mgr inż. Jolanta Cichosz
Uniwersytet Jana Kochanowskiego w Kielcach
Wydział Prawa, Administracji i Zarządzania

SUMMARY OF THE DOCTORAL DISSERTATION

"CYBERSECURITY POLICY OF THE REPUBLIC OF POLAND"

written under the guidance of prof. zw. dr. hab. Marian Kozub
assistant supervisor dr Adrian Mitręga

The cybersecurity has become an important area of research, discussion and debate in recent years. This is due to the fact that the development of countries is increasingly dependent on quick access to information and its secure processing. At the same time, the Internet has become a tool for affecting on the behavior of social groups and influencing the political and social sphere. However, each disruption in the functioning of cyberspace has an impact on the efficiency of public sector institutions, production and service processes, security of business transactions, a sense of security of citizens, and as a result understanding security, including international and national security. Moreover, the cross-border nature of cyber threats makes them difficult to counteract. Poland, like other countries, defines its own cyber security strategy in accordance with national priorities and EU legal regulations.

The aim of the research is to present ***the evaluation of cybersecurity policy and its impact on the national security of the Republic of Poland by the end of the third decade of the 21st century***.

The subject of research is ***the cybersecurity policy of the Republic of Poland from the beginning of the 1990s to the end of the third decade of the 21st century in the context of forecast changes and directions of evolution of the cybersecurity environment***.

The dissertation is interdisciplinary work and supplements the state of research on cybersecurity of the Republic of Poland. The analyzes presented in the doctoral dissertation cover the years 1990-2030. The year 1990 was established as the beginning of these considerations, because it concerns the initiated political, social and economic changes in Poland. During this period, the Polish state made efforts to join the structure of Western European computer networks. The time frame of this work closes 2030, thus referring to long-term strategies in Poland.

This dissertation uses various research methods due to the interdisciplinary nature of the study. Methodological holism was used to verify the hypothesis and achieve the set goal, combining methods from various scientific disciplines, including security, politics and

administration, law, IT, history and sociology. The author used the following research methods: analysis, abstraction, analogy, deduction, induction, historical and descriptive, normative (institutional and legal), comparative, progressive, segmentation, generalization and synthesis. Among the empirical methods, a diagnostic survey (expert interview) and participation in conferences, symposia and scientific seminars, as well as consultations on issues related to the topic of research work were used.

The research revealed that there is a need for extensive actions, as hacker attacks on Polish and EU entities have reached the level of several to several thousand incidents each year. Therefore, changes in technological conditions cause a different perception of threats in cyberspace and the functioning of services essential for the efficient operation of the state. Currently, our state is developing institutionalization as part of the cybersecurity policy, so there is a need to increase the level of specialization of employees (including law enforcement and judiciary) dealing with matters related to cybercrime, including the optimal use of training opportunities conducted by EU bodies in accordance with their mandates, in including: EC3 / Europol, ECTEG, Eurojust, OLAF and CEPOL.

This dissertation proved mainly that the constantly improved cybersecurity policy will significantly affect the stability of the national security of the Republic of Poland, the degree of democratization of public life, as well as the stability of the state in the local and global dimension. The basic issue of changes in cybersecurity policy, which has an impact on the security of the Republic of Poland by the end of the third decade of the 21st century, is the adjustment of strategic goals, tasks, measures, procedures and mechanisms adequate to the pace of development of new technologies and the creation of a digital single market. They will increase the cybersecurity potential of the state, support systemic education, research and implementation and cooperation between the public and private sectors - financial institutions, telecommunications companies, Internet service providers, NGOs, scientific, business, professional associations, etc., because their knowledge has significant added value for the effectiveness of actions to respond to cyber incidents or conducting preparatory proceedings related to cyber crime.

The most advanced forms of the cooperation with the private sector should be institutionalized by establishing appropriate state bodies or working groups. The research has also confirmed that the creation of a cybernetic army (units whose task is to constantly monitor Polish, and not only Polish cyberspace and respond to negative phenomena occurring in or affect Polish cyberspace) is necessary.

Therefore, evaluation of the cybersecurity policy of the Republic of Poland aims to

change into an area that allows ensuring national security in the perspective of the third decade of the 21st century.
Keywords: cybersecurity, cyber threats, cybersecurity policy of the Republic of Poland.