Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Lukáš Vilím, *Connections QJ* 20, no. 2 (2021): 15-20
https://doi.org/10.11610/Connections.20.2.02

Research Article

Evolution of Police Roles in Combatting Cybercrime in the Czech Republic, 2015-2020

Lukáš Vilím

Ministry of the Interior of the Czech Republic, https://www.mvcr.cz/mvcren/

Abstract: The article reviews the expanding roles of the Police of the Czech Republic in countering cybercrime. The author emphasizes the importance of conceptual and strategic considerations underlying the emergence of new legislation, the financial support for purchasing new equipment, and the creation of new staff positions for professionals in cybercrime. Furthermore, it is of utmost importance to develop new strategies in line with the threats, challenges, and opportunities in cyberspace. Enhanced cooperation at all levels of the security system can facilitate the creation of strategies and thus make cyberspace a safer place.

Keywords: cybercrime, Budapest Convention, security system, strategy, contact point, critical information infrastructure.

A significant milestone in the fight against cybercrime in the Czech Republic is the Government's approval on July 10, 2017, of the "Concept for the Development of the Cybercrime Investigation Capabilities of the Police of the Czech Republic" (hereinafter the Concept) under number 502.

Of course, in this context, we cannot overlook the professionals who had been dealing with cybercrime earlier, whether at the local, regional, or national level. Certain changes in addressing this issue were already introduced in October 2015, when the Organized Crime Unit (*Útvar pro odhalování organizovaného zločinu – ÚOOZ*) began to deal intensively with cybercrime. In 2016, countering cybercrime became part of the conceptual program of the newly established nationwide unit of the National Organized Crime Agency (*Národní centrála proti organizovanému zločinu – NCOZ*). It must be noted as well that law enforcement authorities have paid attention to criminal activities in cyberspace since the launch of the Internet.

However, the Concept mentioned above was the first in the Czech Republic to address this issue comprehensively. It focused on various areas of action to strengthen significantly the ability of the Police of the Czech Republic to fight this type of crime – from the field of personnel reinforcement and education to legislative changes with impact across the entire Police of the Czech Republic. The text of the decision to adopt the Concept, also published on the website of the Czech Government, announced that the Concept

> changed the organization and staffing of the Police of the Czech Republic from September 1, 2017. Thirty positions for members of the Police of the Czech Republic are added, with the respective increase of the budget for salaries of serving members of the security forces by CZK 4,595,280 in 2017. This decision will have a lasting effect for the subsequent years, with the implementation of the requirements for 2018 and the medium-term outlook for 2019 and 2020. The allocated budget will exceed the already approved limits for the Ministry of the Interior … and 73 new positions will be added as of 2018.

The Concept set high demands for all those who participated in its implementation and worked to meet the requirements therein. Its advantage was in establishing a clear direction for detecting, documenting, and investigating this new kind of criminal activity. There has been a reinforcement of staff followed by a new system of education that should be able to train and educate police officers dealing with this specific issue at all levels.

In terms of legislation, Act No. 141/1961 Coll., On Criminal Procedure (Criminal Procedure Code) concerning the collection, storing, using, exchanging, and destroying of data was consequently amended. Attention was also paid to detecting, documenting, and investigating attacks on critical information infrastructure, including its protection against terrorist attacks, through amendments to Act No. 40/2009 Coll., The Criminal Code. More specifically, a new item (e) was added to the first paragraph of Article 311, thus adding severe attacks on computer systems essential for society and the state's operation (including important information systems and critical information infrastructure).

