, etc.). Officers' knowledge must be refreshed at least once a year at each level, and specialists must also be given international training opportunities with at least the same frequency in various areas.

In consideration of the security priorities of the EU and Hungary (see previous sections), the Ministry of the Interior is planning to establish a training and research centre in the first half of 2016 that may develop into a centre of excellence in the short run. The Ministry, as the Competent Authority for the Internal Security Fund, wishes to allocate funding from the first half of 2016 onward, under an open round of applications. When deciding on the financial commitment for the creation of the centre of excellence, due consideration was given to the European Commission's document on the European law enforcement training system (European Law Enforcement Training Scheme, LETS COM(2013) 172 final) as well as the strategic documents mentioned earlier. The purpose of the centre of excellence is to carry out research, via broad-based national and international cooperation (involving law enforcement agencies, governmental and non-governmental actors, universities, financial institutions, etc.), into the direction taken by cybercrime and its most recent forms, so that the newest results/achievements, trends and phenomena can be integrated immediately, directly and effectively into the relevant curricula and thereby transmitted to the agencies and organisations involved in the fight against cybercrime.

8.2. Awareness-raising

The private sector plays a major role in preventive and awareness-raising campaigns. And, of course, state-funded and EU-funded grants also play an important part in this area.

One of the tasks of the National Cyber Security Centre is to raise awareness within the Central and Local Government Agencies. Accordingly, in 2014 GovCERT held attitude-forming campaigns for governmental offices in the counties and in the capital.

Furthermore, GovCERT always publishes the main identified software vulnerabilities in its webpage, and it sends newsletters and issues warnings to its partners.

Crime prevention programmes have been operated in schools for several years and a significant number of modules have been dedicated to awareness-raising on the dangers of cybercrime. However, in the near future, using ISS funding as well, Hungary will start special training courses to help combat cyber-bullying, violence in schools and misuse of public networks.

The National Crime Prevention Council would like to incorporate crime prevention modules into the basic materials of higher education courses as well; cybercrime-related issues could be also part of these courses.

8.3. Prevention

8.3.1. National legislation/policy and other measures

Hungary created its first crime prevention strategy in 2003 for the period 2003-2013. During its implementation the Hungarian Victim Support Office and the National Crisis Telephone Information Service were established, the Probation Service was reformed and mediation was introduced. It had several positive results in crime prevention.

The current national strategy of social prevention of crime drawn up by the National Crime Prevention Council came into force on 18 October 2013 by Government Resolution No 1744/2013 on the National Crime Prevention Strategy (2013-2023). The Strategy sets out the necessary legislative, organisational development and training tasks for ten years as well as public awareness programmes and the possibilities of promoting societal actions in the area of crime prevention. The priorities, measures and areas of intervention specified in the Strategy are designed to help achieve the above-mentioned objectives of criminal policy, reduce the vulnerability of children and youth, reduce victimisation and avoid repetition of offences. The strategy has a clear view of actions to be taken; it contains a detailed action programme. Its aim is to be clear and acceptable for experts working in the field of crime prevention as well as for partners and citizens. The strategy takes into account those policies that have common interfaces with crime prevention, namely: health policy, family policy, youth policy, child protection policy, sport policy, education policy, cultural policy, combating the use of drugs and alcohol, social policy, employment policy, local government policy, nature conservation policy, social inclusion and the integration of the Roma community, cybercrime and the fight against corruption and domestic violence.

The Strategy has a long-term plan, so it does not have a static view. It supports best practice, reflexivity and innovative measures in order to provide adequate responses to challenges arising in the sphere of public safety. For that reason a detailed, up-to-date action plan has been set up containing the measures proposed by state bodies and civil organisations.

The Strategy specifies the definition of crime prevention, its actors, the comprehensive goals and the intervention areas in detail. It addresses the background and the European and international environment and contains a detailed crime assessment. It sets out a vision, envisaging a practicable document which can achieve its results.

Priorities:

- Payment security
- Protection of minors and children
- Assistance to victims of crimes and prevention of victimisation
- Prevention of repeat offences
- The Strategy

The Strategy addresses cybercrime under the following points:

8.1.4. Asset protection

D. Establishment and operation of the Crime Prevention Centre

Action: the increase in the number of crimes, the growth of organised crimes and serious crimes against properties requires the application of safety tools and systems from companies and individuals. One of the platforms for transferring information and addressing the needs of the population is the test model called Crime Prevention Centre. It is a non-profit showroom, where visitors can get information on crime prevention, especially security advice on several topics.

8.2.5. Dangers of the media and internet

A. Safer use of the internet

Action: Information about safer use of the internet and media shall be shared with young people

B. Extension of the training themes of the Bűvösvölgy learning centre with crime prevention topics

Action: In 2013 the National Media and Infocommunications Authority established a learning centre called *Bűvösvölgy*. In the centre students can meet the world of the media and infocommunication. he National Crime Prevention Council participates in the development of the following crime prevention programmes:

1. DADA programme

The programme was developed for primary school pupils. The lessons consist not only of lectures but also of discussions about problems raised by the pupils, role-playing and other constructive pedagogical methods. The aim of the programme is for children to be aware of emergency situations and to differentiate positive and negative influences. Some of the topics are discussed with the help of short videos. There is a defined curriculum and the lessons are given by the National Police Headquarters.

Indicators: In the 2013/2014 school year, 33 128 pupils from 342 schools in 193 districts participated in the programme taught by 157 police officers. In the 2014/2015 school year, 30 723 pupils from 364 schools in 203 districts participated in the programme taught by 167 police officers.

2. 'ELLEN-SZER' programme

The 'ELLEN-SZER' programme is recommended for students in the 9th or 10th grade in different secondary schools (grammar schools and vocational schools). The curriculum includes methods as well as lesson plans with a description of the tasks. The main aim of the programme is to teach the children how to think independently and critically and how to behave in groups, to show them where individual responsibility lies, and to develop their decision-making skills and systematic thinking as well as their social skills, empathy and emotional intelligence. A further aim is to shape the core values of young people with regard to social utility. The basic principle of the programme is to enhance the security level of young people regarding the most serious deviancies, criminal activities and use of drugs. In addition to the above, the programme aims to raise awareness of the measures to be taken against criminal offences. In order to avoid becoming victims, the young people concerned must ask for help and use the techniques learnt during the courses. They should not support challenges that can cause damage to them or someone else. An important priority area of the programme is raising awareness of the possible dangers of the internet and safe internet use.

Indicators: As a result of the tasks carried out, 500 copies of the ELLEN-SZER learning materials were made and disseminated among the instructors. Instructors can obtain the handbook in electronic format on the internet as well. The handbook is 297 pages long and has been written by 22 authors from many different backgrounds. 7 098 students from 152 different classes participated in the ELLEN-SZER programme in 43 schools located in 26 . 27 police officers were instructors for the courses. In the 2013/14 school year, courses were given (in the framework of the school crime prevention network) by 99 police officers to 73 708 students from 2 924 classes in 172 different educational institutions in 74 .

The activities implemented under the framework of the school crime prevention network were based on the ELLEN-SZER programme (Action Plan No 29000/15358-8/2003). In the 2014-2015 school year, 116 crime prevention officers carried out their tasks. 232 secondary educational institutions from 97 settlements took part in the programme. Compared with the previous school year, this is a 35 % increase in terms of the number of educational institutions. The programme is implemented by officers of the National Police Headquarters.

3. Multifaceted crime prevention programme (pilot phase)

A school programme called 'Let's do something together for our safety!' (*Tegyünk együtt a biztonságunkért!*) was introduced in Budenz József Primary School for teachers with theoretical and practical training. The handbook for the project, entitled 'Multifaceted Crime Prevention', was written by the National Crime Prevention Council.

The multifaceted crime prevention programme was designed for children attending primary school. The curriculum is based on examples for methodologies and descriptions of tasks. In the lower classes there are between three and five sessions, while pupils in the higher classes have eight sessions. There are workbooks for the different topics and parents are constantly informed about the classes via email. As a result, parents are also involved in the programme, which helps to strengthen family relations and mutual trust between children and their parents.

The programme was tested in the 2015/2016 school year. One of its benefits is that school teachers can also teach these lessons (except for some parts of the curriculum). In this regard the police act as experts in the programme and can thereby add to their capacities (unlike some other programmes). This programme follows the same methods as the DADA and ELLEN-SZER programmes, but it also contains a special session for children in the lower classes. This session is based on the series of children's stories known as 'Woodland Story' (*Erdőváros meséi*), and it is monitored by a professional therapist.

Crime prevention through stories

a)'Woodland Story' (*Erdőváros meséi*) 1-2

The Secretariat of the National Crime Prevention Council publishes storybooks under the name *Erdőváros*, and is also issuing a handbook (entitled 'Crime prevention through stories') in connection with this. The dangers of the internet are presented in the first part, and will be also mentioned in the second part (which is not yet finished). There are also colouring books to accompany the stories. The storybook can be downloaded from: http://bunmegelozes.info/?q=hu/node/68

b) 'Losing our souls' (*Lélekvesztők*)

A workbook containing four stories was designed for 3rd and 4th grade children and is entitled 'Losing our souls' (*Lélekvesztők*). This workbook is based on stories about the dangers of smoking, alcohol consumption, drug abuse and the internet. The dangers of the internet are detailed in the story entitled 'What can be dangerous in something without hands and legs?' Audio material was also created for this story. Comics, playful exercises, crosswords and puzzles have also been designed to accompany the stories.

Children can study these stories and topics at home together with their parents. These two materials are available at the following address: bunmegelozes.info; and on the Facebook page of the National Crime Prevention Council.

5. Programmes for handicapped people (pilot programmes)

a) Tactile Security programme

The aim of the programme is to facilitate the life of blind and partially sighted persons, from the point of view of crime prevention, in public spaces, in their homes and in the world of the internet. A special training programme is being drawn up for this purpose. There will be two programmes for different target groups, one for adults and the other for children.

The special crime prevention programme for blind and partially sighted adults focuses on three areas of training. During the training courses, adopted for a special comprehension environment, this programme provides information and develop the skills of the participants and it aims to strengthen the perception that they are not potential victims and can do more for their personal security and they can shape their social image.

The participants:

- Reference groups formed by the National Institute of Blind People (VÁI) (15-15 persons)
- A co-worker responsible for employment and development, assigned by the VÁI
- Specialists of the National Crime Prevention Council (NBT)

The elements of the programme:

- shaping group attitudes
- awareness-raising materials related to the topics

The groups (15-15 persons) participating in the programme will be created on the basis of these elements.

Topics of the courses:

I. Street crimes – theft, robbery, confidence tricksters, using credit cards

II. Crimes at home – theft, confidence tricksters, peddlers

III. Internet safety – false information, online shopping

As regards the special needs of the participants, audio materials are made for all sessions. Creative methodologies (e.g. experiential education), interactive exercises and situational practices are important factors during the elaboration of the programme. Topics are being created as a pilot programme. The aim of the internet security module is help participants to avoid becoming victims in online space and to raise their awareness of the dangers of using the internet and how to recognise and avoid such dangers. Participants should learn the ethical and judicial basis and culture of internet use. The programme can help people to become conscious users, to evaluate the information and handle it appropriately.

Besides the topics for adults, there will be a methodological manual for children, which uses similar exercises and pedagogical methods. The aim of the project is the elaboration of a programme which educates blind and partially sighted children in safe practices and the introduction of this programme in the vocational training school system. Additional aims are the development of critical skills, cooperation in groups, to create individual responsibility and the elaboration of methodologies regarding the age and special skills of the children.

