Cyber terrorism in the state security policy. Problems of critical infrastructure protection.

Summary

The fundamental problem of the research work is the attempt to answer the question what is the effect of cyber-terrorism and other asymmetrical threats to the development of legal regulations that protect the security of critical infrastructure in Poland. The scope of the study also includes an attempt to identify the most important problems of critical infrastructure protection against cyber threats.

The theoretical research methods, in particular the institutional and legal analysis, were used to achieve the set research goal. The previous state of legislation related to the protection of cyberspace security in strategic documents of the European Union (chapter II) has been reviewed, United States of America (Chapter III) and the Republic of Poland (Chapter IV), paying attention not only to strictly chronological relationships as part of the law-making process, but also to the functions of mutual influence. Significant emphasis was therefore placed especially on the analysis of the non-unification problem of both the phenomenon of cyberterrorism and the concept of critical infrastructure.

Chapter V analyzes the fact that the precise definition of critical infrastructure, although possible at the level of strategic documents created as a result of legislative procedures, is not always achievable and possible in theoretical and research approaches. Only taking into account the broad political context, social and economic environment of critical infrastructure allows for proper defining of critical infrastructure.

Chapter VI, which is an attempt to analyze the strategic assumptions of the protection of the critical infrastructure of the Republic of Poland, presents the most important legal acts regulating the procedures for the identification and protection of critical infrastructure in Poland. Due to the very extensive research material, the analyzed scope was narrowed down to national legislation as opposed to the broad approach previously adopted in the cyberspace security chapters, which also includes the US and the European Union. The adoption of this perspective made it possible to assess to what extent the creation of legal procedures for the protection of critical infrastructure against cyber threats has become one of the state's priorities, as well as to define the difficulties created by the necessity to implement this priority at the legislative level. The decision to subject the analysis of the most important legal acts regulating the procedures for

the identification and protection of critical infrastructure in Poland also resulted in the inclusion in the paper (in Chapter VII) of a detailed description of the critical infrastructure systems of the Republic of Poland.

The most important problems of legal protection of critical infrastructure in Poland include: the definition difficulties of the CI concept, the disadvantages of the adopted approach to the identification of critical infrastructure resources and ambiguities in the assessment of the criticality of individual system components. Security problems were also diagnosed as: incompatible provisions of the National Critical Infrastructure Protection Program with the applicable higher-level regulations, accepted approach to responsibility for the protection of CI systems, and the need to strengthen the legal protection of the power system, recognized as the most important of the critical infrastructure resources catalog.

Key words: cyber terrorism, cybercrime, critical infrastructure, terrorism, state security policy