

Information Warfare

How to Survive Cyber Attacks

Michael Erbschloe

Osborne/McGraw-Hill

New York ▶ Chicago ▶ San Francisco ▶ Lisbon ▶ London ▶ Madrid ▶ Mexico City
Milan ▶ New Delhi ▶ San Juan ▶ Seoul ▶ Singapore ▶ Sydney ▶ Toronto

Contents

	<i>Foreword</i>	<i>xi</i>
	<i>Acknowledgments</i>	<i>xiii</i>
	<i>Introduction</i>	<i>xv</i>
Chapter 1	Information Warfare: A New Framework for Analysis	1
	Types of Information Warfare Strategies and Activities	3
	The Probability of Various Information Warfare Strategies Being Implemented	5
	The Anatomy of a National Information Warfare Defense Structure	9
	Putting International Treaties into Perspective	17
	The Military Side of Information Warfare	20
	Civilian Law Enforcement and Information Warfare	27
	The Impact of Information Warfare on Private Companies	29
	Information Warfare Will Result in Civilian Casualties	32
	Conclusions and an Agenda for Action	35
Chapter 2	Measuring the Economic Impact of Information Warfare	41
	The Nature of the Economic Impact of Information Warfare Attacks	43
	The Immediate Economic Impact of Information Warfare Attacks	46
	The Short-Term Economic Impact of Information Warfare Attacks	51
	The Long-Term Economic Impact of Disruption	57
	There Is No Day After in Cyberwar	61
	Conclusions and an Agenda for Action	62
Chapter 3	The Electronic Doomsday Scenario: How Ten People Could Cause \$1 Trillion in Economic Disruption	65
	The PH2 Team	66
	The Conception of PH2	68
	Day 1: The Launch of PH2	69

Day 2: The Big Bug Bite	70
Day 3: Is It War Yet?	71
Day 4: A Russian Connection?	72
Day 5: Chaos Realized.	72
Day 6: It Isn't Over Yet	72
Day 7: Attacks in Germany and Japan	73
Day 8: A German Bank Goes Down.	75
Day 9: Wall Street Denial-of-Service Attack.	75
Day 10: Middle East Conflict Brews, Wrong Number in Australia	76
Day 11: The Tiger Prowls	79
Day 12: Our Asian Daughters.	80
Day 13: Tonya Strikes	82
Day 14: The Shambles of Electronic Commerce	83
Day 15: Busy Signal in London.	84
Day 16: Target NASDAQ.	86
Day 17: PH2 Realized	87
Day 18: Stock Brokerage Take-Down	88
Day 19: NASDAQ Foiled, Microsoft Hit.	90
Day 20: Information Warfare, Guns, and Bombs.	92
Day 21: Vulnerability and Exposure	93
Day 22: Santa Claus Hits.	94
Day 23: Merry Christmas	94
The Aftermath of Information Warfare Attacks.	95
Chapter 4 Preparing to Fight Against Major Threats	97
Assessing the Preparedness for Information Warfare in the United States	99
Assessing the Preparedness for Information Warfare of Other Governments.	105
Assessing the Preparedness for Information Warfare of Terrorists and Criminals	107
Assessing the Preparedness for Information Warfare of Industry Groups	108
Traditional Diplomacy and Information Warfare	110
The Role of International Organizations	112
The Role of the Global Military Alliances	113
Martial Law and Cyberspace.	115
The Super Cyber Protection Agency.	117
Preparation from a Global Viewpoint	118
Conclusions and an Agenda for Action	119

