Crime prevention policy	
EU- priority	Cybercrime; • Child sexual exploitation • Payment card fraud • Cyber-dependent crimes
Country	Czech Republic
Year	2018

1. Overview of the field

Definition of cybercrime

The Police of the Czech Republic defines cybercrime as crime committed using information and communication technologies including computer networks. Information and communication technologies themselves are attacked or offences are committed by using information and communication technologies extensivelly as important tools to commit these offences.

The Cyber Security Glossary defines cybercrime as follows:
"Criminal activity in which a computer appears in some way as an aggregate of hardware and software (including data), or only some of its components may appear, or sometimes a larger number of computers either standalone or interconnected into a computer network appear, and this either as the object of interest of this criminal activity (with the exception of such criminal activity whose objects are the described devices considered as immovable property) or as the environment (object) or as the instrument of criminal activity."

Assessment of trends and developments

Number of cases in the area of cybercrime rise every year while crime in general is in constant decline. It is assumed that there is growing transfer of activities into the realm of the Internet. The most common manifestations of cybercrime are various forms of frauds. A growing phenomenon in the field of fraudulent activity is that of drawing and transferring financial resources into virtual currencies, especially into bitcoins.
Phishing attacks are constantly on the rise. The so called hacking is the second most common act. The so called ransomware cases are also on the rise. There were, however, recorded cases of a big antivirus company trying to overestimate the level of danger by ransomware in the media to support sale of its own products. Furthermore, DDoS attacks, e-mail servers attacks, public administration servers and the critical information infrastructure attacks were recorded in 2017.
Vice crime in cyberspace is constantly on the rise, in 2017 this area experienced the highest annual growth. The most common vice crimes committed in cyberspace include: threatening moral development of children, distribution of pornography, production and other disposal with child pornography, abuse of a child for production of pornography, participation in pornographic performances, illicit contacts with child. Hate crime was on the rise in 2017. Phishing attacks aimed at collecting sensitive data (passwords, credit card numbers, etc.) in electronic communication but also at collecting sensitive data of the public administration

information systems. Identity thefts were detected used to compromise both physical and legal persons or to commit further crimes, especially fraud.

Recent overview of statistics and research

In 2017, 5.654 cases were recorded, that is slight increase (+310) compared to 2016 (5.344 cases). 3.140 fraudulent acts were recorded in 2017, that is 95 cases less than in 2016 (3.235 cases). 608 cases in the area of hacking were recorded in 2017 compared to 534 cases in 2016. The number of vice crime in cyber space rose in 2017 - 561 cases compared to 344 cases in 2016. In the area of hate crime, 318 cases were recorded compared to 265 cases in 2016.

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

Based on the objectives formulated by the National Cyber Security Strategy, the National Cyber and Information Security Agency defines wide area of social pathological phenomena and defective behavior online including:

- misuse of personal and sensitive data
- identity theft
- cyberbullying
- sexting
- social engineering
- cyber grooming
- child pornography
- hacking
- promotion of non-democratic regimes
- disseminating hate content
- education and awareness raising

2. Crime strategy and coordination

Objectives of the crime strategy

The Crime Prevention Strategy in the Czech Republic for 2016 to 2020 defines the strategic objective: “Czech Republic reacts to new threats and trends in the field of security and public order and applies new and efficient approach to prevention.” As part of this objective, it defines a specific objective in the area of new approaches to fighting cybercrime:

- To promote and implement projects aimed at combating crime in the virtual environment, in particular targeting dissemination of information about existing risks and possibilities of protection against them, including technical measures, and providing assistance and support to victims of crime on the Internet.

Objectives of the National Cyber Security Strategy:

A. Efficiency and enhancement of all relevant structures, processes, and of cooperation

in ensuring cyber security
B. Active international cooperation
C. Protection of national CII and IIS
D. Cooperation with private sector
E. Cooperation with private sector
F. Research and development / Consumer trust
G. Education, awareness raising and information society development
H. Support to the Czech Police capabilities for cybercrime investigation and prosecution
I. Cyber security legislation (development of legislative framework). Participation in creation and implementation of European and international regulations.

