Prof. Dr. Hüsamettin İNAÇ

Aymene HADJI

Introduction to Cyberspace and National Security

FİLİZ KİTABEVİ

İSTANBUL

2024

Aralık 2024

ISBN: 978-625-6134-91-1

Bu çalışma Kütahya Dumlupınar Üniversitesi Bilimsel Araştırma Projeleri Koordinasyon Birimi tarafından desteklenmiştir.

Proje numarası: 2024-59

Bu kitap, Kütahya Dumlupınar Üniversitesi'nin "100. Yılımızda 100 Kitap" projesinde listelenmektedir.

BASKI - CİLT

Filiz Kitabevi Basım Yayın Dağıtım
Petrol Ürünleri Sanayi ve Tic. Ltd. Şti.
Matbaacı Sertifika Numarası: 77398

YAYINLAYAN

Filiz Kitabevi Basım Yayın Dağıtım
Petrol Ürünleri Sanayi ve Tic. Ltd. Şti.
Cemal Yener Tosyalı Cad. No: 57/A (113)
Vefa-Fatih/İSTANBUL
Tel: (212) 527 0 718
(850)441 0 359
Faks: (212) 519 20 71

www.filizkitabevi.com
bilgi@filizkitabevi.com
Yayıncı Sertifika Numarası: 77398

Table of contents

Introduction

The rapid transformations in the post-Cold War world resulted in a number of new interactions at the international level, and the concept of national security was the most important concept affected by these new interactions and forces on the international scene. The electronic revolution that the world has witnessed has cast its shadow over countries in a remarkable way, and the challenge of achieving national security has become a major challenge for countries in varying degrees, as the standard of electronic control has become decisive in achieving national security in its new dimensions.

Information and communications technology has brought about a comprehensive revolution in all aspects of life. At the social level, it has had a major impact on society's behavior and identity, and the spread of networking mechanisms between human groups represented by social media, via computers and mobile phones, which has resulted in major changes in major social foundations. Such as privacy, culture, media, dating, and building social relationships.

In this context, research into the issues of cyber threats and security challenges requires delving into the aspects of the new digital age and describing the environment of these threats, as the Internet contains more than one billion and 700 million websites with a wide spread of innovations on the network, and in a report by the "Foundation Symantic" for the year 2018, it is estimated that more than 40 billion devices will be connected to the Internet, represented by smart cars and digital home appliances.

In connection with the issue of cyber threats, several reports and statistics indicate that 95% of major multinational companies admit that they have been exposed to piracy, as more than 135 governments in the world have taken firm measures regarding the virtual world and electronic security. Especially with the many cyber-attacks between countries, the most important of which are the mutual attacks between the United States of America on the one hand, and China, Russia, Iran, and North Korea on the other hand,Not to mention the increase in intellectual property theft and piracy of economic and commercial establishments, universities, research institutes and media institutions, in addition to the spread of cyber-terrorism networks that provide points of convergence and coordination between terrorist organizations and the exchange of information and expertise.

As such, the cybersecurity challenge can be considered the highest national security challenge in the twenty-first century, noting that the modern concept of security is not limited only to military aspects, Rather, it keeps pace with all the threats and challenges that could constitute a stumbling block to the digital economy and the flow of knowledge. Information and communications technology has eliminated the concept of geopolitical and cultural borders between countries, which puts national sovereignty at stake, especially with the hacking of official government websites and information spying on countries.

The cultural and intellectual challenge also emerges as one of the most important gateways to cyber threats, through intellectual invasion in social networks, spreading a culture of violence and exclusion, and incitement to crime under religious, sectarian, or sectarian pretexts. This is what calls for attention to electronic content based on spreading knowledge and introducing civilizations.

The future of information and communications technology will witness major cyber threats, and the Internet will turn into a large arena where fears of threats and attacks abound. These fears will also constitute investment opportunities for cyber security institutions, which requires dealing with cyber security issues with complete flexibility and proactive consideration.

The subject of the book falls within security and strategic studies, which emerged as a central field in international relations, especially after the end of the Cold War, and the new discussions it witnessed to expand the concept of security to include multiple issues and fields: political, economic, social, cultural, environmental, and cyber.

The importance of the issue lies in the steady escalation of attacks in cyberspace, which is expanding day after day, and the negative repercussions of these attacks.

Through this book, we aim to:

- Highlighting and clarifying new concepts in cyberspace and clarifying the relationship between cybersecurity and national security, the relationship of influence and being affected.
- Highlighting the contributions and efforts of countries, especially the United States of America, in confronting cyber threats.

The book seeks to provide an analytical vision of cyber threats and their impact on the national security of countries by clarifying security policies to confront these threats.

As we are interested in technological developments and are researchers in the field of strategy and international relations, through this book we will seek to enlighten the ordinary reader and researcher alike about the hidden danger that technology carries if it is used without taking strict security precautions, in addition to enriching the scientific and cognitive aspect.

In our digital age, the number and risks of cyber threats are increasing, and their effects and repercussions vary in the world in general, as these threats have extended to affect various sectors, whether military, political, economic, social and cultural, thus threatening the national security of countries. Accordingly, we pose the following central research question:

How do cyber threats affect the national security of countries?

The following sub-questions fall within the central research question:

- How has cyberspace affected concepts of security, power conflict, and war?
- What are the manifestations of cyber threats? What is its relationship to national security?
- What are the mechanisms used to address it?

Study hypotheses:

- There have been major changes in the concepts of security, power, conflict, and war due to the influence of cyberspace
- The more severe the cyber threats, the greater the threat to national security.
- Increased coordination and cooperation between countries in cyberspace reduces the risks of cyber threats.