# Cyber Terrorism: Politieal and Economic Implications

Andrew Michael Colarik

JCP=y

**IDEA GROUP PUBLISHING**

Hershey • London • Melbourne • Singapore

# Cyber Terrorism:

**Foreword** ..... **viii**

**Preface** ..... **xi**

**Chapter I**

**Introduction** ..... 1
*Objectives of This Chapter* ..... 1
*Terrorist Atrocities* ..... 2
*State Sponsors of Terror* ..... 3
*Frequency of Attacks* ..... 5
*The Role of Information and Technology* ..... 7
Network Approach by Terrorist Groups ..... 8
Main Issue and Problem: The Global Infonnation Infrastructure ..... 9
*Organization of This Book* ..... 11
*Final Thoughts of This Chapter* ..... 11

**Chapter II**

**The Power of Terrorism** ..... **14**
*Objectives of This Chapter* ..... 14
*What is Terrorism?* ..... 15
*Domestic* ..... 18
Intimidation ..... 19
Political Strife ..... 20
Economic Consequences ..... 22
*Global...:* ..... 23

Media Empowerment 23
Minority Solidarity 24
Extremist Subgroups 25
Subgroup Confederation 26
*Final Thoughts of This Chapter* 28

**Chapter ni**
**Cyber Terrorism Evolution 33**
*Objectives of This Chapter* 33
*Introduction* 34
*Bits and Chips* 36
*Hacking and Hacktivism* 37
*Crackers and Cracking* 40
*Cyber Criminals and Cyber Crime* 42
*Cyber Terrorism and Cyber Terrorists* 45
Communication, Coordination and Information Sharing 48
Activity Dissemination 50
Cyber Terrorist Tasks 51
*Final Thoughts of This Chapter* 52

**ChapterlV**
**GlobalInformation Infrastructure 58**
*Objectives of This Chapter* 58
*Introduction* 59
*Telephone System* 61
Landlines 62
Mobile 63
*Cable* 64
*Satellites* 65
*Internet* 68
*Security Services* 69
Authentication 70
AccessControl 70
Data Integrity and Confidentiality 71
Nonrepudiation 71
Auditing 72
Mechanisms and Protocols 72
*Final Thoughts of This Chapter* 76

Chapter V
Current Cyber Attack Methods ..... 82
*Objectives of This Chapter* ..... 82
*Introduction* ..... 83
*Internal Penetration* ..... 85
Usage Portals ..... 86
Deliverables ..... 91
*External Penetration* ..... 94
Social Engineering ..... 94
Physical ..... 95
Wireless Communication Medium ..... 96
User Access Points ..... 97
Firewalls ..... 99
Web Sites and Servers ..... 100
Routers and Gateways ..... 103
DomairiNaine Servers ..... 104
Audit Logs ..... 106
*Final Thoughts of This Chapter* ..... 107

Chapter VI
Attack Scenarios ..... Ill
*Objectives of This Chapter* ..... ill
*Introduction* ..... 112
*Target Intelligence* ..... 112
Histories ..... 113
Physical Layout ..... 114
EmergencyPlans ..... 115
Schedules ..... 116
Key Personnel ..... 116
*Electronic Attack Targets* ..... 118
Public and Private Utilities ..... 120
Banking and Finance ..... 124
Transportation ..... 128
Medical ..... 131
Education ..... 132
Government ..... 135
*Precursor to a Physical Attack* ..... 137
*Final Thoughts of This Chapter* ..... 139

**Chapter VII**
**Thoughts for the Future** 147
*Objectives of This Chapter* **147**
*Introduction* 148
" Key Issues to Be Considered 150
*Proposed Solutions* 154
Information as aProperty Right 155
GlobalInformation Security Center 156
AlterSoftwareLicensureAgreements 157
CreationofanUnderwritersLaboratoryofSecurityProducts ' 158
Law Enforcement Tiger Teams 160
Create the League of Cyber Communities 161
EliminationoftheOpenHandshake Protocol '.. 161
*Final Thoughts* 162

About **the Author** **166**

**Index** **168**