

CONTENTS

Preface	ix
Acknowledgment.....	xi
Chapter 1 Introduction	1
National Cyber Threats, Vulnerabilities, and Attacks.....	4
Botnet Threat	6
National Cyber Security Methodology Components	9
Deception	11
Separation	13
Diversity	16
Consistency	17
Depth	19
Discretion	20
Collection	21
Correlation	23
Awareness	25
Response	26
Implementing the Principles Nationally	28
Chapter 2 Deception	31
Scanning Stage	35
Deliberately Open Ports	37
Discovery Stage.....	39
Deceptive Documents	41
Exploitation Stage	42
Procurement Tricks	45
Exposing Stage	46
Interfaces Between Humans and Computers	47
National Deception Program	49

Chapter 3 Separation	51
What Is Separation?	53
Functional Separation	55
National Infrastructure Firewalls	57
DDOS Filtering	60
SCADA Separation Architecture	62
Physical Separation	63
Insider Separation	65
Asset Separation	68
Multilevel Security (MLS)	70
 Chapter 4 Diversity	 73
Diversity and Worm Propagation	75
Desktop Computer System Diversity	77
Diversity Paradox of Cloud Computing	80
Network Technology Diversity	82
Physical Diversity	85
National Diversity Program	87
 Chapter 5 Commonality	 89
Meaningful Best Practices for Infrastructure Protection	92
Locally Relevant and Appropriate Security Policy	95
Culture of Security Protection	97
Infrastructure Simplification	99
Certification and Education	102
Career Path and Reward Structure	105
Responsible Past Security Practice	106
National Commonality Program	107
 Chapter 6 Depth	 109
Effectiveness of Depth	111
Layered Authentication	115
Layered E-Mail Virus and Spam Protection	119

Layered Access Controls	120
Layered Encryption	122
Layered Intrusion Detection	124
National Program of Depth	126
Chapter 7 Discretion	129
Trusted Computing Base	130
Security Through Obscurity	133
Information Sharing	135
Information Reconnaissance	137
Obscurity Layers	139
Organizational Compartments	141
National Discretion Program	143
Chapter 8 Collection	145
Collecting Network Data	148
Collecting System Data	150
Security Information and Event Management	154
Large-Scale Trending	156
Tracking a Worm	159
National Collection Program	161
Chapter 9 Correlation	163
Conventional Security Correlation Methods	167
Quality and Reliability Issues in Data Correlation	169
Correlating Data to Detect a Worm	170
Correlating Data to Detect a Botnet	172
Large-Scale Correlation Process	174
National Correlation Program	176
Chapter 10 Awareness	179
Detecting Infrastructure Attacks	183
Managing Vulnerability Information	184

Cyber Security Intelligence Reports	186
Risk Management Process	188
Security Operations Centers	190
National Awareness Program	192
Chapter 11 Response	193
Pre- Versus Post-Attack Response	195
Indications and Warning	197
Incident Response Teams	198
Forensic Analysis	201
Law Enforcement Issues	203
Disaster Recovery	204
National Response Program	206
Appendix Sample National Infrastructure Protection	
Requirements	207
Sample Deception Requirements (Chapter 2)	208
Sample Separation Requirements (Chapter 3)	209
Sample Diversity Requirements (Chapter 4)	211
Sample Commonality Requirements (Chapter 5)	212
Sample Depth Requirements (Chapter 6)	213
Sample Discretion Requirements (Chapter 7)	214
Sample Collection Requirements (Chapter 8)	214
Sample Correlation Requirements (Chapter 9)	215
Sample Awareness Requirements (Chapter 10)	216
Sample Response Requirements (Chapter 11)	216
Index	219