
Contents

INTRODUCTION	vii
ACKNOWLEDGEMENT	x
CHAPTER 1. CYBERCRIME	1
1.1. The perpetrators of cybercrime	22
1.1.1. Motives of the perpetrators of cybercrime . . .	25
1.1.2. Types of offenders.	26
1.1.3. Organization of perpetrators	28
1.2. Tools for implementing attacks.	31
1.3. System protection against attacks.	32
1.4. Fear of cybercrime.	34
1.5. Investigation of cybercrime	37
1.6. Cost of cybercrime	39
1.6.1. Measuring the cost of cybercrime model	41
1.6.2. Cost framework for cybercrime model.	45
1.7. Laws and legal bodies	49
1.7.1. The Council of Europe Convention on Cybercrime.	49
1.7.2. Agreement on Trade-Related Aspects of Intellectual Property Rights.	52
1.7.3. Digital Millennium Copyright Act	53
1.7.4. United Nations Charter	54
1.8. Cybercrime conclusion	55

CHAPTER 2. CYBERWARFARE	57
2.1. Information and cyberspace	60
2.1.1. Cyberspace and ICT	60
2.1.2. Information power and information conflict	64
2.2. Understanding cyberwarfare	67
2.2.1. The nature of cyberwarfare	70
2.2.2. Types and techniques of cyberwarfare	72
2.3. Perpetrators and victims of cyberwarfare	80
2.4. Committing cyberwarfare	82
2.4.1. Espionage	82
2.4.2. Active warfare	85
2.4.3. Information operations	88
2.4.4. Propaganda activity	90
2.5. Organizations and cyberwarfare	95
2.5.1. Industrial espionage	98
2.5.2. Politically and ideologically motivated groups – perpetrators of cyberwarfare	103
2.6. The role of countries in cyberwarfare	107
2.6.1. The United States	108
2.6.2. China	113
2.6.3. Russia	117
2.6.4. India	119
2.6.5. Iran	121
2.6.6. Israel	121
2.6.7. North Korea	122
2.7. Efforts against cyberwarfare: international and national legislation	123
2.8. Defense against cyberwarfare	133
2.9. Cyberwarfare conclusion	139
CONCLUSION	141
BIBLIOGRAPHY	145
INDEX	163