Topics of the courses:

I. Street crime – theft, robbery, confidence tricksters, using credit cards

II. Addiction – values, decisions, consequences

III. Internet safety – false information, shared information, online contacts

IV. Parties, entertainment – cultural entertainment, secure entertainment

b) 'I understood…' – creation of an informative software for crime prevention

The National Crime Prevention Council in collaboration with the National Alliance on Mental Illness (ÉFOÉSZ) is developing a crime prevention software which provides practical information and exercises for mentally disabled people, hearing-impaired people, the elderly, people who are not Hungarian native speakers, and children.

The software does not provide exact solutions for the emerging crimes and damaging consequences, but teaches self-defence processes and support skills in a large perspective. The application includes the topic of the risks of the internet.

6. 'Crime prevention at school' training programme for teachers and training programme for elementary and high schools

In 2014-2015, the Secretariat of the National Crime Prevention Council created a 30-lesson curriculum for teachers of a previous training programme 'Crime prevention at schools' that included short movies. It was supported by the Ministry of the Interior. The curator of the programme is the Service Centre Association of Crime Prevention and Education. The short movies can target school-age children effectively, can form the basis for discussions and can help to prevent violence at school, robberies and theft. Among the films are some which deal with the risks of using the internet. The films provide professional and methodological help for teachers and police officers to integrate crime prevention in the school curriculum and create lessons in crime prevention.

Indicators: the first training session took place in 2014 in Budapest. Of the 114 applicants, 86 were able to participate in the training.

In 2015 the training was also accessible in other locations outside the capital. The number of applicants and participants was as follows:

Location:	Applicants:	Participants:
Budapest	234	24
Debrecen	43	24
Hódmezővásárhely	58	25
Szeged	56	20
Veszprém	93	26
Total	484	119

The training is still ongoing. It is aimed at preparing teachers to give crime prevention lessons. Basic knowledge of the judicial system and criminology are provided during the theoretical part of the training (14 lessons) focusing on crimes related to minors and recognising and handling domestic violence. The teachers can learn about other fields of crime prevention through situation games and group exercises. The media education module introduces the methodology, mechanism and effectiveness of teaching with crime prevention short films which are accessible in the media library. The theoretical background of the practical part of the training consists of the description of the pedagogical method of cooperation and group work. During the practical part (16 lessons), the teachers can apply the cooperative methods learned and the techniques of being a group leader. After the training the participants have to prepare a curriculum or syllabus based on the crime prevention short films, which are evaluated using the classification 'acceptable' or 'non acceptable'.

8.3.2. Public Private Partnership (PPP)

Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies

Chapter III - 11. Ensuring government coordination

Article 21(1) As a body making proposals and comments to the government, the **National Cyber Security Coordination Council**, led by the minister responsible for electronic public administration (hereinafter 'the Council'), shall coordinate the activities of the organisations specified in paragraphs (1) to (6) of Article 2 and in Article 14(1) as defined in this Act and in the relevant implementing decrees.

(2) Led by the minister responsible for electronic public administration and supported by the cyber coordinator delegated by the minister, the Council shall:

a) coordinate the cooperation of various organisations subject to this Act in performing cyber security responsibilities;

b) promote cyber security regulation and support the work of sectoral cyber security teams/ working groups;

c) support the work of the National Cyber Security Forum (hereinafter 'the Forum'), which provides a framework for cooperation with non-governmental actors;

d) promote efficient fund management;

e) monitor the implementation of Hungary's National Cyber Security Strategy and prepare the relevant report for the National Security Cabinet;

f) promote the development of a coherent Hungarian Government position on cyber security and contribute to the international political representation of Hungary.

(3) The work of the National Cyber Security Coordination Council shall be supported by the ***National Cyber Security Forum***, comprising professional and non-governmental business managers invited by it, and by ***cyber security working groups***, which ensure sectoral governmental and non-governmental cooperation with the right to make proposals and comments.

Government Decree No 484/2013 (XII.17) on the rules governing the establishment and operation of the National Cyber Security Coordination Council, the Cyber Security Forum and the sectoral cyber security working groups, and their related competence and responsibilities.

National Media and Infocommunications Authority (NMHH):

Internet service providers operating in Hungary are required to block content deemed unlawful. Each internet service provider has to join the central database of rulings on disabling access to electronic information (hereinafter referred to as 'KEHTA') and has to put in place with immediate effect the prohibitions ordered by the court or other authority. The NMHH provides the connection to KEHTA through the 'Data Portal'.

The NMHH has been operating the central database of rulings on disabling access to electronic information (KEHTA) since 1 January 2014 in accordance with Subsection (3) of Article 159/B of Act C of 2003 on Electronic Communications, and processes the data entries to that end.

On the basis of point 33 of Subsection (3) of Article 182 of Act C of 2003 on Electronic Communications, the President of the NMHH has been given authorisation to lay down detailed regulations in the form of a decree for the providers of electronic communications services and providers of browsing and caching services in terms of connecting to the KEHTA and for electronic communication, and the rules of exemption from joining the KEHTA. NMHH Decree No 19/2013 (X. 29) entered into force on 1 January 2014 and is available on the webpage of the NMHH.

http://nmhh.hu/cikk/160577/Kozponti_elektronikus_hozzaferhetetlenne_teteli_hatarozatok_adatbazisa_KEHTA

Technical assistance to service providers (TSR):

The aim of the technical assistance system is to partly relieve service providers of the technical burden of preventing access, if they request or are in need of such assistance.

http://nmhh.hu/cikk/160587/Technikai_segitsegnyujto_rendszer_TSR

8.4. Conclusions

- The NBI Cybercrime Unit cooperates on a consistent and regular basis with the National University of Public Service Faculty of Law Enforcement in the setting up of educational activities in the following areas: Introducing Cybercrime, Cybercrime Criminalistics and Investigation Techniques, Cyber Attacks, Forensic Work, the Darknet, and International Cooperation in the Field of Cybercrime.
- Moreover, the Unit organises regular presentations to prosecutors and judges on matters related to cybercrime and launches or takes part in ad hoc conferences, workshops, round-table discussions, etc.

- At governmental level, the actions in respect of public awareness seem to be effective. The National Crime Prevention Council is a designated department within the governmental sector which is responsible for the policy related to cybercrime awareness and more specifically for the preparation of awareness material and its effective distribution.

- The Hungarian National Crime Prevention Council has, amongst its sectoral objectives, specific tasks and programmes concerning child and youth protection in general, and focusing on the dangers of the media and the internet in particular. In the context of the Council's activities, the evaluation team attended an impressive awareness-raising and prevention action targeted at visually impaired children and experienced a visit to the Magic Valley (*Bűvösvölgy*), a media literacy education centre at Budapest. This centre is run by the National Media and Telecommunications Authority of Hungary (NMHH) and is designed to provide students aged between 9 and 16 with first-hand experience of new technologies and media, making available various types of media content as well as the technical means to create TV shows, newspaper articles or magazine photo reports. The establishment of such a centre could serve as an example to other countries.

- Prevention of victimisation through education and awareness-raising is taken very seriously by the Hungarian authorities. However, it seems that activities in this area are mainly carried out by public entities, and there is no consistent, regular involvement of the private sector (telecommunications companies, banks and ISPs).

9. FINAL REMARKS AND RECOMMENDATIONS

9.1. Suggestions from Hungary

9.2. Recommendations

As regards the practical implementation and operation of the Framework Decision and the Directives, the expert team involved in the evaluation of Hungary was able to satisfactorily review the system in Hungary.

Hungary should conduct a follow-up to the recommendations given in this report 18 months after the evaluation and should report on progress to the Working Party on General Affairs, including Evaluations (GENVAL).

The evaluation team saw fit to make a number of suggestions for the attention of the Hungarian authorities. Related recommendations to the EU, its institutions and agencies, in particular Europol, are also put forward based on the various good practices.

As good practices to be reported, the team noted the real efforts of the authorities to unify statistics in a common tool for all investigation structures, to reinforce the capacities of the NBI and to increase the involvement of the judicial authorities (prosecutors' network, forensic units).

9.2.1. Recommendations to Hungary

1. Hungary should continue to develop the capacities of the National Bureau of Investigation, including by acquiring special investigation tools, for example: a) a data base for suspects, victims and child abuse material; b) special software tools for peer-monitoring; and c) performing cyber patrols. These new capacities should be useful for a more proactive approach in the area of fighting child sexual abuse on the internet.

2. In order to address the previous recommendation, Hungary should make more use of Internal Security Funds.

3. Hungary should develop more cooperation with the private sector (telecommunications companies, banks and ISPs) on a regular basis, mainly by organising prevention campaigns for small and medium companies about secure behaviour.

4. Hungary should consider developing the existing hotlines or creating an online platform in order to offer the possibility of reporting cybercrimes through user-friendly technical means of communication.

5. Hungary should encourage better cooperation between the national CERT and LEAs in order to develop a more coordinated approach and more reporting for combating cybercrime.

6. Hungary should develop prevention activities for the private sector, especially for small and medium companies, which lack cyber security structures even if they operate at international level.

7. Hungary is encouraged to create a sex offenders register for child sexual abuse in line with Directive 2011/93/EU.

9.2.2. Recommendations to the European Union, its institutions and other Member States

1. The EU should take further steps in order to foster better international cooperation between Member States' LEAs and foreign private companies. Support should be provided at both political level (EU) and operational level (Europol).

2. The EU should also continue to improve relations with the USA, especially with regard to MLA requests and their execution.

3. The EU should promote, by the most appropriate means, the establishment in the MS of legal conditions favoring data retention, especially providing for timescales which are really suited to operational needs.

4. Member States are encouraged to explore the possibility of applying for financial support from the EU for IT equipment, up-to-date forensic software and hardware.

5. Member States should consider using the EJN and the assistance of its contact points in order to make judicial cooperation in criminal matters more expeditious.

6. Member States are encouraged to explore the possibility of making more frequent use of Eurojust and the tools available through Eurojust, in particular the Liaison Prosecutor for the USA at Eurojust in order to obtain faster responses to MLA requests from the USA.

9.2.3. Recommendations to Eurojust/Europol/ENISA

1. Eurojust should raise awareness of the added value it may offer in providing judicial assistance in complex, cross-border cases.

2. Europol and other competent EU bodies should continue to support Member States, especially by providing forensic and operational training in the field of combating cybercrime.

Annex A: Programme for the on-site visit and persons interviewed/met

GENVAL - SEVENTH ROUND OF MUTUAL EVALUATIONS

'The practical implementation and operation of the European policies on prevention and combating cybercrime'

AGENDA OF THE ON SITE VISIT TO HUNGARY

Day 1 – 8 March 2016

Venue: Ministry of Interior (H-1051 Budapest, József A. u. 2-4.) with the participation of Mr. Ákos Kara, Ms Ágnes Kormányos and Ms. Emma Kunsági from the HU Ministry of Justice.