The importance of section 311 e) is in its focus on terrorist attacks in cyberspace and the related need to protect the constitutional system or the defense of the Czech Republic, as well as the basic political, economic or social structure, the citizens, and international organizations against political or extremist violence. A terrorist attack of this type can break the law by inserting data into a computer system or information rack or deleting or damaging data stored in a computer system (information rack) by reducing its quality or rendering it unusable. An attack against a computer system may affect the functioning of the state, the health of persons, the security, the economy, or the provision of the basic living needs of the population. Furthermore, an attack utilizing tailored

malware may impact a large number of computer systems and cause considerable damage.[1]

In 2019, the issue of expedited retention of data stored in a computer system or on an information carrier for the purposes of criminal proceedings was simplified when § 7b was added to the Criminal Procedure Code, allowing, under the fulfillment of specified conditions, to order a person to carry out expedited retention of data important for criminal proceedings. According to § 7b, data retention is a preliminary measure that provides the police authority with the necessary time to secure the data.[2]

Another relevant norm was introduced through amendment of Act No. 104/2013 Coll., On International Judicial Cooperation in Criminal Matters. A new § 65a enabled the provision of expedited transfer of data stored on a computer system located in the territory of a foreign state. This Act directly regulates the use of the relevant contact point for cybercrime of the Police of the Czech Republic to make data preservation requests abroad upon the consent of the Public Prosecutor's Office. Among the European member states, the stored data is requested through the European Investigation Order. Such request is issued or validated by the judicial authority in one EU country to allow the application of investigative measures to gather or use evidence in criminal matters carried out in another EU country. It is valid throughout the EU but does not apply in Denmark and Ireland.[3] Outside the European Union, data is requested through a Mutual Legal Assistance Treaty (MLAT) – an agreement between two or more countries to gather and exchange information in an effort to enforce public or criminal laws. A mutual legal assistance request is commonly used to formally interrogate a suspect in a criminal case when the suspect resides in a foreign country.[4]

A National Contact Point for Cybercrime was established to facilitate cooperation in an exemplary manner and thus fulfill the tasks arising for the Czech Republic from the Council of Europe Convention on Cybercrime (Convention on Cybercrime, Budapest, November 23, 2001, ETS No. 185). The necessary tasks are performed 24/7. This contact point also contributes significantly to the detection of cybercrime and is involved in saving lives in cases of suspected threats to life and health in cyberspace. The Czech National Contact Point for Cybercrime respects the following laws and conventions:

---

1 Act No. 40/2009 Coll., "The Criminal Code of the Czech Republic," section 311, letter e).

2 Act. No. 141/1961 Coll., "The Criminal Procedure of the Czech Republic."

3 Eurojust, European Union Agency for Criminal Justice Cooperation, "European Investigation Order," accessed April 18, 2021, https://www.eurojust.europa.eu/judicial-cooperation/eurojust-role-facilitating-judicial-cooperation-instruments/european-investigation-order-eio.

4 European Commission, "Mutual Legal Assistance and Extradition. Combating Crime Across Borders," https://ec.europa.eu/info/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/mutual-legal-assistance-and-extradition_en.

- National Cyber Crime Contact Point pursuant to Article 35 of the Convention on Cybercrime (the Budapest Convention, ETS No. 185)
- Contact Point pursuant to Article 13 – Directive 2013/40/EU of the European Parliament and of the Council of August 12, 2013, on attacks against information systems – in cooperation with the national investigation division
- Contact Point pursuant to the EU Law Enforcement Emergency Response Protocol to handle major cross-border cybersecurity attacks – in cooperation with the national investigation division
- Contact Point for the Czech Banking Association (CBA), for an administrator of .cz domain and a national CSIRT team (CZ.NIC)
- Contact Point – G7 24/7 HTC Network.

The main tasks pursuant to Article 35 of the Convention on Cybercrime are:

- provision of technical advice
- preservation of data
- collection of evidence
- provision of legal information
- localization of suspects and missing persons
- communication with the other contact points on an expedited basis.

The four-year development of the fight against cybercrime based on the presented Concept was successful. This was confirmed in the Resolution of the National Security Council of the Czech Republic on June 8, 2020, approving the "Final Report on the Fulfillment of Tasks Resulting from the Concept for the Development of the Cybercrime Investigation Capabilities of the Police of the Czech Republic." It also decided on the development of a new strategy to combat cybercrime.

