NÁZEV DIPLOMOVÉ PRÁCE V ANGLICKÉM JAZYCE

The Criminalization of Cyberattacks on Information Systems

ABSTRACT

Cybercrime represents an increasing danger to human society. The main aim of this thesis is to find out which attacks on information systems pose a threat to the state and whether new technological trends represent a challenge for the current Czech legislation in the field of criminal law. The methodology varies across this thesis. The analytical method together with the synthesis is used to fulfil the aim. In some parts, an empirical approach is used.

The introductory part of the thesis explains the key institutes in the field of cybercrime and international instruments for combating cybercrime. The most important document is the Council of Europe Convention on Cybercrime. The main part of the thesis is devoted to the difficulties of current Czech legislation in connection with cyberattacks. The final part of the thesis deals with current technological trends, such as Artificial Intelligence, Cloud Computing, Cryptocurrencies and the Internet of Things, which play an important role in the field of attacks on information systems.

The current Czech legislation has responded to the growing tendency of cybercrime, and therefore new types of criminal offenses have been introduced. Artificial Intelligence is primarily a problem in terms of liability for the crime. Cloud Computing poses a challenge in criminal investigations, specifically in securing evidence. Cryptocurrencies can very well serve to hide money obtained from crime. The interconnection of all things within the Internet of Things creates vulnerable structures that can be attacked. Although the current legislation is sufficient, the development of technology is so turbulent that a new legal framework will need to be adopted in the near future. At the same time, it is appropriate to increase the security of computer systems, both at the state level and at the level of the users themselves.

KEYWORDS

cybercrime, cyberspace, cyberattack