09:00 - 09:30	**Arrival and registration of the EU delegation and invited national experts into the building of the Ministry of Interior**
09:30 - 09:45	**Welcome note on behalf of the Ministry of Interior by Mr. Péter Stauber; the Head of the Department of European Cooperation**
09:45 - 10:00	**Introduction and some practical information in relation to the programs of the evaluation of Hungary by Ms. Zsófia Tóth**
10:00 - 10:30	**General presentation by the representative of the Hungarian Ministry of Interior on fighting against cybercrime in Hungary by Ms. Adrienn Szabó**
10:30 - 10:45	*Coffee break*
10:45 - 11:30	**Presentations on criminal and criminal procedure law including international cooperation aspects of fighting against cybercrime by representatives of the Hungarian Ministry of Justice: Mr. Ákos Kara and Ms. Emma Kunsági**

12:00– 13:15 *Lunch break (Lunch will be provided for the EU delegation by the Ministry of Interior at Rétesház Restaurant; Budapest, Október 6. u. 22., H-1051)*

Venue: Full afternoon is organized and hosted by the Riot Police National Bureau of Investigation (RP NBI) with the participation of Mr. Zsolt Csatlós and Mr. Balázs Krepsz from the National Tax and Customs Administration (NTCA).

13:15 – 15:45 **Law enforcement and investigation aspects of combatting cybercrimes – presentation by Mr. Richárd Szongoth and his colleagues on behalf of the Hungarian Police**

15:45 – 16:00 *Coffee break*

16:00 - 16:45 **Law enforcement and investigation aspects of combatting cybercrimes – presentation by Mr. Zsolt Csatlós and Mr. Balázs Krepsz from the NTCA**

16:45 – 17:00 **Questions and answers**

Day 2 – 9 March 2016

Venue: Full morning session will be organized and hosted by the Hungarian Judicial Academy (HJA) with the participation of Ms. Mária Rahói; representative of the Chief Prosecutor's Office.

09:00 - 12:00 **Presentations**

- Presentation by Ms. Mária Rahói; representative of the Chief Prosecutor's Office on relevant aspects of international assistance in criminal matters

- Presentation by Mr. Attila Kökényesi-Bartos; representative of the Chief Prosecutor's Office on the role of the Prosecutor's Office in combatting cybercrime

10:30-10:45 *Coffee break*

- Presentation by Ms. Natasa Fülöp; representative of the National Office for the Judiciary on the general role of judges in relation to cybercrime

- Presentation by Mr. Sándor Molnár; representative of Central District Court of Pest on the practice of judges in relation to cybercrime

12:00 – 13:30 *Lunch break (Lunch will be provided by the Judicial Academy for the participants of the morning session)*

Venue: National Cyber Security Centre (NCSC)

14:30 – 15:30 **Presentations by Ms. Anita Tikos and Mr. Illés Solt; experts of the National Cyber Security Centre**

Venue: IT Security Centre for Critical Infrastructures

16:00 - 17:00 **Presentation by Mr. Balázs Bognár; expert of the IT Security Centre for Critical Infrastructures**

18:30 – 20:30 *Official Dinner for the EU delegation offered by the HU MoI at Spoon Boat Restaurant; H-1052 Budapest, Vigadó tér 3-as kikötő http://www.spoonrestaurants.hu/*

Day 3 – 10 March 2016

Venue: Full morning session will be organized and hosted by the National Crime Prevention Council (NCPC)

09:30 - 11:30 **Discussion and interactive presentation on prevention with the expert of the NCPC; Ms. Katalin Baracsi**

Visit to a special institution for visually impaired children guided by Ms. Tünde Bácskai

11:30 – 13:00 Lunch (Lunch will be offered for the EU delegation by the HU MoI at Bagolyvár Restaurant; Budapest, Gundel Károly út 4, H-1146)

http://www.bagolyvar.com/

Venue: Full afternoon session will be organized and hosted by the National Media and Infocommunications Authority (NMIA)

14:00 – 16:00 **- Presentation by Mr. Gábor Németh; representative of the National Media and Infocommunications Authority on roles of the Authority in contributing to combatting cybercrime**

- Presentation by Ms. Dorottya Gerencsér on operation of the Internet Hotline

Visit to National Media and Infocommunications Authority, Magic Valley (Bűvösvölgy in Hungarian) - Hungary's first Media Literacy and Education Centre guided by Mr. Miklós Császár and Mr. András Csillény.

Day 4 – 11 March 2016

Venue: Ministry of Interior (H-1051 Budapest, József A. u. 2-4.) with the participation of

Mr. Ákos Kara - HU MoJ
Mr. Balázs Bognár - IT Security Centre for Critical Infrastructures
Mr. Gábor Németh - HU NMIA
Mr. Zsolt Csatlós - NTCA
Ms Ágnes Kormányos MoJ
Ms. Anita Tikos - NCSC
Ms. Emma Kunsági - HU MoJ
Ms. Mária Rahói- CPO
Ms. Natasa Fülöp - National Office for the Judiciary

09:00 – 11:30 **Closing remarks, further questions and answers**

ANNEX B: PERSONS INTERVIEWED/MET

Venue: Ministry of Interior and National Bureau of Investigations

Person interviewed/met	**Organisation represented**
Ms. Adrienn Kisné Szabó	Head of unit Ministry of Interior – Hungary Department of European Cooperation
Ms. Zsófia Tóth	Legal officer Ministry of Interior - Hungary Department of European Cooperation
Ms Zsuzsanna Pethő	Ministry of Interior
Ms Ágnes Bokodi	Ministry of Interior
Mr. Ákos Kara	Ministry of Justice
Ms Ágnes Kormányos	Ministry of Justice
Ms. Emma Kunsági	Ministry of Justice
Mr Attila Kökényesi-Bartos	Representative of the Chief Prosecutor's Office
Mr Richárd Szongoth	Representative of the National Bureau of Investigation
Mr. Zsolt Csatlós	National Tax and Customs Authority
Mr. Balázs Krepsz	National Tax and Customs Authority

Venue: Hungarian Judicial Academy, National Cyber Security Centre and IT Security Centre for Critical Infrastructures

Person interviewed/met	**Organisation represented**
Ms. Mária Rahói	Chief Prosecutors´ Office
Mr. Attila Kökényesi-Bartos	Chief Prosecutors´ Office
Ms. Natasa Fülöp	National Office for the Judiciary on the general role of judges in relation to cybercrime
Mr. Sándor Molnár	Central District Court of Pest on the practice of judges in relation to cybercrime
Ms. Anita Tikos and Mr. Illés Solt	National Cyber Security Centre

Mr. Balázs Bognár	IT Security Centre for Critical Infrastructures

Venue: National Crime Prevention Council (NCPC) and National Media and Infocommunications Authority

Person interviewed/met	**Organisation represented**
Ms. Katalin Baracsi	National Crime Prevention Centre
Mr. Gábor Németh	National Media and Infocommunications Authority
Ms. Dorottya Gerencsér	National Media and Infocommunications Authority
Mr. Miklós Császár	National Media and Infocommunications Authority
Mr. András Csillény	National Media and Infocommunications Authority

Venue: Ministry of Interior

Person interviewed/met	**Organisation represented**
Mr. Ákos Kara	Ministry of Justice
Mr. Balázs Bognár	IT Security Centre for Critical Infrastructures
Mr. Gábor Németh	National Media and Infocommunications Authority
Mr. Zsolt Csatlós	National Tax and Customs Authority
Ms. Anita Tikos	National Cyber Security Centre

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	HUNGARY OR ACRONYM IN ORIGINAL LANGUAGE	HUNGARY OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
BM NOK			International Training Centre of the Ministry of Interior
BRFK			Department of Children and Youth Protection of Budapest Police Headquarters
CDMA			Cyber Defence Management Authority
EGC			European Government CERTs Group
ENYÜBS			Unified System of Criminal Statistics of Investigating Authorities and of Public Prosecution
ENISA			European Network and Information Security Agency
EPE			European Platform for Experts
EUCTF			European Cybercrime Task Force
FIRST			Forum of Incident Response and Security Teams
ICSE			International Child Sexual Exploitation image database
IES			Institute of Expert Services

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	HUNGARY OR ACRONYM IN ORIGINAL LANGUAGE	HUNGARY OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
ILEA			International Law Enforcement Academy
IMEI			International Mobile Equipment Identity
INHOPE			International Association of Internet Hotlines
I-OSINT			Internet Based Open Source Investigation
ISP			Internet Service Providers
IT Division			Information Technology Division
IWWN			International Watch and Warning Network
KEHTA			Central Database of rulings on disabling access to electronic information
MLA			Mutual Legal Assistance
NAIH			National Authority for Data Protection and Freedom of Information
NCDI			National Cyber Defence Institute
NCMC			National Centre for Missing and Exploited Children
NCTC			National Counter Terrorism Centre
NDGDM			National Directorate General for Disaster Management

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	HUNGARY OR ACRONYM IN ORIGINAL LANGUAGE	HUNGARY OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
NEBEK			National Police Headquarters National Criminal Cooperation Centre
NKE RTK			Law Enforcement Faculty of the National University for Public Service
NMIA			National Media and Infocommunications Authority
NSA			National Security Agency
NTCA			National Tax and Customs Authority
ORFK			National Police Headquarters
SSNS			Special Service for National Security
TI			Trusted Introducer
UNWTO			UN World Tourism Organisation

ANNEX D: RELEVANT NATIONAL LEGISLATION

Search

Article 149 of CPA

(1) Search means the search of a house, flat, other premises, an enclosure attached thereto, or the vehicle, as well as the examination of an information system placed there or a data medium containing data stored in such a system; the search is conducted in order to enhance the efficiency of the proceedings.

(2) A house search may be ordered when there is reasonable cause to believe that it will result in

a) apprehending a person having committed a criminal offence,

b) uncovering the traces of a criminal offence,

c) finding means of evidence, or object subject to confiscation or forfeiture of assets.

(3) A house search shall be ordered by the court, the prosecutor or – unless the prosecutor provides for otherwise – the investigating authority; the court and the prosecutor may request the assistance of the investigating authority for conducting the house search. In the cases specified in Paragraph (2) b) and c), inasmuch as possible, the search warrant shall indicate the means of evidence and the object subject to confiscation or forfeiture of assets desired to be found during the house search.

(4) As a rule, the search shall be conducted in the presence of the person concerned, who shall be informed about the decision ordering the search prior to the commencement of the search; further – if the purpose of the search is to find a designated or known means of evidence, an object to be confiscated or a person – the person concerned shall be demanded to surrender the object, to make available the data stored in the information system or data medium, or to surrender the designated person. If the person concerned obeys and surrenders the object, makes the data stored in the information system or data medium available, or surrenders the designated person, the search shall not be continued, unless there is reason to suspect that other means of evidence or other object to be confiscated or assets to be forfeiture could also be found in the course of the search.

(5) If the person concerned or his defence counsel, representative or appointed relative is not present during the house search, a person – who is reasonably believed to be able to properly protect the interests of the person concerned by the house search – shall be appointed to protect the interests of the person concerned by the search.

(6) The house search of the office of a notary public, a law office or a health institution– when conducted in order to find some professional secret related to the notary public's or lawyer's activity or to find a document holding health data – prior to the filing of the indictment shall be ordered by the court. The search may only be conducted in the presence of the prosecutor.

(7) The prosecutor may direct a house search pursuant to paragraph (6) without a court warrant if the delayed performance of the house search jeopardizes the realization of the objectives set forth in paragraph (2).

(8) In the case regulated in paragraph (7) the court warrant shall be obtained subsequently. Should the court reject the motion, the results of the house search may not be admitted as evidence.

Seizure

Article 151 of the CPA

(1) Seizure means taking into custody or preservation in any other way of the object by the court, the prosecutor or the investigating authority to substantiate or attest the confiscation or the forfeiture of assets.

(2) The court, the prosecutor or the investigating authority shall order – excluding real estate property – the seizure of the object, information system, data medium containing data stored by such a system, or data if

a) it means of evidence;

b) it may be confiscated or the forfeiture of assets may be ordered to it in accordance with law.

