Summary

"Cybercrime in the Silesian Voivodeship. Study on risk sociology"

The PhD dissertation deals with the problems of cybercrime and the risks associated with its occurrence.

The main scientific objective of this PhD dissertation is to examine the risk level associated with the phenomenon of cybercrime in the Silesian voivode ship. Not only the knowledge of policemen about the threats to the chosen phenomenon was examined, but also the personal attitude to take risk and their behavior taken on the Internet. Taking into account the above-mentioned research goal, main research problems have been formulated:

- What is the role of risk and readiness to take it in the lives of the respondents?
- How intensively do the respondents use the Internet?
- What do the respondents consider as the essence of cybercrime?
- What are the hazards on the network of the respondents so far?
- What is the level of knowledge of the respondents on the copyright protection?
- What is the attitude of the respondents to share personal data with a person met on the Internet?
- What are the possibilities of specialized police divisions to fight cybercrime effectively?

In order to find answers to the above questions, the following main research hypothesis was formulated: knowledge of police officers regarding cybercrime is limited, unstructured and requires trainings to improve their professional qualifications. The questionnaire addressed to the Police employees was considered as a reliable and effective research technique. These people have a professional contact with crime, including often with various types of cybercrime and its victims. Their answers to questions about the subject of the study can, therefore, be considered as highly reliable.

The research was supplemented by interviews conducted with specialists dealing with combating cybercrime.

The thesis begins with a theoretical presentation of the risk sociology issue and the Internet impact on interpersonal communication. The free flow of information and opinions on the Internet has fundamentally changed social communication, causing – through anonymity – the disclosure of many extreme behaviors and worldviews.

The next chapter presents a review of literature to present cyberspace as a risk space – the possibility of using modern technologies in the field of information processing contrary to its purpose.

In the third chapter, views on threats related to a specific form of cybercrime – cyber terrorism – were collected and systematized.

The fourth chapter deals with threats from cyber-terrorists for the basis of the functioning of society. Focuses on the issue of securing individual systems necessary for the functioning of society against cyber-attacks.

The fifth chapter is devoted to the approximation of the threat to the functioning of basic social systems related to cybercrime. The aim was to present and approximate the forms of cybercrime chosen because of their universality.

The sixth chapter focuses on the depiction of cybercrime threats that are lurking in the network for the ordinary user.

The seventh chapter is devoted to the presentation of the phenomenon of cybercrime in selected countries of the European Union. It also presents the regulations in the field of combating cybercrime and organizations & services dealing with this problem in force in the EU and Poland.

The eighth chapter deals with presenting the methodology of own research, defining the basic premises for carrying out research, methods and techniques used in the research part.

The ninth chapter contains an overview of available statistical data on the phenomenon of cybercrime and published research results on this subject. In particular, available police statistics were used.

The tenth and eleventh chapter present the results of research on the phenomenon of crime and cybercrime.

The research was performed in the police officers' environment, as people who have direct contact with the phenomenon of cybercrime and especially their fight against it. The idea was to acquire the knowledge they accumulate during everyday business activities as part of conducting cases related to crimes in cyberspace.

The author's intention was that the thesis would contribute to further development of the combat cybercrime program, with particular emphasis on the specificity of the Silesian region. That is why the thesis ends with recommendations of specific police activities to improve their capabilities in the field of combating cybercrime.

The main objective of the thesis was carried out on the basis of compact literature and other literature, due to the research issues also many internet publications were used. The current legal regulations, both national and EU, were also very important.