Summary

The dissertation addresses the topic of the level of digital competences of network (Internet) users and their possible impact on the cyber security system of the Republic of Poland. The main aim of the dissertation is to examine existing solutions of polish state within the scope of activities implemented for building and improvement of digital competences of users specified in strategic documents and strategic documents and legal regulations on the cybersecurity of the Republic of Poland. Hypothesis is as follows: effective raising of awareness and digital competences may be of key importance for shaping the system of the country's cyber security.

The work is of a theoretical and empirical. Chapters I-V are devoted to introduce and explain the basics related to cyber security, cyber digital competences and legal regulations in this area. The next part of the dissertation analyses the expert interviews and survey conducted survey. In order to obtain the data necessary to answer the questions presented in the dissertation, five expert interviews and a survey of 1,500 teachers and 2,500 students were conducted.

Chapter I was devoted to the methodological foundations of the dissertation. It covers the reasons to undertake the research, the subject of the study, its purpose, and the research problems. The working hypotheses, research methods and research limitations are also detailed. A analysis of the state of knowledge, which included a review of the literature on the subject.

Part II, entitled ‘The essence of cyber security’ mainly covered terminological issues and the conceptual scopes of ‘cyberspace’ and ‘cyber security’. At the end of the chapter, as in the previous one, the author's own conclusions were concretised.

Chapter III handle with strategic documents policy documents and legal regulations in the area of cyber security. Consideration was given to both national and international legal conditions. Entities and institutions competent in the area of building digital awareness and competence. The conclusions include concretised content and examples.

With reference to the legal regulations of individual countries, discrepancies in the area of cyber security should be bridged. Each EU member state must comply with certain criteria that are set before it. This is to facilitate co-development of an integrated system to ensure effective security in cyberspace. These measures should focus on the security of citizens and the country as a whole, so that every user can freely and without fear of taking full advantage of the inventions brought about by digitisation and the development of ICT technologies.

The following part of the dissertation indicates identification, classification and characteristics of threats in cyberspace, i.e. attacks, theft, blocking of access, spam or socio-technical attacks and the resulting challenges of of cyberspace.

When analysing the problem of threats in cyberspace, one can find opinions that these threats are not particularly significant, because in the area of civil systems, people cannot be physically harmed, harmed in health or harmed in life. This argumentation is not accurate. Attacks by hackers on some of the civilian IT systems may cause direct threats to the health and lives of people, e.g. in terms of air traffic control systems or systems controlling the course of telesurgical operations.

Chapter V of the dissertation contains an analysis of the level of digital competences of users, with particular emphasis on primary school students and teachers. Thanks to an in-depth exploration indicated area it was possible to develop a comparison with European countries. Different understandings of the concept of ‘digital competence’ in key national and international institutions and developed their own characterisation of the term. When analysing the division of digital competences, their ranges should be kept in mind (i.e., among other things, the ability to use software, digital problem-solving skills, digital content creation skills or online collaboration skills). or online collaboration skills).

The final element of the dissertation concerns deals with the key issue, from the point of view of this work, which is expert interviews and a survey. The dissertation concludes with a concept for changes, a conclusion and a list of bibliographies.

Keywords: cyber security, cyber threat, digital competences