(2a) The seizure shall also be ordered when it cannot be executed during the time-period of the special protection determined by the Act on the special protection of the borrowed cultural goods.

(3) Seizure of documents kept in the office of a notary public, a law firm or a health institution and containing any professional secret related to the notary public's or lawyer's activity or health data shall be ordered by the court.

(4) Seizure of mail and news communication not delivered to the addressee as yet, as well as of documents of the editorial office of printed matters may be ordered prior to filing the indictment by the prosecutor, or thereafter by the court. Until the decision is made, the consignment may only be subject to retention.

(5) If seizure is ordered by the court or the prosecutor, they may request the assistance of the investigating authority for the execution of the order.

(6) If the prosecutor or the investigating authority is not entitled to order the seizure but immediate action is required, the object may be taken into custody. In this case the order for seizure shall be obtained subsequently, as early as possible from the authority entitled to issue it. The object shall be released from custody and returned to the holder if seizure is not ordered by the authority entitled to issue such an order.

Article 152 of the CPA

(1) In order to effectuate the seizure, the holder of the object, information system or data medium containing data stored in such system or the data manager shall be demanded to surrender the object or, make the data stored in an information system available. Failure to obey the above demand voluntarily may be subject to disciplinary fine provided however, that no disciplinary fine may be imposed on the defendant, a person entitled to refuse to testimony as a witness and persons who may not be heard as a witness. The refusal to surrender or render the object accessible shall not prevent obtaining the object or data stored in an information system by way of a search or body search. The person concerned shall be warned of the above.

(2) Letters and other written communication between the defendant and the defence counsel, and the notes of the counsel for the defendant pertaining to the case may not be seized.

(3) Letters and other written communication between the defendant and a person who may refuse to testify as a witness under Article 82 (1) may not be seized when they are kept by the latter person.

(4) Documents the contents of which may be subject to the refusal of a testimony may not be seized, either, when they are kept by the person who may refuse to testify as a witness. This restriction shall also apply to the papers and properties kept at the official premises of a person who may refuse to testify as a witness pursuant to Article 82 (1) c).

(5) The restrictions set forth in paragraphs (3) and (4) shall not apply if

a) the person entitled to refuse to testify as a witness is suspected on reasonable grounds to be an offender, an accomplice, or with harboring a criminal, or with receiving of stolen goods or with money laundering,

b) the object to be seized is the instrument of the criminal offence,

c) the person entitled to refuse to testify as a witness voluntarily surrenders the object to be seized, after being advised of the provisions of paragraphs (3) and (4),

d) the court according to Article 82 (6) obliged the person entitled to refuse to testify as a witness based on Article 82 (1) d) to expose the identity of the person providing information to him/her.

Article 153 of the CPA

(1) It shall be ensured that the contents of documents are not disclosed to unauthorized persons.

(2) If the prosecutor is not present at the detection of a document in respect of which its holder believes to have the right to refuse to testify as a witness pursuant to Article 82 (1) b) and the owner of the document or the defence counsel, representative or appointed representative thereof denies his consent to examine the contents of the document, the data medium containing the document or the document itself shall be handed over in a sealed envelope to the investigating authority, which will then forward the document in the sealed envelope to the prosecutor without examination. If the above solution is not feasible, the investigating authority shall arrange for the safekeeping of the document by applying Article 154 (3) as appropriate. After the examination of the document, the prosecutor shall make a decision on the seizure thereof, or – in the case of documents falling under the scope of Article 151 (3) – on submitting the motion for the seizure thereof to the court. Should the prosecutor or the court not order the seizure, the document may not be admitted as a means of evidence either in that case or in other criminal proceedings.

(3) At the request of the owner of the document, a certified copy shall be issued on the document seized, unless this jeopardizes the interests of the procedure.

Article 154 of the CPA

(1) Any object seized shall be deposited; if it is unsuitable for depositing or other important reasons justify it, its safe-keeping shall be arranged in another manner. In the latter case, a document or photograph reflecting the unique features of the object seized, as related to the criminal offence, shall be attached to the file of the case. The object which is left in safe-keeping of person concerned or is given to safe-keeping of another authority shall not be given to the possession or handling of other person without approval of the court, prosecutor or investigating authority ordering the seizure. The court, the prosecutor or the investigating authority oblige the new holder or handling to the safe-keeping of the seized object.

(2) The seized objects shall be listed in a minutes or other document indicating their quantity, value, condition and other features making them suitable for individual identification.

(3) The seized object shall be kept in a way that ensures that the object is reserved unchanged and easily identifiable, and that prevents the disappearance of any traces of the criminal offence or the exchange of the seized object.

Article 155 of the CPA

(1) The court, the prosecutor or the investigating authority terminates the seizure, if it does not serve the interests of the procedure any longer; while seizure shall be terminated if the investigation has been terminated, or if its maximum period has expired. In lieu of the termination of seizure, actions stipulated in another legal regulation shall apply, if the possession of the object seized violates the law. Prior to filing the indictment, seizure ordered by the court may also be terminated by the prosecutor.

(2) Upon terminating seizure, the object shall be returned to the person who can authentically verify having been the owner of the object seized at the time of the commission of the criminal offence.

(3) If no person exists to whom the object shall be returned under paragraph (2) and the files of the procedure contain no data thereon, either, the object shall be returned to the person whose announced claim for the object seems justified.

(4) In the absence of a person to whom the object shall be returned under paragraph (3), or the files of the procedure contain no data on such claim, the object shall be returned to the person from whom it was seized.

(5) Any object seized may only be returned to the defendant, if no other person exists to whom it may be returned under paragraphs (2)-(4).

(6) Based on a court decision, the object seized from the defendant shall become state object, if the identity of the person to whom it is due beyond doubt cannot be established. Late claimants may claim the return of the object or the amount realized on the sale thereof. The application of the claim shall be decided upon by the court having the competence and jurisdiction under the Code of Civil Proceedings.

(7) Upon the termination of seizure, if the object cannot be returned in kind, the amount realized on its preliminary sale, reduced by handling and storage expenses shall be refunded. In relation to non-community goods, the amount realized on the sale shall be paid following the settlement specified in the customs regulations. Any excess claims may be enforced by the beneficiary according to the rules of civil law. In the event of unfounded seizure, the amount realized on its preliminary sale may not be reduced by handling and storage expenses. The above shall be stated in the decision of the court, prosecutor or investigating authority making the decision on the termination of seizure.

(8) If the object seized has no value and is not claimed by anyone, it shall be destroyed after the termination of the seizure.

(9) If the sequestration was not performed in order to ensure confiscation or forfeiture of assets, and the expert has already examined the sequestrated materials, another expert has not been ordered upon the request of the authorized therefore, and the court, the prosecutor or the investigating authority do not consider reasonable another expert examination, the sequestration shall be terminated.

Furthermore, other special rules determine instructions for data preservation and on their rendering temporarily inaccessible that can be crucial in terms of successful conduct of criminal proceedings.

Order to preserve data stored in an information system

Article 158/A of the CPA

(1) Compulsion to preserve data means the temporary restriction of the right of disposal of a person possessing, processing or managing data recorded by an information system over specific data stored in an information system, in order to investigate and prove a criminal offence.

(2) The court, the prosecutor or the investigating authority shall order the preservation of data stored in an information system constituting a means of evidence or required to trace any means of evidence or the establishment of the identity or location of a suspect.

(3) From the time of being notified of the order, the obliged party shall preserve the data stored in the information system designated in the order, and ensure its safe storage, if necessary, separately from other data files. The obliged party shall prevent the modification, deletion, destruction of the data stored in an information system, as well as the transmission and unauthorized copying thereof and unauthorized access thereto.

(4) The party ordering the preservation of data may affix its advanced electronic signature on the data to be preserved. If the preservation of the data at its original location considerably hindered the activity of the obliged party to process, manage, store or transmit data, the obliged party may, with the permission of the issuer of the order, ensure preservation by copying the data into another data medium or information system. After the copy has been made, the issuer of the order may wholly or partially relieve the restrictions concerning the data medium and information system holding the original data.

(5) While the measure is in effect, the data to be preserved may solely be accessed by the court, prosecutor or investigating authority having issued the order, and – with their respective permission – the person possessing or managing the data. The person possessing or managing the data to be preserved may only be provided information of such data with the express permission of the issuer of the order during the effect of the measure.

(6) The obliged party shall forthwith notify the issuer of the order if the data to be preserved has been modified, deleted, copied, transmitted or viewed without authorization, or an indication of an attempt of the above has been observed.

(7) After issuing the order for preservation, the issuer shall start to review the affected data without delay, and depending on its findings, and either order the seizure of the data by copying them to the information system or other data medium, or terminate the order for their preservation.

(8) The obligation to preserve data shall be in effect until the seizure of the data medium containing the original data or in the case of paragraph (4) until the copy of the data, but no longer than for 3 months. The obligation to preserve the data shall terminate if the criminal proceedings has been concluded. The obliged party shall be advised of the conclusion of the criminal proceedings.

Rendering electronic data temporarily inaccessible

Article 158/B of the CPA

(1) Rendering electronic data temporarily inaccessible means a temporary restriction of a person's right of use of data posted via electronic communication systems (hereinafter: electronic data) and temporarily disabling access to data.

(2) Proceedings instigated due to criminal acts that warrant prosecution and require that electronic data be rendered permanently inaccessible also in order to prevent the criminal act from continuing, an order may be issued to render electronic data temporarily inaccessible.

(3) Courts are authorized to issue an order to render electronic data temporarily inaccessible.

(4) Orders to render electronic data temporarily inaccessible may require

a) the temporary removal of electronic data,

b) the temporary prevention of access to electronic data.

(5) Entities subject to a court order issued to render electronic data temporarily inaccessible shall notify users of the legal grounds of removing, or preventing access to, the affected content and shall cite the name of the court and the number of the court order in such notices.

(6) Orders to render electronic data temporarily inaccessible as envisaged in paragraph (4) a) and to preserve data stored in an information system may be issued simultaneously.

Article 158/C of the CPA

(1) Orders to remove electronic data temporarily shall oblige the web hosting providers defined in the Act on Electronic Trading Services and Certain Issues Concerning Services Related to Information Society. Obliged parties shall have one working day to give effect to the temporary removal of electronic data after the communication of the court order.

(2) The court lifts the obligation to render electronic data temporarily inaccessible as envisaged in Article 158/B (4) and issues an order to restore electronic data if

a) the reason for the order to render electronic data temporarily inaccessible ceases to exist, or

b) investigations have been terminated, except in case the option to issue an order to render electronic data permanently inaccessible exists under Article 77(2) of the Criminal Code.

(3) The obligation to render electronic data temporarily inaccessible as envisaged in Article 158/B (4) a) is lifted upon the termination of criminal proceedings. If a court refrains from issuing an order to render electronic data temporarily inaccessible, it shall require the web hosting provider to restore electronic data.

(4) The ruling on the termination of rendering electronic data temporarily inaccessible and on restoring such data shall be communicated to the obliged party immediately. Web hosting providers shall have one working day to restore electronic data after the communication of the court ruling.

(5) It is the duty of the bailiff to give effect to orders issued to remove temporarily or to restore electronic data.

(6) The courts, acting ex officio or upon a motion to that effect by the prosecutor, may impose a disciplinary fine between one hundred thousand and one million Hungarian Forints whenever an obliged party fails to abide by its obligation to remove temporarily or to restore electronic data. Disciplinary fines may be imposed repeatedly.