Chapter 5	Information Warfare Strategies and Tactics from a Military Perspective	123
	The Context of Military Tactics	124
	Offensive and Defensive Ruinous Information Warfare Strategies and Tactics	125
	Offensive and Responsive Containment Information Warfare Strategies and Tactics	130
	Defensive Preventive Information Warfare Strategies and Tactics	135
	Random and Sustained Terrorist Information Warfare Strategies and Tactics	139
	Sustained and Random Rogue Information Warfare Strategies and Tactics	143
	Amateur Rogue Information Warfare Strategies and Tactics	146
	Conclusions and an Agenda for Action	147
Chapter 6	Information Warfare Strategies and Tactics from a Corporate Perspective	151
	Overview of Defensive Strategies for Private Companies ..	152
	Participating in Defensive Preventive Information Warfare Planning	154
	Surviving Offensive Ruinous and Containment Information Warfare Attacks	158
	Surviving Terrorist Information Warfare Attacks	162
	Countering Rogue Information Warfare Attacks	165
	Dealing with Amateur Rogue Information Warfare Attacks	168
	Conclusions and an Agenda for Action	171
Chapter 7	Strategies and Tactics from a Terrorist and Criminal Perspective	173
	Why Terrorists and Rogues Have an Advantage in Information Warfare	174
	The Future Computer-Literate Terrorist and Criminal	176
	Selecting Information Warfare Targets	177
	Targets that Appeal to Both Terrorists and Rogue Criminals	185
	Targets that Appeal to Terrorists, but Not Rogue Criminals	186

Targets that Appeal to Rogue Criminals,
but Not Terrorists 189

Working from the Inside of Information
Warfare Targets 190

Avoiding Pursuit and Capture 192

Fund Raising for Terrorist and Rogue Criminal
Information Warriors 193

Conclusions and an Agenda for Action 194

**Chapter 8 The Arms Dealers and Industrial Mobilization in
Information Warfare 197**

Mobilization Requirements for Technology
Companies in Information Warfare 198

The Top Technology Companies that Can Provide
Information Warfare Expertise 200

Aerospace and Defense Companies that Can Provide
Information Warfare Expertise 202

Computer System Manufacturers that Can Provide
Information Warfare Expertise 205

ZiLOG Computer Networking Product Companies
that Can Provide Information Warfare Expertise 208

Telecommunications Systems Companies that Can
Provide Information Warfare Expertise 209

Telecommunications Service Providers that Can
Provide Information Warfare Support 212

Software Producers that Can Provide Information
Warfare Expertise 217

Computer Services and Consulting Firms that
Can Provide Information Warfare Expertise 222

Internet Service Providers that Can Provide Support
to Information Warriors 224

Cooperation Between Governments and Technology
Companies in Information Warfare 225

Conclusions and an Agenda for Action 226

Chapter 9 Civilian Casualties in Information Warfare 229

Why the Cyber Masses Are at Risk 231

Circumstances with the Highest Potential Impact
for Individual Citizens 232

Conclusions and an Agenda for Action 234

Chapter 10	The New Terrorist Profile: The Curious Nerd Is Moving to the Dark Side	237
	The New Techno-Terrorists and Criminals	238
	Computer Crimes and Terrorist Attacks	242
	Where Information Warriors Will Come From	249
	Understanding Why People Become Cyberwarriors	252
	Motivations for Warriors in the New Frontier	254
	The Alienation of Computer Geeks	255
	Affinity Within the Pocket Protector Sect	256
	Why Cybercrime and Terrorism Can Be Fun and Profitable	257
	Will Americans Make Good Terrorists and Cyber Soldiers of Fortune?	261
	Gender, Race, and Nationality in Information Warfare Careers	262
	Conclusions and an Agenda for Action	264
Chapter 11	Law Enforcement: Being Behind the Technology Curve and How to Change That	267
	The Good Guys: Poorly Paid and Under-Trained	269
	Computers and Beyond: New Requirements for Cops and Special Agents	271
	The Challenge of Developing Cyber Cops	276
	Working for Big Brother: The New Information Highway Patrol	278
	Terrorist and Criminal Profiling in Cyberspace	280
	Conclusions and Agenda for Action	280
Chapter 12	Final Words for Policy Makers, Military Planners, and Corporate Executives	283
	Cutting Through the Rhetoric	284
	Funding National Defense	285
	Risk Management in the Corporate Environment	286
	Ecommerce and Information Warfare	286
	Closing Comments	287
	<i>Glossary</i>	289
	<i>Index</i>	299