

Abstract

Today, the phenomenon of cybercrime can no longer be considered something obscured or unknown to the general public. Yet the majority of general population is aware of only a fraction of the offenses committed in cyberspace. As a result, a substantial proportion of Internet users act in violation of valid legislation in cyberspace, whether they do so knowingly or not.

Cybercrime cannot be considered less dangerous than other forms of crime. On the contrary, due to its availability, globality and possible distance of the offender from the crime itself, this kind of criminal behaviour is on the rise year by year and its effects are becoming more severe, mainly due to the dependence of today's society on information and communication technologies.

The aim of this thesis is to provide an introduction to the cybernetic world crime and offer a general view of the various aspects of this criminal activity.

The introduction of my thesis deals with detailed description of the basic terminology present throughout the whole thesis and contains a brief description of the history and origins of the computer and Internet.

An essential part of my thesis is the presentation of the legislative framework in the field of cybercrime regulation. This section mentions the laws that apply in the cyberspace environment and changes in the international regulations that affect the national legislation.

The third part of the thesis deals with specific features of cybercrime that are characteristic for this type of criminal activity and the occurrence of which makes this criminality a phenomenon.

A more extensive chapter in the entire thesis is the part dealing with the subject of a crime, namely the perpetrator and their victims. In this chapter, the general characteristics of a perpetrator and a victim are provided first. Subsequently, specific offenders who are found in cyberspace are described.

The most extensive chapter of the whole thesis is the part that aims to provide an almost complete list of individual types of crimes that occur in the cyberspace environment. These crimes are divided into four sections that correspond with the international regulation. In certain instances a well known examples of criminal cases are mentioned, in order to provide a better notion of the severity of this criminality.

The sixth chapter features individual foreign institutes in the field of defense against cybercrime and their effectiveness. The countries mentioned are France and it's efforts to solve problems related to copyright infringement law and the United Kingdom with its regulation of

child pornography. The last chapter of this work contains two parts. The first part focuses on the current state of cybercrime in the Czech Republic and its prognosis. The second part focuses on the matters how law in this area should be constituted and on individual non-functional and unregulated institutes in Czech law system.