Article 158/D of the CPA

(1) The courts shall issue an order to render electronic data temporarily inaccessible as envisaged in Article 158/B (4) b) if

a) a web hosting provider fails to comply with its obligation to remove electronic data temporarily, or in case a letter rogatory by a foreign government agency seeking the temporary removal of electronic data fails to achieve its intended purpose within a period of thirty days after being sent, and

b) criminal proceedings have been instituted to combat drug trafficking (Article 176-177 of the Criminal Code), inciting substance abuse (Article 181 of the Criminal Code), aiding the manufacture or production of narcotic drugs (Article 182 of the Criminal Code), criminal offences with drug precursors (Article 183 of the Criminal Code), illegal possession of new psychoactive substances (Articles 184-184/D of the Criminal Code), child pornography (Article 204 of the Criminal Code), criminal acts against the state (Chapter XXIV of the Criminal Code) or terrorist act (Articles 314-316 of the Criminal Code) or financing of terrorism (Article 318 of the Criminal Code) and the electronic data are connected to these forms of criminal offences.

(2) By issuing an order, the courts oblige electronic communications providers to temporarily disable access to electronic data.

(3) If the person with the right to use the electronic data is unknown, court rulings to render electronic data temporarily inaccessible as envisaged in Article 158/B (4) b) shall be served to recipients by posting an announcement. Such announcements shall be posted on the bulletin board of the court for a period of fifteen days and on the central website of courts, provided that the rules of delivery of such announcements shall otherwise be subject to Article 70 (5) and (6). The party holding the right to use electronic data has eight days to appeal the ruling after it is served.

(4) The courts shall immediately send electronic notification to the National Media and Info-communications Authority (NMIA) about its orders to render electronic data temporarily inaccessible as envisaged in Article 158/B (4) b).

(5) The NMIA organizes and supervises the execution of orders to render electronic data temporarily inaccessible as envisaged in Article 158/B (4) b). With reference to electronic notifications received from the courts, the NMIA records the obligation to render electronic data temporarily inaccessible in a central database of court rulings issued to render electronic data inaccessible and shall immediately notify electronic communications providers about court rulings, and electronic communications providers have one working day to temporarily disable access to electronic data after the notice is served. The NMIA notifies the courts immediately about any failure by an electronic communications provider to comply with this obligation.

(6) The court lifts the obligation to render electronic data temporarily inaccessible as envisaged in Article 158/B (4) b) if

a) the web hosting provider complies with its obligation to remove electronic data temporarily,

b) the reason for issuing the order has otherwise ceased to exist, or

c) investigations have been terminated, except in case the option to issue an order to render electronic data permanently inaccessible exists under Article 77(2) of the Criminal Code.

(7) The courts shall immediately notify the NMIA about lifting the obligation to render electronic data temporarily inaccessible as envisaged in Article 158/B (4) b) and the NMIA removes the obligation to render electronic data temporarily inaccessible from the central database of court rulings issued to render electronic data inaccessible and shall immediately notify electronic communications providers about the termination of the obligation by electronic means, and electronic communications providers have one working day to provide access to electronic data after the notice is served.

(8) The obligation to render electronic data temporarily inaccessible as envisaged in Article 158/B (4) b) is lifted upon the termination of criminal proceedings. When the courts have refused to issue an order to render electronic data permanently inaccessible, the courts shall immediately notify the NMIA about lifting the obligation to render electronic data temporarily inaccessible, and the NMIA in turn shall remove the obligation to render electronic data temporarily inaccessible from the central database of rulings issued to render electronic data inaccessible and shall simultaneously notify electronic communications providers about the termination of the obligation by electronic means, and electronic communications providers have one working day to provide access to electronic data after the notice is served.

(9) The NMIA notifies the courts immediately about any failure by an electronic communications provider to ensure access once again.

(10) The courts, acting ex officio or upon a motion to that effect by the prosecutor, may impose a fine between one hundred thousand and one million Hungarian Forints on electronic communications providers that fail to abide by the obligation to temporarily disable or to restore access to electronic data. Fines may be imposed repeatedly.

Covert data gathering subject to judicial permit

Article 200 of the CPA

General rules

(1) In order to establish the identity, locate or arrest the perpetrator or to find means of evidence, from the time the investigation is ordered until the records thereof are presented, subject to a judicial permit, the prosecutor and the investigating authority may, without informing the person concerned

a) keep under surveillance and record the events in a private home with a technical device,

b) open, check and record with a technical device the contents of mail consignments and closed consignments which can be connected to an identified person, as well as learn and record with a technical device the contents of communications made by way of electronic telecommunication service,

c) learn, record and use data transmitted or stored by way of a computer tool or system (hereinafter: covert data gathering).

Investigative authorities put forward these in practice as follows:

Common regulation 11 of 2003 of the Ministry of Justice-Interior -Finance on enforcement of seizure and confiscation and on rules of handling assets seized during a criminal procedure, and on their registration, preliminary sale or destruction.

Common regulation 23 of 2003 of the Ministry of Justice-Interior on investigation protocol for investigative agencies under the authorisation of the Minister of Interior with detailed rules on investigation and rules for recording criminal investigation actions other ways instead of in minutes. In relation to Article 158/B158/D of the CPA on rendering electronic data temporarily inaccessible

Article 87/A. Paragraph (1) The Head of the investigative authority initiate rendering electronic data temporarily inaccessible towards the prosecutor.

(2) This motion on rendering electronic data temporarily inaccessible should contain the following elements:

a) name of the initiator authority, file number

b) name of crime according to the CC,

c) description of the historical facts,

d) suspicion of crime, and evidence proving the necessity and lawfulness of rendering electronic data temporarily inaccessible,

e) motion on rendering electronic data temporarily inaccessible according to the Article 158/B.

f) data on identification of the source of the electronic data:

fa) I address according to standard ipv4 or ipv6 and subnet Mask,

fb) domain name,

fc) URL address,

fd) port number,

g) name and address and all registered data of the preserver service provider, including name, address and residence of the company and also the name of the person is entitled to represent the company.

(3) In relation to paragraph (2) Point g) in case of foreign service providers, registered data in the resident State should be obtained.

(4) If all electronic data under a domain should be make temporarily inaccessible such a reference should be incorporated to the motion.

(5) If the exploration of the source of electronical data requires special skills, consultant should be used.

(6) If the temporary electronic data inaccessible making further maintenance is no longer justified or investigation has been closed – instead of the case when procedure according to Article 569 of the CPA takes place – indication should be sent to the prosecutor in order to stop the compulsory measures and restore data without delay. The Head of investigation authority is entitled to indicate such motion.

In relation to the content of the motion Paragraph (2) shall be applied mutatis mutandis.

(7) In relation to this Article

1. domain name: a specific part of the Internet that individually registered,

2. electronic data: data published via electronic communication network by service providers, which could be identified by unique identifiers, such as IP address and URL, domain name and port number

3.IP address: unique identifier in the network that shows with the connected subnet Mask, that where electronic data is available at,

4. port number in the TCP/IP and the UDP, and SCTP protocol for that purpose index server defining the logical connection,

5. URL address common power source identifier, which concludes in one single address the most important concerned data such as protocol, domain name, IP address, a port number, and the path at the target server.

Common regulation 17 of 2003 of the Ministry of Finance-Justice on investigation protocol for investigative agencies under the authorisation of the Minister of Finance with detailed rules on investigation and rules for recording criminal investigation actions other ways instead of in minutes contains exactly the same legislation as the above presented.

Of course these rules appear in parallel in the Act C of 2003 on Electronic Communication in relation to service providers. According to these rules service providers are obliged to operate a system which is capable of real-time traffic data monitoring and recording.

Cooperation in Rendering Electronically Published Information Inaccessible Temporarily or Permanently

Article 92/A of the Act C of 2003

(1) Electronic communications service providers functioning as intermediaries of mere conduit and network access services in accordance with the Act on Electronic Commerce and on Information Society Services (hereinafter referred to as "electronic communications service provider of access") shall execute the court order adopted in criminal proceedings, or as ordered by an authority referred to in specific other legislation, immediately upon receipt thereof, at the latest within one working day, on rendering information published by way of an electronic communications network inaccessible temporarily or permanently, by means of disabling access to such information.

(2) The Authority, if it finds that the electronic communications service provider of access fails to comply with the obligation delegated under Paragraph (1), shall order the given service provider to comply with the obligation without delay. If the electronic communications service provider of access refuses to comply despite of being ordered to do so, the Authority shall inform the court of competence, or the authority of competence referred to in specific other legislation, thereof.

(3) The court shall have the option to impose a disciplinary fine upon the electronic communications service provider of access in the amount specified in the Act on Criminal Proceedings. The authority referred to in specific other legislation shall have the option to impose a financial penalty upon the electronic communications service provider of access in the amount specified in said other legislation.

(4) The electronic communications service provider of access shall inform the users, disclosing the name of the court of competence or of the authority of competence referred to in specific other legislation and the number of the ruling, as to the legal basis for disabling access to the content in question temporarily or permanently.

(5) The electronic communications service provider of access shall move to disable access to electronic information temporarily or permanently in accordance with Paragraph (1) of Section 159/C if so ordered by the court or by the authority referred to in specific other legislation before the time of starting up the provision of services in Hungary.

Service Providers should collect and preserve the traffic data as follows:

The Authority's Role in Rendering Electronically Published Information Inaccessible Temporarily or Permanently

Article 159/B the Act C of 2003

(1) The Authority shall organize and monitor the execution of rendering electronic information inaccessible temporarily or permanently, on the basis of a court order adopted in criminal proceedings under Paragraph (5) of Section 158/D and Paragraph (6) of Section 596/A of Act XIX of 1998 on Criminal Procedure, or as ordered by other legislation, and also the rendering of electronic information inaccessible as ordered by an authority referred to in specific other legislation.

(2) Upon receipt of notice from the court or the authority referred to in specific other legislation by way of electronic means, the Authority shall communicate exclusively by electronic means to the electronic communications service providers of access the court order on rendering electronic information inaccessible temporarily or permanently, or the order of the authority referred to in specific other legislation for rendering of electronic information inaccessible.

(3) For the purpose of discharging the task delegated under Paragraph (1), the Authority shall operate the central database of rulings on disabling access to electronic information (hereinafter referred to as "KEHTA"), and shall process the data entries to that end. The data contained in the KEHTA are not considered public information,

a) it may be accessed only by the courts, public prosecutors, investigating authorities and by members of the competent Parliament committees if rendering electronic information inaccessible temporarily or permanently was ordered by a court,

b) it may be accessed only by the courts, public prosecutors, investigating authorities and by members of the competent Parliament committees if rendering electronic information inaccessible was ordered by the authority referred to in specific other legislation.

(4) Upon receipt of notice from the court or from the authority referred to in specific other legislation by way of electronic means, the Authority shall record in the KEHTA in the form of an entry:

a) the name of the competent court or the authority referred to in specific other legislation, and the case number;

b) the court order for disabling access to the electronic information, and for restoring access to such information;

c) data for the identification of, and access to, the electronic information in question.

(5) If the notice is incomplete, the Authority shall request the court or the authority referred to in specific other legislation for remedying such deficiencies by way of electronic means, and shall inform the court or the authority referred to in specific other legislation if execution of the order based on the data supplied may be problematic for the providers of electronic communications services.