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

The National Cyber Security Strategy states that "the Czech Republic shall aim at a continuous development of cyber security expertise and of capabilities to resist the newest cyber threats. At the same time, it shall support and develop the prevention and early warning capacities of the state security forces. The National Security Authority decides on proposals and guidelines for prevention and solution measures in respect of cyber security incidents and ongoing cyber-attacks."

For role of prevention of cybercrime in the national Crime prevention strategy see 2. - Objectives of the crime strategy. Regions and cities create their own regional and municipal security strategies where prevention of cybercrime may be mentioned. There is no analysis available about the role of prevention of cybercrime through regional and municipal crime prevention strategies.

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

The Crime Prevention Strategy is implemented with the help of specific, measurable, and evaluable tasks that is a part of the subsequent Action Plan for Crime Prevention for the period of 2016 to 2020. The implementation of the Strategy is monitored and evaluated on an annual basis by the Government and updated where appropriate. The Minister of the Interior submits the Action Plan, after the preparatory period and its approval by the National Committee, to the Government.

Based on the main goals of the National Cyber Security Strategy and in coordination with all stakeholders involved, an Action Plan for the National Cyber Security Strategy is prepared to define specific steps, responsibilities and deadlines for their fulfilment and auditing. The NSA and the NCSC as its specialized department shall continuously monitor, discuss, and evaluate, in cooperation with other stakeholders, the levels of achievement of individual goals. It shall submit an annual "Report on the State of Cyber Security in the Czech Republic" to which information on fulfilment of the Action Plan shall be annexed. The report shall inform the government and the general public on effectiveness of measures adopted and on progress in fulfilment of tasks defined by the Strategy.

Stakeholders (working groups, specialised agencies, partners, etc)
Computer Emergency Response Team Computer Security Incident Response Team National Cyber and Information Security Agency National Security Authority of the Czech Republic

Participation in European/ international networks, working groups, etc.
STOP. THINK. CONNECT.™ is the global online safety awareness campaign to help all digital citizens stay safer and more secure online. The message was created by an unprecedented coalition of private companies, non-profits and government organizations with leadership provided by the National Cyber Security Alliance (NCSA) and the APWG. STOP. THINK. CONNECT.™ partners help create a culture of online safety and security by integrating STOP. THINK. CONNECT.™ into their education and awareness efforts and sharing the message in their communities. In this campaign the National Safer Internet Centre is involved and National Cyber and Information Security Agency is an observer at this moment. **MNCDE&T Project** The MN CD E&T project builds upon the fact that both at NATO and Allied nations levels, Education and Training (E&T) perform a central role in the development, operation and maintenance of skills and competencies associated with cyber defense capabilities. On October 2013, Portugal was invited to assume the leadership of a Multinational Smart Defense Project on Cyber Defense Education and Training (MN CD E&T). The aim of this project is to create a CD E&T Coordination Platform (central coordination point for a web of E&T activities) and to provide new initiatives to fulfil Nations' and NATO's CD E&T shortfalls. MN CD E&T will contribute to enhance national cyber defense capability development processes, as well as to improve interoperability between experts within NATO and Allies. Under the Smart Defense framework, Participating Nations will have the possibility to offer national CD E&T activities to NATO and other Allies, and obtain NATO certification on those activities.

3. Good practices

Overview of recent good practices, prevention programs, etc.
• **Police of the Czech Republic – the form to report defective content and activities** Whoever detects an internet content that might be harmful may report it to the Police via a form on the Police website. • **E-Safety (E-Bezpeci)** E-Safety is a national project dealing with a comprehensive solution to the issue of risky

behaviour on the Internet and related phenomena. It specializes in prevention, education, research and intervention. E-Safety was presented during the ECPA 2015. More information about the project in English (ECPA entry): https://eucpn.f2w.fedict.be/document/e-safety).
The project is led by the Centre for the Prevention of Risky Virtual Communication, Pedagogical faculty, Palacky University. The Centre focuses on prevention of hazardous behaviour associated with the use of information and communication technologies by children, especially cyber bullying, cyber grooming, cyber stalking, hoax and spam, sexting, social engineering methods, the issue of sharing of personal information through social networks and other dangerous communication techniques. It implements an educational, research, prevention and intervention activities. The Centre also focuses on positive using of modern IT technologies by children and adults. (http://www.prvok.upol.cz/)

