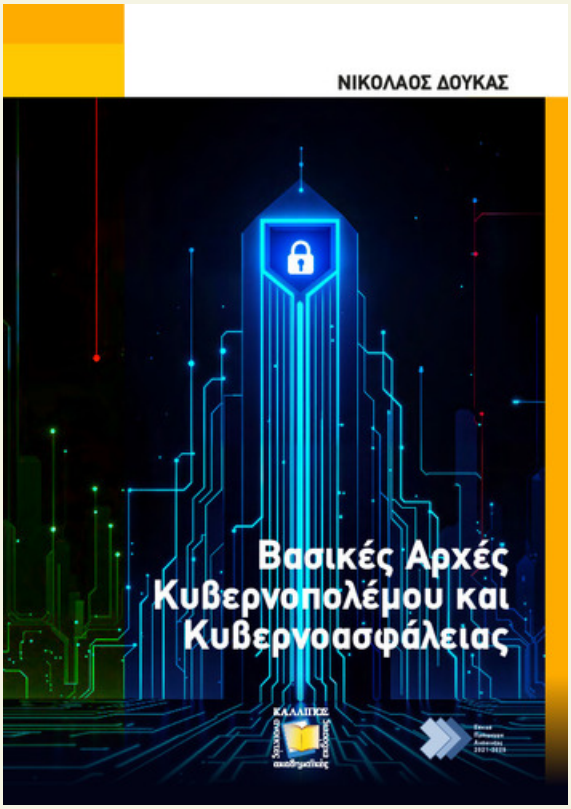

METADATA

Title: Fundamentals of Cyberwar and Cybersecurity

Other Titles: -

Language: Greek

Authors: Doukas, N., Associate Professor, Hellenic Army Academy

ISBN: 978-618-228-288-5

Subject: MATHEMATICS AND COMPUTER SCIENCE

Keywords: Cyberwar / Cyber-defense / Cyberattack / Information warfare / Error correction

Bibliographic Reference: Doukas, N. (2025). Fundamentals of Cyberwar and Cybersecurity [Postgraduate textbook]. Kallipos, Open Academic Editions. http://dx.doi.org/10.57713/kallipos-1043

Abstract

This book presents fundamental principles of information processing in the context of operations, as well as new scenarios that have been developed and are known as cyberwar. The first chapter covers fundamental principles of information theory. Error detection and correction schemes and cryptographic techniques for remote user authentication are outlined. The second chapter presents security requirements, threats, and vulnerabilities in information systems. In the third chapter, sensor technologies are presented for information acquisition. Visualization and information technologies are overviewed. The concept of simulation is analyzed, along with its applications. The C4ISR systems are introduced together with the digital battlefield. The fourth chapter presents cyberwar, the information field, and its relation to sovereignty. Additionally, network-centric, information, electronic and hybrid warfare are introduced. Cybercrime, cyberespionage, and defenses against cyberattacks are analyzed. The fifth chapter presents information system network technologies that will be used for the practical exercises given later. In the sixth chapter, these technologies are used to describe various kinds of cyberattacks, the methodology of cyber-intruders via the Cyber Kill Chain as well as network cryptography. The seventh chapter covers ethical and legal issues related to defending cyberspace. In the eighth chapter, a series of simple cybersecurity exercises is presented that include the creation of a simple virtual lab. In the ninth chapter, more complicated attacks are presented, such as the man-in-the-middle, WEP-Crack, mobile phone espionage and Denial of Service. The last chapter of the book analyzes the effects of cyberattacks in the physical world are explored and passive protection measures are analyzed. Dynamic detection techniques using anomalies are analyzed. Finally, the field of cyber forensics is introduced for the study of the effects of cybercrimes. A practical exercise on this domain is also presented that uses currently available software tools.

The Project is funded by the National Development Programme 2021-2025 of the Ministry of Education and Religious Affairs and implemented by the Special Account for Research Funds of the National Technical University of Athens and the Hellenic Academic Libraries Link.