The fact that the issue of cybercrime is still evolving dynamically and the ever-more-notable increase in crime in the virtual world suggests that even greater efforts will be needed in the future to tackle cybercrime. Towards this end, attention will be required from law enforcement agencies and other security experts, whether in the civil service or the private sector. Cyberspace has become an integral part of our daily lives, which poses a number of risks and needs to be properly secured.

In the 21st century, it will be necessary to focus not only on the common crime committed in the virtual world but also on securing critical information infrastructure. This is a comprehensive problem that affects all levels of the security system and includes crisis management. It is necessary to realize that critical infrastructure is essential for society and the functioning of a democratic state and a cornerstone of a thriving economy. Its protection is therefore vital in order to prevent the escalation of incidents into crises.

The security of critical information infrastructure in cyberspace can be divided into three basic levels: cyber defense, cyber security, and cybercrime. Institutionally speaking, the provision of security requires effective and coordinated activities of the armed forces, the relevant cyber security office (The National Cyber and Information Security Agency; *Národní úřad pro kybernetickou a informační bezpečnost – NÚKIB*), the security forces (especially the Police of the Czech Republic), eventually the intelligence services, as well as the private sector.

The state's role also lies in setting basic security standards and legally enforcing them on the private sector. However, these measures must not be financially detrimental, and the state must ensure the adequate protection of cyberspace. It should be borne in mind that a significant part of the state's critical infrastructure is not in its exclusive ownership. The state merely participates in its management in a majority or minority role.

Related to this is the further need to define the division of cybercrime in order to give space to computer technology experts to detect, document, and investigate serious cases of cybercrime, such as attacks on cyber information infrastructure and essential information systems, which may have different origins, including the most serious ones such as terrorism or espionage.

To this end, cybercrime has been redefined, namely as:

- a crime committed in the environment of information and communication technologies, including computer networks where the main target of the attack is the area of information and communication technologies itself and the data contained in them; it follows that the primary attention of experts will be on meeting the established criteria – examples are § 230 Unauthorized Access to a Computer System on an Information Carrier, and § 231 Acquisition and Encoding of an Access Device and Password to a Computer System and Other Similar Data;
- any other crime committed in cyberspace, defined as a crime committed with the significant use of information and communication technologies where the main target of the attack is primarily life, health, property, freedom, human dignity, and morality.

Conclusion

For the reasons mentioned above, a new cybercrime strategy will need to be developed in the near future, which will need to consider many factors, including close cooperation among the various partners who play an important role in ensuring the security of cyberspace. The new strategy is to be submitted to the Security Council of the Czech Republic in 2021. It cannot be ruled out that it will be influenced by the COVID-19 pandemic, which forced a large part of society to work and spend its free time on the Internet; for some, it became a second living space. Last but not least, it can also focus on cyber defense against ransomware attacks on critical information infrastructure by criminal organized groups as well

as hostile powers and their investigation. Another serious future challenge will be the fight against disinformation campaigns, which, however, will require more comprehensive cooperation across the entire security system, and not only in the Czech Republic.

The Budapest Convention on Cybercrime can be used as a good example of how to approach other security challenges in cyberspace. Therefore, I can state with peace of mind that the Czech Republic is on the right track in the fight against cybercrime and believe that it will make the needed enhancements in the future.

Disclaimer

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

Acknowledgment

This article presents research results from the project V20192022117 "Detection of Radicalization in the Context of Protection of the Population and Soft Targets from Violent Incidents," supported by the Ministry of the Interior of the Czech Republic.

Connections: The Quarterly Journal, Vol. 20, 2021, is supported by the United States government.

About the Author

Lukáš Vilím is Lieutenant Colonel in the National Organized Crime Agency in the Ministry of the Interior of the Czech Republic, a police officer in the Cybercrime Unit of the Criminal Police and Investigation Service in Prague. He holds a Ph.D. degree from the Police Academy in Prague. Dr. Vilím is a graduate of the Cyber Security Studies program and the European Security Seminar-East of the George C. Marshal Center.
E-mail: lukas.vilim@email.cz