Article 159/C the Act C of 2003

(1) Electronic communications service providers of access and providers of browsing and caching services are required to join the KEHTA so as to be able to comply with the court order or the order of the authority referred to in specific other legislation on rendering electronic information inaccessible, and for restoring access to such information, and for providing assistance for execution by way of disabling access to the results of any search made in connection with information that has been rendered inaccessible or by way of disabling access to the stored version of such information.

(2) Providers of public Internet access shall not be required to join the KEHTA if connected to the Budapest Internet Exchange (BIX) and to other international internet exchange points exclusively through another electronic communications service provider that has already joined the KEHTA.

(3) Data exchange between the KEHTA and electronic communications service providers of access or providers of browsing and caching services shall take place by way of electronic means, through a secure data link. Electronic communication between the courts or the authority referred to in specific other legislation, and the Authority shall take place by means of secure delivery service.

(4) The Authority shall - to the extent of the technical means available - participate in providing the technical environment necessary for the execution of court orders when so requested by electronic communications service providers of access and providers of browsing and caching services.

(5) If the Authority collaborates in rendering electronic information inaccessible temporarily or permanently as provided for in Paragraph (4), it shall conclude an agreement with the electronic communications service providers of access and providers of browsing and caching services affected. Within the framework of such cooperation the Authority shall provide access - by way of the methods and under conditions set out in an administrative agreement - for the electronic communications service providers of access and providers of browsing and caching services affected to technical support with facilities for rendering electronic information inaccessible.

(6) The internet exchange points located in the territory of Hungary, such as the Budapest Internet Exchange (BIX), shall cooperate in carrying out the measures defined in this Section.

(7) The Authority may publish recommendations regarding the best practices for the methods of execution of disabling access under this Section, and shall offer assistance to the courts, electronic communications service providers of access, and providers of browsing and caching services for the use of KEHTA.

One of the most frequently used opened investigation technique is the I-OSINT (Internet-based Open Source Intelligence). The search application and the social network analysis of the I-OSINT are great tools to search for people and companies. These are simple searching services offered by different webpages, and they can find a lot more information than the simple searching engines, if they are used in parallel.

If there is a suspicion that criminal offence was committed, the investigation must be ordered. Until this moment evidence can be collected by covered technics and actions. The investigating authority (if authorised by law) can carry out covered information and data gathering. One part of these requires judicial permission. These tasks are (if the judicial permission is granted) implemented by the National Security Special Service and ordered by the investigating authority.

Secret information gathering

Article 63 of Act on Police

(1) The Police shall be entitled to secretly collect information for the purposes of preventing, investigating, stopping the commission of criminal acts; finding the identity, capturing of perpetrators; finding persons under warrant or their whereabouts; or to gain evidence.

(3) The measures taken under paragraphs (1)-(2) and the data of the natural persons, legal entities and unincorporated organisations affected thereby shall not be disclosed.

(5) The authorised unit of the Police and, in respect of the data collected and the fact of information collection, the prosecutor and the judge shall be entitled to inspect protected state secrets without a special permit during the secret collection of information. The data and information specified in paragraph (2) may be disclosed to international and foreign criminal prosecution and judicial authorities on the basis of an international convention, treaty or agreement or, in lack thereof, on the basis of reciprocity if it is necessary for eliminating a serious and direct danger or preventing a serious criminal act, provided that the conditions of handling personal data are met by the foreign data handling organisation in respect of each data.

Secret information gathering not subject to a Court Permit

Article 64 of Act on Police

(1) In order to discharge its criminal tasks set out in paragraph (1) Article 63, the Police may

a) employ informers, trustees or other persons secretly cooperating with the Police;

b) gather and check information concealing the purpose of the procedure or employing cover investigators;

c) issue or use cover documents and establish and maintain cover organisations to conceal its own staff or persons cooperating with it and the police nature of the same;

d) watch and gather information from persons suspected of a criminal act and other persons related therewith as well as premises, buildings, other objects, land and road sections, vehicles and events which may be connected with the criminal act, and record its observations by sound, image, other signal or trace recording technical devices (hereinafter: technical devices);

e) use a trap not causing injury or detriment to health to detect the perpetrator of a criminal act or to get evidence;

f) employ informers, trustees or other persons secretly cooperating with the Police or cover investigators to make sample purchases; and - subject to a permit from the prosecutor - cover investigators to make false purchases, confidence purchases, infiltrate in a criminal organisation and - also subject to the provisions of paragraph (4) of Article 2 -to perform a controlled delivery.

g) If there are no other means of preventing or detecting crime or capturing or identifying the perpetrator, it may substitute the victim - in order to protect his/her life and corporeal integrity - employing a police officer;

h) gather information from communications systems and other data storage devices.

(1a) In order to detect property from crime during asset-recovery process the police may

a) employ the provisions of sub-paragraphs a) – c) and f) – g) of Paragraph (1) of Article 64;

b) watch and gather information from persons suspected of a criminal act and other persons related therewith as well as premises, buildings, other objects, land and road sections, vehicles and events which may be connected with the criminal act, and record its observations by sound, image, other signal or trace recording technical devices (hereinafter: technical devices);

c) use a trap not causing injury or detriment to health.

(2) In order to perform the tasks set out in paragraphs (1) and (1a), the Police may enter into secret cooperation agreements with natural persons, legal entities or unincorporated organisations. As part of such agreements, the Police may initiate the employment of the employees of such organisations who are important for the fight against crime as a regular police officer, public service or public servant (hereinafter: employment).

(3) In order to discharge its tasks set out in this Act, the Police may initiate employment - for a term set out in a relevant agreement - at the organisations referred to in paragraph (2).

(4) The Police shall not be entitled to initiate employment at a court of justice, prosecutor's office, the Constitutional Court, the State Audit Office, the Office of Ombudsmen, the Office of the President of the Republic and the Office of the Parliament.

(5) The special rules relating to the police nature of the employment shall be contained in the special agreement made between the Police and the organisation concerned, subject to the provisions of the relevant laws. The police nature of the employment shall be a state secret unless the parties to the agreement provide otherwise.

(6) In the case of threat to life, corporeal integrity or property or blackmailing or abetting to a criminal act, the Police may, at the user's written request and using technical devices, monitor and record telephone calls made on the user's line within the period set out in such request. Any irrelevant information obtained and recorded in the case shall be promptly destroyed.

(7) Law enforcement organisations and national security services may be used as cover organisations and their documents may be used as cover documents only after informing the relevant Minister and the national-level chief of the relevant organisation.

(8) In order to protect informers, trustees or other persons secretly cooperating with the Police, cover investigators, cover documents and cover institutions, the Police may place cover data in various public records including the personal data and home address registry, the personal identity certificate registry, the birth and death registry, the travel documents registry, the drivers' licence and motor vehicles registry, the real estate registry and the corporate registry. The placement of such covers data and the document or other data carrier containing the order for the placement shall be deemed state secret. The cover data shall be deleted after the underlying interest of criminal prosecution has ceased to exist.

(9) Compensation for damage caused to third parties by informers, trustees or other persons secretly cooperating with the Police during the secret collection of information shall be governed by the provisions in paragraph (2) of Article 67.

Secret information gathering subject to a Court Permit

Article 69 of Act on Police

(1) To attain the criminal prosecution objective set out in paragraph (1) of Article 63 and subject to a court permit, the Police shall be entitled in the case of serious criminal acts to

a) secretly search a private home (secret search) and record its findings;

b) to observe and record the events taking place in a private home using technical devices;

c) to get access to and record the information contained in letters, other postal sendings, or transmitted through telephone lines or equivalent telecommunications systems;

d) to get access to and use data and information generated by E-mail messages exchanged on the Internet or using other computer technology.

(2) Information collected using the devices set out in sub-paragraphs c)-d) of paragraph (1) relating to persons obviously not affected by the procedure on which the secret collection of information is based shall be promptly destroyed and shall not be processed and used any longer.

(3) The Police shall be entitled to use the devices and techniques of secret information collection (hereinafter: special devices) referred to in paragraph (1) according to the provisions set out therein for the purpose of finding a person searched under the suspicion of a criminal act and if the criminal act not mentioned in paragraph (1)

a) can be connected with cross-border crime;

b) is aimed at a minor;

c) is perpetrated in series or in an organised manner;

d) is connected with drugs or other narcotic substances;

e) is connected with the counterfeiting of banknotes or securities;

f) is perpetrated with arms;

g) is a terrorist act or act of terrorist type;

h) seriously disturbs public security.

(4) Detecting criminal acts against the State (Chapter X CC), criminal acts against humanity (Chapter XI CC), desertion (Article 343 CC), mutiny (Article 352 CC), endangering of combat-readiness (Article 363 CC) shall be the competence of the national security services until an investigation is ordered.

(5) Detecting terrorist acts (Article 261 CC) shall be the competence of the Police if the relevant report is submitted to the Police or if it became known to the Police.

(6) In the case of sub-paragraph c) of paragraph (1), the telecommunications or postal organisation shall give assistance falling within its competence.

(7) For the purposes of sub-paragraphs a)-b) of paragraph (1), 'private home' shall be deemed to include all other premises and locations open to the public in addition to sub-paragraph c) paragraph (1) of Article 97.

Article 70 of Act on Police

(1) The request for the application of special devices shall be submitted by the head of the investigation authority of the Police having competence and powers (hereinafter: the investigation authority).

(2) The request shall contain the following:

a) the place of application of the special device, the name and any other data suitable for identification and available to the Police, of the person affected by its application;

b) the description of the special device to be used;

c) the starting and ending date and time of the application;

d) the reasons providing the legal grounds of the application.

Article 71 of Act on Police

(1) The application of special devices is authorised by a judge of the local court competent according to the head office of the investigation authority requesting the permit who is appointed by the Chairman of the county (capital) court (hereinafter: judge).

(2) The judge shall make a decision within 72 hours after submitting a request for permitting the application of a special device; he/she shall either approve the request or reject it in the lack of lawful grounds.

(3) The judge may authorise the use of a special devices on a case-by-case basis for up to 90 days and may extend the permit by additional 90 days subject to a request set out in paragraph (2) of Article 70.

Article 72 of Act on Police

(1) If the permit procedure for the use of a special device would cause such a delay which would obviously injure the interest of criminal prosecution in the given case, the head of the investigation authority may order the secret investigation and the use of the special device for a period of 72 hours (urgency order).

(2) In the case of an urgency order the request for permit shall be promptly submitted. If the request is rejected, the urgency order shall not be repeated for the same purpose, on the same grounds or matter of fact.

Article 73 of Act on Police

(1) The head of the investigation authority shall promptly order to stop the use of a special device if

a) it has attained the goal specified in the request;

b) the deadline set out in the permit has expired;

c) it is obvious that no result is expected from any further use thereof;

d) its use based on an urgency order was not permitted by the judge.

(2) In the case of sub-paragraph d) of paragraph (1), any information recorded using the special device shall be promptly destroyed.

(3) Any information irrelevant to the objective of the investigation and the data of persons not connected with the case shall be destroyed within 8 days after the conclusion of the operation using a special device.

Article 74 of Act on Police

The permitting judge shall be entitled to inspect the data obtained and recorded during the secret collection of information subject to a special permit.

Covert data gathering subject to judicial permit

Article 200 of the CPA –

General rules

(1) In order to establish the identity, locate or arrest the perpetrator or to find means of evidence, from the time the investigation is ordered until the records thereof are presented, subject to a judicial permit, the prosecutor and the investigating authority may, without informing the person concerned

a) keep under surveillance and record the events in a private home with a technical device,

b) open, check and record with a technical device the contents of mail consignments and closed consignments which can be connected to an identified person, as well as learn and record with a technical device the contents of communications made by way of electronic telecommunication service,

c) learn, record and use data transmitted or stored by way of a computer tool or system (hereinafter: covert data gathering).

