

SUMMARY

The doctoral dissertation entitled “The role of open-source intelligence (OSINT) in ensuring the security of ICT systems and personal security” in the author’s intention concerned the identification and evaluation of the techniques used in the scope of open-source intelligence in order to gather the information about the construction and operation of an IT infrastructure as well as the information from a personal and business domain.

Within this dissertation, an analysis was performed to examine the possibility of using OSINT to protect IT infrastructure and to ensure both personal and business security, by an advance reconnaissance and the implementation of security measures protecting against using open-source intelligence as one of the methods and phases of an attack on organisational or personal safety.

The main reason for writing this Ph.D. thesis was the extremely limited current Polish academic literature on the topic of the matter of open-source intelligence itself, its basics, techniques, tools used, and most of all the methods for defending against the use of OSINT, performed by individuals or organisations, that may pose a threat to personal and business security.

The main research problem of the dissertation, according to the subject and the purpose of the research, is determined by the question: In what extent the available tools for gathering information during the open-source intelligence process and the techniques for analysing this information influence the security of ICT systems and personal security, and what are the abilities to defend against the identified techniques?

The dissertation, excluding the introduction and conclusion, consists of five substantive chapters: Chapter 1 Methodological assumptions; Chapter 2 The characteristics of open-source information gathering methods; Chapter 3 The analysis of information acquired from the Internet as the foundation of intelligence; Chapter 4 Using open-source intelligence in the scope of ICT systems security as well as personal and business security; Chapter 5 Security recommendations possible to use against open-source intelligence.

In the first chapter the subject and purpose of the dissertation, research problems and work hypotheses were discussed in detail. Research procedures, methods, techniques and tools were described.

In the second chapter methods for acquiring information from open sources were characterised, the scope and division of open-source intelligence were presented, and selected OSINT techniques were discussed.

The third chapter presents the characteristics of the intelligence cycle, the methods for the analysis of gathered information as well as it describes human reasoning patterns and cognitive biases, which may have a negative impact on performing proper open-source intelligence.

In the fourth chapter the threats were identified, which may result from open-source intelligence performed against individuals or whole organisations. Also, the possibilities of using OSINT for personal, business, and operational security were presented.

The fifth chapter describes the security measures, based on existing standards and other guidelines, including the OPSEC and PERSEC rules, possible to implement to defend against open-source intelligence techniques. Also, this chapter presents the security of the high value individuals in organisations.

The doctoral dissertation is a broad collection of content, related to open-source intelligence techniques and security measures basing on them. A thorough analysis of the subject literature enabled creating a compact and innovative work, that exhausts the main research problem.