ABSTRACT

The internet and computer criminality is a part of a cybercrime which is a very wide and relatively inhomogeneous category of criminal offences. The master's thesis focuses on criminal offences against confidentiality, integrity and availability of computer data and computer systems. These cyber attacks can endanger the cyber security at the national level and inflict immeasurable damage. In the present day, a Cybersecurity Act is being prepared in the Czech Republic whose goal is to respond to these attacks. Master's thesis examines especially penal aspects of this law. Moreover, a large space in the thesis is devoted to the recently ratified Convention on Cybercrime.

Besides the two above-mentioned legal norms the master's thesis arises from the Czech and foreign legal regulation and case law, for which it uses literature available in the Czech, English or German language. With regard to the chosen topic, it has been necessary to use also considerable amount of a non-legal literature.

The whole work is divided into six chapters. The first chapter provides a brief introduction into the topic and also short explanations of the basic terms. Chapter two provides questions about legitimacy and beneficial effect of a state regulation in the cyberspace which are of a partially philosophical character. This section also describes specifics in the cyberspace which should be taken into account while judging the cybercrime and before every legal regulation of the cyberspace as well. Chapter three focuses on *modus operandi* of the criminal offences committed in the cyberspace. Chapter four summarizes fundamental European and international legal instruments for fighting the attacks against confidentiality, integrity and availability of computer data and computer systems. Chapter five deals with the criminal offences in the Czech Criminal Code which are relevant to the topic. The last chapter evaluates the penal consequences which are arising from the future Cybersecurity Act.