Contents

1 Introduction 1

1.1 Summary 3

2 Bridging the Classical D&D and Cyber Security Domains 5

2.1 Classical D&D 5

2.1.1 Reveal Facts 7

2.1.2 Reveal Fictions—Simulation 7

2.1.3 Conceal Facts—Dissimulation 8

2.1.4 Conceal Fictions 9

2.1.5 Deception Dynamics 11

2.2 Translating D&D to Cyber Security 14

2.3 Using D&D in Cyber Security 17

2.3.1 Reveal Facts 17

2.3.2 Conceal Facts 18

2.3.3 Reveal Fictions 20

2.3.4 Conceal Fictions 23

2.4 D&D Operations 24

3 Intrusions, Deception, and Campaigns 31

3.1 Intrusion Attempts 32

3.2 Cyber Kill Chain 33

3.2.1 Reconnaissance 36

3.2.2 Weaponization 37

3.2.3 Delivery 38

3.2.4 Exploit 39

3.2.5 Control 40

3.2.6 Execute 40

3.2.7 Maintain 42

3.2.8 Recursive Cyber Kill Chain 42

3.3 Deception Chain 43

3.3.1 Purpose 44

3.3.2 Collect Intelligence 44

3.3.3 Design Cover Story 45
3.3.4 Plan 46
3.3.5 Prepare 46
3.3.6 Execute 47
3.3.7 Monitor 47
3.3.8 Reinforce 47
3.3.9 Recursive Deception Chain 48
3.4 Intrusion Campaigns 49

4 Cyber-D&D Case Studies 53
4.1 The Stuxnet Campaign 53
4.1.1 Tactical Cyber-D&D 56
4.1.2 Operational Cyber-D&D 58
4.1.3 Strategic Cyber-D&D 60
4.1.4 Benefits of Stuxnet Cyber-D&D 62
4.1.5 Challenges of Stuxnet Cyber-D&D 62
4.2 APT Espionage 64
4.2.1 Assumptions 65
4.2.2 Reconnaissance Phase 66
4.2.3 Weaponization Phase 69
4.2.4 Delivery Phase 72
4.2.5 Exploit Phase 75
4.2.6 Control/Execute Phase 77
4.2.7 Maintain Phase 80

5 Exercising Cyber-D&D 83
5.1 Incorporating D&D in Red/Blue Team Exercises 83
5.2 Example: SLX II Exercise Parameters 86
5.3 Example: SLX II Exercise Design 87
5.4 Example: SLX II Exercise Red/Blue Interplay 89
5.5 Example: SLX II Exercise Results 91

6 Considerations, Adaptation, and Sharing 93
6.1 Risk, Unintended Consequences, Compromise, and Failure 94
6.2 Benefits, Challenges, and Drawbacks of Cyber-D&D 97
6.3 Post Exploit Manhunting 102
6.3.1 Elements Underlying Hunter Strategies 103
6.3.2 Hunter Strategies 104
6.3.3 PONI Strategies 105
6.4 Standardization and Sharing 106

7 Countering Denial and Deception 109
7.1 Defining Counterdeception 109
7.2 Defining Counter-Deception 111
7.3 Applying Cyber-CD to Computer Intrusions 112
7.3.1 Building a Tripwire 112
7.3.2 Sharing Intrusion Data 113
7.4 Counterdeception Components 114

7.5 Applying Cyber-CD to Network Defense 118
7.6 A Cyber-CD Process Model 119
7.6.1 Case Study 123

8 Capability Maturity Model 127
8.1 Cyber-D&D Maturity Model Framework 128
8.2 People-CMM 132
8.3 Services-CMM 140
8.3.1 Service Processes 140
8.3.2 Maturity Levels of Delivery of Cyber-D&D Services 141
8.4 Processes-CMM 145
8.5 Technologies and Techniques-CMM 147
8.5.1 General Characteristics of Technology Maturity Levels 147
8.5.2 Specific Technology Maturity Attributes in the Context of Cyber-D&D 148
8.6 Implications 157

9 Cyber-D&D Lifecycle Management 159
9.1 Overview of Spiral D&D Lifecycle Management 160
9.2 Plan 160
9.3 Implement 163
9.4 Deploy and Execute 164
9.5 Post-deployment Analysis 165

10 Looking to the Future 167
10.1 Live Defensive Operations 167
10.2 Vulnerability Assessment 168
10.3 Game Theory Models 168
10.4 Cyber-Deception Education and Training 169
10.5 Chinese Cyber-Deception Research 170
10.6 Immune System and Biological Models 170
10.7 Cyber-Counterdeception Capability Maturity Model 171
10.8 Cyber-Counterdeception in Active Defense 172
10.9 Moving Forward 174

Appendix A: Cyber-D&D Taxonomy 175

Appendix B: False Virtual Persona Checklists 201

Appendix C: Deception Maxims Applied to Defensive Cyber-D&D 213

Appendix D: Strategic Denial & Deception Capabilities 221

Appendix E: Definitions 227

References 245

Springer

http://www.springer.com/978-3-319-25131-8

Cyber Denial, Deception and Counter Deception
A Framework for Supporting Active Cyber Defense
Heckman, K.E.; Stech, F.J.; Thomas, R.K.; Schmoker, B.;
Tsow, A.W.

2015, XV, 251 p. 30 illus., 28 illus. in color., Hardcover
ISBN: 978-3-319-25131-8