(2) After the order for the investigation has been issued, the prosecutor and the investigating authority shall perform covert data gathering which is subject to a judicial permit in compliance with this Act.

(3) The provisions set forth in this Title shall not apply to covert intelligence gathering performed prior to the order for an investigation, which is subject to a judicial permit or the permit of the minister in charge of justice; such activity shall be conducted by authorised organisations in compliance the rules governing them and separate legal regulations.

(4) If covert intelligence gathering has commenced under a separate legal regulation issued pursuant to a judicial permit or the permit of the minister in charge of justice prior to the order for an investigation, but then an investigation is ordered, thereafter covert intelligence gathering may only be continued in compliance with the provisions of this Act as secret data gathering.

(5) For the purposes of paragraph (1) a) “private home” means a home (holiday home, summer-house or other premises used for dwelling, establishment, object), premises, establishment or enclosed area belonging to the home but not intended to be used for dwelling, as well as any other premises or areas not open for the (general) public, or vehicle excluding community transport vehicle.

Article 201 of the CPA

(1) Covert data gathering may be applied to

a) a criminal offence committed intentionally and punishable by up to five years' or more severe imprisonment,

b) a criminal offence committed in a business-like manner or in a criminal conspiracy and punishable by up to three years' imprisonment,

c) illegal possession of new psychoactive substances, living on earnings of prostitution, violation of the freedom of conscience and religion, criminal offences with ozone-depleting substances, abuse of authority,

d) falsification of health care products, trafficking in human beings, pandering, procuring for prostitution or sexual act, child pornography, damaging of the environment, damaging the natural environment, violation of waste management regulations, harbouring a criminal, active bribery, passive bribery, active bribery of a public official, passive bribery of a public official, illegal immigrant smuggling, when punishable by up to three years' imprisonment,

e) criminal offences against classified data and public records and registers recognized as national assets,

f) an attempt of the criminal offences identified in paragraphs a)-e), further – if the law orders any preparations punishable – the preparation of the above.

(2) If the investigation is conducted by the prosecutor, covert data gathering may also be performed in the following cases apart from the criminal offences listed in paragraph (1):

a) assault on a public official or threatening to commit assault of an internationally protected person punishable by imprisonment for up to three years where the violence committed to the injury of a person enjoying immunity due to holding a public office or a person enjoying immunity under international law,

b) assault on a public official punishable by imprisonment for up to three years where the violence committed to the injury of judge, a prosecutor, a court clerk, a junior prosecutor, a legal trainee of the court or the prosecutor's office, an independent bailiff and a bailiff at a tribunal or their respective deputies, a notary public or an assistant notary public, a professional member of the police, Parliamentary Guard, National Tax and Customs Administration, or a financial investigator employed by the National Tax and Customs Administration in governmental service legal relationship, further, corruption criminal offences punishable by imprisonment for up to three years committed in relation of the above;

c) criminal offences against the administration of justice specified in Article 29 e), with the exception of misleading of authority,

d) criminal offences against the foreign public official,

e) criminal offences subject to military criminal law, listed in paragraphs a)-d).

Article 202 of the CPA

(1) The subject of covert data gathering may primarily be the suspect, or the person who may be suspected of having committed the criminal offence based on the available data of the investigation.

(2) Other persons may be subjected to covert data gathering if data indicate that they have culpable communications with the person specified in paragraph (1) or there is reasonable ground to suspect the same. The fact that an outsider is unavoidably affected shall not be an obstacle to covert data gathering.

(3) Covert data gathering may only be conducted in the private home and office of a lawyer acting as the defence counsel in the case, and in connection with the telephone line, other means of communication and correspondence (including electronically transmitted mail) of the lawyer if there is reasonable ground to suspect that the lawyer has committed a criminal offence related to the case in progress against the defendant.

(4) Covert data gathering may be conducted in the visitors' room for lawyers within a police detention room or in a penal institution if there is reasonable ground to suspect that the lawyer has committed a criminal offence related to the case in progress against the defendant.

(5) The provisions set forth in paragraphs (3) and (4) shall also apply to persons who may not be questioned as a witness pursuant to Article 81 (1) a) and those who may refuse to testify under Article 82 (1).

(6) Even in the cases specified in Article 201 and paragraphs (1) to (5), covert data gathering may only be conducted if obtaining evidence by other means reasonably appear to be unlikely to succeed if tried or would involve unreasonable difficulties, and there is probable cause to believe that evidence can be obtained by covert data gathering.

Judicial permit

Article 203 of the CPA

(1) Covert data gathering shall be permitted by the court at the motion of the prosecutor in compliance with the procedure set forth in Title VI of this Chapter.

(2) The motion shall contain the following:

a) the name of the prosecutorial body or investigating authority conducting the investigation, the date of the order for the investigation, the case number,

b) the location planned to be subjected to covert data gathering, including, in the case of eavesdropping, the phone number,

c) the name or data suitable for the identification of the person planned to be subjected to covert data gathering, as well as the description of the means and method of covert data gathering to be applied against this person,

d) the starting and ending time when covert data gathering is planned to be maintained, specified in calendar days and hours,

e) detailed description substantiating the conditions for the application as specified in Articles 201 and 202, thus especially the description of the underlying criminal offence and the data establishing suspicion that the criminal offence has been committed, the circumstances justifying that covert data gathering is indispensable, the objective thereof and facts establishing probable cause to believe that the evidence may be obtained by the means or method to be applied in the course of covert data gathering,

f) if applicable, the reason for and the date of an exigent order [paragraph (6)].

(3) The supporting documents shall be attached to the motion. Upon the submission of a motion for prolongation, the documents produced since the previous permit shall also be presented.

(4) The court shall adopt a decision within seventy-two hours following the submission of the motion. When the court fully or partially accepts the motion, it shall determine the subject person, the means and methods of covert data gathering and the time period for which the above means and methods may be applied in respect of such subject person.

(5) Covert data gathering may be permitted for a maximum period of ninety days; upon a repeated motion, this period may be extended for a further maximum ninety days on one occasion. If the court accepts the motion and by the time of the permit the starting day of covert data gathering as indicated in the motion has already passed, the actual starting day shall be the date of the permit.

(6) If the permission procedure caused a delay that would jeopardise the success of covert data gathering, the prosecutor may, for a maximum period of seventy-two hours, order covert data gathering (exigent order). In this case, simultaneously with the order, the motion for the permit shall also be submitted. If the court has rejected the motion, a new exigent order may not be issued based upon the same facts.

Performance of covert data gathering

Article 204 of the CPA

(1) Covert data gathering is performed by the organisation specified in a separate Act. If the subject of covert data gathering ordered in the course of an investigation conducted by the prosecutor's office is a criminal offence committed by a professional member of the national security services the prosecutor may also request the affected national security service to perform covert data gathering.

(2) The organisations forwarding, processing and managing communications services, pieces of mail and computer data stored in an information system shall be obliged to provide for the conditions of performing covert data gathering and co-operate with the authorities authorised to perform covert data gathering. The obligations of organisations providing communications services and forwarding mail and the detailed rules of co-operation are set forth in a separate legal regulation.

(3) Covert data gathering shall be forthwith terminated by the prosecutor or the head of the investigating authority if

a) in the case of an exigent order, the court has rejected the motion,

b) the objective specified in the permit has been achieved,

c) the time period specified in the permit has lapsed,

d) the investigation has been terminated,

e) its maintenance is unlikely to yield any result.

(4) Within eight days following the end of covert data gathering, the prosecutor or investigating authority having performed covert data gathering shall destroy the data which had been recorded but are of no interest for the objective of this covert data gathering, as well as the recorded data of persons not concerned in the case, with the exception of the data that may be used pursuant to Articles 206 (4)-(5). If paragraph (3) a) applies, the data recorded so far shall be immediately destroyed.

(5) A report (Article 168) shall be compiled on the performance of covert data gathering, detailing the process thereof, thus especially, the means and methods applied, the time period and location of the application, the natural persons, legal entities and organisations without a legal person that had been affected by the covert data gathering – except for the covert investigator (Article 178) –, and the data obtained in the course of covert data gathering – and not destroyed pursuant to paragraph (4) –, as well as the method, source, place and time of obtaining the data. The report shall allow establishing whether the provisions in the court permit have been complied with. The report shall also state whether covert data gathering has achieved its objective, or if not, the reason for failure. The report shall be signed by the head of the prosecutorial body or investigating authority having performed the covert data gathering.

Disclosure of the results of covert data gathering

Article 205 of the CPA

(1) Protection of the data produced and recorded during covert data gathering shall be the responsibility of the prosecutor or the investigating authority having performed the covert data gathering, in compliance with the provisions of the Act on the Protection of Certified Data.

(2) While covert data gathering is in progress and thereafter until the report thereon is filed by the prosecutor with the documents, the fact of performing covert data gathering, as well as the data produced and recorded in the course thereof may be disclosed only to the judge having issued the permit, the prosecutor and the investigating authority, further, by the superior (senior officer) of the prosecutor and the investigating authority. Court documents related to the permission of covert data gathering may also be disclosed to the superior in charge of distribution of cases of the judge having issued the permit, as well as the administrative superior of the same judge, as specified in Article 207 (1).

(3) At the request of the judge having issued the permit for covert data gathering, the prosecutor shall present the data obtained by covert data gathering until the time of such request. Should the judge establish that the permit has been misused, he shall, while in the event of other breach of law, he may terminate the covert data gathering. Such ruling may not be appealed.

(4) The results of covert intelligence gathering performed prior to the investigation under a separate legal regulation [Article 200 (3)] – until they are used in the criminal proceedings – may be disclosed to the persons specified in separate acts.

(5) After the conclusion of the covert data gathering, the prosecutor shall inform the person concerned by the judicial permit of the fact that covert data gathering had been performed, unless criminal proceedings have been instituted against such person and unless such notification jeopardises the success of the criminal proceedings.

Using the results of covert data gathering

Article 206 of the CPA

(1) If the prosecutor intends to use the result of covert data gathering as evidence in the criminal proceedings, the motion for the permit of the covert data gathering, the court decision and the report on the performance of covert data gathering shall be attached to the files of the investigation. If the documents are attached after disclosing the files of the investigation (Article 193), the suspect and the defence counsel shall be notified thereof and be allowed to examine the attached documents.

(2) After being attached to the files of the investigation, the report concerning the performance of covert data gathering may be used as evidence in accordance with the rules pertaining to documents (Article 116).

(3) The results of covert data gathering may only be used for evidencing the criminal offence due to which, and against the person for whom, the court permitted covert data gathering.

(4) If the court permitted covert data gathering against a specific person, the result of covert data gathering may also be used to evidence a criminal offence that was not designated in the permit, provided the conditions of covert data gathering stipulated in this Act (Article 201) also apply to this latter criminal offence.

(5) The results of the covert data gathering may be applied for evidencing the criminal offence concerning which the court permitted covert data gathering against all the perpetrators.

(6) The results of covert data gathering may not be admitted as evidence if covert data gathering was terminated pursuant to Articles 204 (3) a) or e) or Article 205 (3), or if the person concerned by the covert data gathering – without a court permit – is the defence counsel acting in the case, or a person who may not be questioned as a witness or may refuse to testify under Article 82 (1).

