

Crime prevention policy	
EU- priority	Cybercrime; <ul style="list-style-type: none"> • Child sexual exploitation • Payment card fraud • Cyber-dependent crimes
Country	Hungary
Year	2019

1. Overview of the field

Definition of cybercrime

By following the international trends the Hungarian Criminal Code covers the following factums of crime in connection with cybercrime.

Child pornography (Section 204)

Counterfeiting of Cash-Substitute Payment Instruments (Section 392)

Cash-Substitute Payment Instrument Fraud (Section 393)

Aiding in Counterfeiting Cash-Substitute Payment Instruments (Section 394)

Breach of Information System or Data (Section 423)

Compromising or Defrauding the Integrity of the Computer Protection System or Device (Section 424)

See the text of the Hungarian Criminal Code below:

http://thb.kormany.hu/download/a/46/11000/Btk_EN.pdf

Assessment of trends and developments

According to the gathered data by the Cyber Crime Unit of the National Bureau of Investigation in the previous year's breaches of Information Systems and the cost of the damages have increased. The perpetrators of child sexual abuse more often use systems/methods that protect their anonymity. In regard to cash-substitute payment fraud the Hungarian police forces said that they had seen a significant rise in the number of card-not present fraud cases. Also logic attacks on ATMs are on the rise over the last years.

Recent overview of statistics and research

According to the international trends some of the cyberattacks are functioning as online services and available for anyone who is willing to pay for them. As a result, many of these attacks are committed by younger and technologically less educated people. The responsible authorities are focusing on the distribution of the preventive goals through press conferences hoping to stir these youngsters toward a socially acceptable line.

Other national priorities besides child sexual exploitation, payment card fraud and cyber-dependent crimes?

According to the national and international experiences it is not necessary atm.

2. Crime strategy and coordination

Objectives of the crime strategy

National Cyber Security Strategy

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.*' 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. 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.

The objectives stated in the National Cyber Security Strategy are the following:

- a, Government coordination.
- b, Improved cooperation and efficient information sharing.
- c, Specialised institutions.
- d, Regulation.
- e, International cooperation projects.
- f, Awareness.
- g, Education, research & development.
- h, Child protection.
- i, Motivation of business actors.

Find the National Cyber Security Strategy of Hungary below:

https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf

Role of prevention in the crime strategy on state/regional/local level

The Hungarian Police is dedicated to prevention. They focus on awareness raising and child protection. They run several programmes (DADA, ELLEN-SZER, and Crime Prevention Advisors at schools) and occasional campaign at schools and they educate teachers and parents as well. On the Facebook page of the Police visitors can find preventive content and updates about the current trends.

Implementation of the policy (which level is responsible for the implementation and how is the implementation coordinated?)

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

There are three organisational units in the National Cyber Security Center according to their tasks, the National Electronic Information Security Authority, the GovCERT-Hungary for incident handling issues and the unit that is responsible for the security management and vulnerability assessment.

The tasks of the units:

National Electronic Information Security Authority

- registering the customers and systems data
- control of the identified security classes and security levels
- control whether the requirements are complied
- Imposition of vulnerability assessment
- suggestion for identifying a vital (information) system
- suggestion, to designate a person responsible for the security of electronic information systems

GovCERT-Hungary as incident handling unit:

- management of security incidents
- threat management
- duty service
- analysis / assessment
- cyber security exercise
- training, raising awareness
- support of the identification of the responsible person
- vulnerability assessment
- cooperation with Internet Service Providers in case of management of security incidents
- to inform regularly the Management
- security management and vulnerability assessment unit
- vulnerability assessment
- Investigation of security incidents
- perform tasks in connection with information security in the EMIR/FAIR systems

Further information about the National Cyber Security Center:

<http://nbsz.hu/?mid=2>

<http://www.cert-hungary.hu/>

<http://neih.gov.hu/>

Stakeholders (working groups, specialised agencies, partners, etc)

- Special Service for National Security, National Cyber Security Center
- Riot Police, National Bureau of Investigation Cyber Crime Unit
- National Tax and Customs Administration of Hungary (NTCA)
- National Directorate General for Disaster Management, Ministry of the Interior (NDGDM)
- Secret Services
- National Authority for Data Protection and Freedom of Information
- National Media and Infocommunications Authority
- The Hungarian Banking Association

Participation in European/ international networks, working groups, etc.

The Riot Police National Bureau of Investigation trade information on a daily basis with EUROPOL through SIENA to ensure the effective and quick data exchange in regard to cyber security.

Experts of the NBI also participate in the work of EMPACT and they take part in various trainings of CEPOL both as trainers and trainees.

3. Good practices

Overview of recent good practices, prevention programs, etc.

European Cyber Security Month : <https://kiberhonap.hu/>

In 2016 the NBI participated in the development of actions and campaigns that aimed to distract young people from criminal career. In the following years together with the Crime Prevention Department of the Police they take part in the campaigns of EUROPOL.

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

The National Media and Infocommunications Authority developed the Internet Hotline website where online content which is unlawful or detrimental to minors can be reported. <http://english.nmhh.hu/internethotline/>

The International Children's Safety Service (ICSS) coordinates different campaigns and serves as its national awareness centre - <http://www.biztonsagosinternet.hu/>

The Kék Vonal Child Crisis Foundation manages Hungary's national helpline - www.kek-vonal.hu

UNICEF Hungary developed an application called HelpApp - <https://unicef.hu/helpapp/>