- **Don't Be a Victim – Risks of the Internet and Communication Technologies Association**
  The project Risks of the Internet and Communication Technologies Association (a.k.a. Don't Be a Victim) is focused on preventive education of pupils in elementary schools, teachers and parents in areas of dangerous use of the Internet and communication technologies. Our association warns against possible misusing of personal information and it gives information about new phenomena in cyberspace such as sexting, grooming, phishing or happy slapping. We are engaged in making videos, production of comic strips and educational programmes, organisation of lectures and international co-operational projects.
  The Do Not A Victim Mission is to protect children from the threats and risks of the virtual world and modern communication technologies through preventive education and various projects and events, and with the help of lectures and trainings we try to address secondary target groups of parents, teachers, school leaders, Ostrava and the Moravian-Silesian Region, Librarians of the Ostrava City Library. Within the Moravian-Silesian Region, we are the only organization specializing in Internet and communication technologies that actively organizes and organizes events aimed at minimizing these risks, in which we repeatedly and actively involve our primary target group of pupils of elementary and secondary schools and apprenticeships. (http://www.nebudobet.cz/)

- **Online Helpline** https://pomoconline.saferinternet.cz/o-online-helpline/jak-fungujeme.html

- **Safer internet**
  Safer internet (SI) is a website that offers complex information about safer internet use as well as services concerning education, illegal content reporting and help for people bullied on the internet. It is part of Safer Internet project. Safer Internet is operated by National Centre for Safer Internet and cofounded by European Commission. It is a part of European INSAFE network, that comprises of 31 national awareness centres (27 of the EU member states, plus Iceland, Norway, Russia and Serbia). The goal of Safer Internet is to serve as an awareness centre for empowering children, their parents and teachers to make the best use of the Internet, building on enhanced digital resource centres (repositories), from which specific awareness toolkits and services will be adapted and deployed, in cooperation with third parties (schools, industry). Safer Internet also operates Pomoconline.cz (Help line) for reporting and dealing with harmful contact (e.g. grooming, online abuse), conduct (e.g. cyberbullying, hate speech, sexting) and content online and Stoponline.cz (Hotline) for receiving and managing reports and data on online illegal child sexual abuse material. (https://www.saferinternet.cz/english.html)

- **Regions for Safer Internet**
  The Regions for Safer Internet Project has started as the initiative by the Association of Regions of the Czech Republic. 12 regions of the Czech Republic actively cooperate as partners in terms of the project. The main aim is to increase the awareness about risks connected with the use of internet and methods of prevention and assistance. Within the project, there were created online quizzes for students and E-learning courses for children, students, teachers, parents and public, police officers, and social workers. The project continues with educational seminars for various target groups and more knowledge online quizzes for students. (http://www.kpbi.cz/en)
  More information about the project (ECPA entry): http://eucpn.org/document/regions-safe-internet.

- **Videos by the Police of the Czech Republic** warning young people not to share their intimate photos: https://www.youtube.com/watch?v=7820hxcXj2A (long version) and https://www.youtube.com/watch?v=rT0tKTXsif0 (short version) and videos for parents: https://www.youtube.com/watch?v=KIjxtRLvRW4 (long version) and https://www.youtube.com/watch?v=FhujQP52_xM (short version).

- **#SayNo! European campaign**

- **Safe on the Internet (Internetem bezpečně)**
  The aim of the project is to raise awareness on risks in cyberspace through various educational activities. It addresses new threats on its website and during educational events in order to prevent consequences of such threats and eliminate crimes committed on the Internet. The project aspires to be innovative; it uses new educational methods, trends and interactive approaches. As part of the educational activities the project presents practical examples of cyber threats and directions against them. The target group includes children and the youth, parents, disabled, teachers, crime prevention specialists, social workers, policemen etc. **https://www.internetembezpecne.cz/**