Using the results of covert information collection

Article 206/A of the CPA

(1) The result of the covert information collection for criminal law enforcement purposes and of the covert information collection for other than criminal law enforcement purposes subject to authorisation by a judge or by the minister responsible for justice matters can be used as an evidence in the criminal procedure only, if

a) the conditions of covert data gathering stipulated in this Act (Article 201) are met concerning the criminal offence subject to evidencing, and

b) the body asking for the authorisation of covert information collection has ordered the investigation or has fulfilled its obligation to lodge a complaint promptly after funding all the conditions for the initiation of a criminal procedure stipulated in this Act.

(2) The body asking for the authorisation of covert information collection initiates at the prosecutor the procedure on establishing the appropriateness of the using the result of the covert information collection at the same time of the initiation of the criminal procedure or the lodge of the complaint, if

a) the data emerged and recorded during the covert information collection for criminal law enforcement purposes is related to a person and/or a criminal offence not described in the authorisation,

b) the data emerged and recorded during the covert information collection for other than criminal law enforcement purposes is related to a person not described in the authorisation.

(3) In order to get the decision on the appropriateness of using the result of the covert information collection the prosecutor turns to the investigative judge within 72 hours. The use of result of covert information collection is appropriate, if the conditions stipulated in paragraph (1) are met, and there are reasonable grounds to presume that the collection of evidence otherwise would be beyond hope, or it would cause unjustifiable difficulties. The investigative judge decides in a ruling with an explanation of the reasons on the appropriateness of use. The decision on the appropriateness of use is without prejudice to the classified nature of the data emerged and recorded during the covert information collection. If the appropriateness of the use of the result of covert information collection is established, the data concerned shall only be destroyed if the prosecutor does not motion the use of it as evidence according to paragraph (4).

(4) The prosecutor may motion – after ordering the investigation – the use of the result of covert information collection, if the conditions stipulated in paragraph (1) are met. The investigative judge decides on the motion.

(5) The fact of the covert information collection subject to authorisation by a judge is verified by the president of the regional court. The verification contains the naming of the court, the number and subject of the case subject to authorisation, the name of the person subject to authorisation, the framework of the authorisation.

Cooperation in Covert Investigation and Covert Information Gathering Operations, and During Extraordinary Periods of Emergency and in the Interest of National Defence

Article 92 of Act on Electronic Communications

(1) Electronic communications service providers shall be required to cooperate with organizations authorized under specific other legislation by another act to conduct covert investigations and covert information gathering operations. Providers of electronic communications services shall operate facilities in their electronic communications systems so as not to prevent or block covert investigations and covert information gathering operations.

(2) At the request of the National Security Agency made in writing, providers of electronic communications services are required to come to an agreement with the National Security Agency within the time limit prescribed in specific other legislation concerning the application of the means and methods of covert investigation and covert information gathering operations.

(3) Providers of electronic communications services are required to inform the National Security Agency directly, concerning any activities, services, products, or any changes therein, to which the notification requirements prescribed under Paragraphs (1) and (6) of Section 76 do not apply, which, however, have the capacity to effect or influence the functioning of covert investigation and covert information gathering operations through the conditions, means, methods and procedures the providers of electronic communications services are required to provide.

(4) Providers of electronic communications services shall be required to ensure, at the time of commencement of providing the service as provided for in specific other legislation, the applications and means of access to the equipment and areas of operations, and the names of contact persons, concerning the consignments and messages forwarded through its electronic communications network and the data and information processed by the service provider to be obtained for the purposes of covert investigations and covert information gathering operations. In addition to the above, service providers shall also provide, when so requested by the National Security Agency, the means of access up to the exit point for the purposes of covert investigations and covert information gathering operations to the extent necessary as permitted by the technical characteristics of the service.

(5) Providers of electronic communications services shall be required to install the technical means necessary to comply with the requirements set out in Paragraph (4) in connection with electronic communications services, such as a basic monitoring subsystem, with access terminated at the exit point, for the National Security Agency within six months from the date of receipt of notice concerning the basic requirements in terms of technical means. All costs for the installation of a basic monitoring subsystem shall be borne by the service provider.

(6) Providers of electronic communications services shall supply - upon individual requests - information to agencies authorized to conduct covert investigations and covert information gathering operations, by way of direct electronic data link, via a platform installed by the provider of electronic communications services in compliance with the technical specifications supplied by the National Security Agency. If the electronic data link installed is unable to support access to the data requested, the provider of electronic communications services shall supply the data in question in writing or - if so requested - on electronic data medium. Providers of electronic communications services shall supply data to agencies authorized to conduct covert investigation and covert information gathering operations that did not request an electronic data link in writing or on electronic data medium. All costs and expenses incurred in connection with data supply facilities shall be covered by the providers of electronic communications services, and all data shall be supplied by the providers of electronic communications services free of charge.

(7) In the cases defined by the relevant legislation, electronic communications service providers shall cooperate with the operators of restricted government networks.

(8) For the elimination of breakdowns induced by reasons attributable to technical and traffic conditions, natural disasters and other reasons, service providers shall have incident, contingency and business continuity plans, with content defined in specific other legislation and reviewed and updated on a regular basis, and shall also have reserves in the quantities and of the composition required to fulfil the responsibilities prescribed by legal regulations on preparations.

(9) In the interest of working out and executing action plans applicable in the event of extraordinary emergency situations, electronic communications service providers shall cooperate, in a manner defined in specific other legislation, with each other and with the competent agencies.

(10) Electronic communications service providers shall be entitled to compensation with respect of their justified costs incurred in connection with the measures taken according to the action plans or services provided according to the relevant legal regulations in the course of extraordinary periods of emergency and in the interest of national defence.

Obligation to Retain Data for Reasons of Law Enforcement, National Security and Defence

Article 159/A of Act on Electronic Communications

(1) Electronic communications network operators and providers of electronic communications service shall be required - for the purpose of compliance with any request made by the investigating authority, the public prosecutor, the court or the national security service pursuant to the authorization conferred in specific other legislation, with a view to discharge their respective duties - to retain the data generated or processed by the service provider in connection with the provision of electronic communications services relating to the subscribers or users of such electronic communications services:

a) the data specified in Paragraph a) of Paragraph (5) of Section 129 related to fixed network telephony and mobile telephony services, internet access, internet telephony, internet mail services, or the combination of these;

b) in connection with fixed network telephony and mobile telephony services, internet access, internet telephony, internet mail services, or the combination of these, the telephone number allocated to the terminal equipment of the user or subscriber or to the subscriber access point, or the user ID or any technical identifier fixed in the subscriber contract or otherwise assigned to the subscriber or user by the provider of electronic communications services;

c) in connection with fixed network telephony services, fixed internet access services, or the combination of these, the address where the terminal equipment of the user or subscriber or the subscriber access point is installed, and the type of equipment;

d) in connection with fixed network telephony and mobile telephony services, internet access, internet telephony, internet mail services, or the combination of these, the telephone numbers of the users and subscribers participating in the communication, their technical means of identification, user IDs, type of electronic communication services involved, and the data necessary to identify the date, time and duration of a communication;

e) in connection with fixed network telephony and mobile telephony services, or the combination of these, in cases involving call forwarding or call transfer, the subscriber or user number or numbers to which the call is routed;

f) in connection with mobile telephony services, concerning the equipment used at the time of communication, the International Mobile Equipment Identity (IMEI) of the calling and the called party, and the International Mobile Subscriber Identity (IMSI) of the calling and the called party;

g) in connection with mobile telephony services, the location label (cell ID) and network identifier at the start of the communication, and the data identifying the geographic location of cells by reference to their location labels (cell ID) during the period when the service was provided;

h) in connection with internet mail services and internet telephony services, or the combination of these, the data referred to in Paragraph d) of the intended recipient(s) of the communication;

i) in connection with internet access, internet mail services, internet telephony services, or the combination of these, type of the electronic communication service, the date and time of the log-in and log-off by the subscriber or, together with the IP address allocated to the communication, and the user ID of the subscriber or registered user, including the calling number;

j) in connection with internet access, internet mail services and internet telephony services, or the combination of these, the data necessary to trace any changes made in the unique identifiers of subscribers and users by the provider of electronic communications services (IP address, port number);

k) in the case of pre-paid anonymous mobile telephony services, the date and time of the initial activation of the service and the location label (cell ID) from which the service was activated.

(2) The obligation to retain data provided for in Paragraph (1) shall include the retention of the data specified in Paragraph (1) relating to unsuccessful call attempts.

(3) Providers of electronic communications services, for the purposes of compliance with the obligation of disclosure referred to in Paragraph (1), shall retain the data specified in Paragraphs a)-

c) of Paragraph (1) for a period of one year following termination of the subscriber contract, the data specified in Paragraphs d)-k) of Paragraph (1) for a period of one year following the time they were generated, and the data specified in Paragraph (2) for a period of six months following the time they were generated.

(4) In connection with the data disclosures prescribed under Paragraph (1), responsibility for the legitimacy of such requests of information shall lie with the requesting party. The provider of electronic communications services transferring the data files shall be liable to ensure that the date retained and transferred according to Paragraph (1) are complete, of good quality and properly updated.

(5) Providers of electronic communications services subject to the obligation of retention prescribed in Paragraph (1) shall be authorized to subcontract their data processing operations, or to store the data retained in another Member State of the European Economic Area, if the agreement for the retention of data concluded with the data processing contractor contains provisions laying down the requirements for security and access in due compliance with Hungarian regulations concerning secrecy and the protection of classified information relating to the data requests made under Paragraphs (1)-(2). Providers of electronic communications services shall not be authorized to store any data retained in the territory of a country, and may not contract the services of a data processing contractor that is established in a country, which country is other than a Member State of the European Economic Area.

(6) For the purposes of this Section, ‘communication’ means any information exchanged or conveyed between a finite numbers of parties by means of a publicly available electronic communications service, including unsuccessful call attempts. For the purposes of this Section, this shall not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information.

(7) Bodies authorized to request data under specific other act shall prepare statistics and send it to the European Commission on a yearly basis. Such statistics shall include:

a) the cases in which service providers have provided information to the competent authorities in accordance with this Section,

b) the time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data,

c) the cases where the service provider was unable to meet requests for data.

The usage of special tools is permitted only if the previously mentioned criteria are met. If these criteria are met the legislation offers a wide frame regarding the tools and methods to be selected for the practical implementation of data gathering.

Regarding the topic of cybercrime it must be noted that the legislation does not define how the content of a communication provided by the electronical intelligence service, as well as the data provided by IT equipment or data stored on it, is used or recorded. Since the choice of the used method in not mandatory, it is not excluded that the excess to the IT system, of the person concerned, is carries out from a distance. This is obviously means that the activities of Hungarian authorities are limited in cases when the information systems are located in a foreign country. The covert data gathering can be carried out in these cases if a request for international procedural legal assistance was sent by the concerned country.

The documents derived from the covert information and data gathering are classified documents, which are handled by the concerned authorities separately from the ordinary databases, these documents are not present in the central registers. From this reason it is not possible to examine them, or to provide statistical summaries on the methods of covert data and information gathering. As guidance, we can note that the sample purchase, the ghost shopping, the trusted shopping or the examination of the content of electronical communication requires less activity than to infiltrate in criminal organisations or to examine and record the data stored on information systems. From this reason these methods can be used frequently in cases regarding copyright infringement and child pornography.

Often happens that persons under coercive measures cooperate with the authorities in order to achieve investigation bargain. During these bargains the persons concerned often provide information which is useful for the investigation of criminal offences regarding cybercrime.