Contents

1 Introduction **1**

1.1 Motivation . . . 1

1.2 Goals and contributions . . . 2

1.3 Thesis outline . . . 4

1.4 Background and state of the art . . . 5

1.4.1 Information Operations . . . 5

1.4.2 Cyberspace Operations . . . 7

1.4.3 Intelligence . . . 8

1.4.4 Cyber intelligence . . . 13

1.4.5 Threat modeling . . . 17

1.4.6 Threat actors' categorization . . . 19

1.4.7 Threat actors' characterization . . . 22

1.4.8 Threat actors' detection . . . 26

2 A Taxonomy for Threat Actors' Delivery Techniques **33**

2.1 Introduction . . . 34

2.2 Background . . . 35

2.2.1 Mitre ATT&CK . . . 35

2.2.2 Cyber Kill Chain ® . . . 37

2.3 Problem Statement . . . 38

2.4 Techniques and Limitations . . . 39

2.5 Our Proposal . . . 44

2.5.1 Mapping to MITRE ATT&CK . . . 50

2.5.2 A Practical Example . . . 55

2.6 Discussion . . . 58

2.7 Conclusions . . . 59

3 A Taxonomy for Threat Actors' Persistence Techniques **61**

3.1 Introduction . . . 62

3.2 Background . . . 63

3.3 Problem statement . . . 64

3.4 Approaches and limitations . . . 65

3.5 Our proposal . . . 69

3.5.1 Pre–OS persistence . . . 70

3.5.2 OS native persistence 72
3.5.3 Server software persistence 76
3.5.4 User dependent persistence 77
3.5.5 Summary 79
3.6 Discussion 80
3.7 Conclusions 87

4 CNA tactics and techniques: a structure proposal 89
4.1 Introduction 90
4.2 Background 92
4.2.1 Computer Network Attack 92
4.2.2 MITRE ATT&CK 93
4.3 The issue 94
4.4 Approaches and limitations 95
4.5 Proposed Approach: A Novel CNA Tactics Taxonomy 99
4.5.1 Degradation 101
4.5.2 Destruction 104
4.5.3 Manipulation 106
4.5.4 Summary 107
4.5.5 Mapping to MITRE ATT&CK 108
4.5.6 Practical Example 113
4.6 Discussion 115
4.7 Conclusions 116

5 SOC Critical Path: a defensive kill–chain approach 119
5.1 Introduction 120
5.2 Background 122
5.2.1 SOC concepts 122
5.2.2 Kill chain models 124
5.3 The Issue: A Lack of Defensive Kill Chain 125
5.4 Techniques and limitations 127
5.5 Our proposal 130
5.5.1 A practical example 133
5.6 Discussion 136
5.7 Conclusions 137

6 Key Requirements for the Detection and Sharing of Behavioral Indicators of Compromise 139
6.1 Introduction 140
6.2 Background 141
6.2.1 Indicators of compromise 141
6.2.2 Intelligence cycle 143
6.3 The issue 145
6.3.1 Threat specification 145
6.3.2 Real–world IOC 146
6.4 Approaches and limitations 147

6.5 Key requirements for behavioral IOC detection and sharing 150
6.5.1 Acquisition 153
6.5.2 Processing 154
6.5.3 Analysis 155
6.5.4 Dissemination 156
6.5.5 A practical example 157
6.6 Discussion 160
6.7 Conclusions 161

7 Discussion 163
7.1 Advanced Threat Actors in cyberspace 163
7.2 Categorization of Advanced Threat Actors 165
7.2.1 Motivation of Advanced Threat Actors 166
7.2.2 Nation–state actors 169
7.2.3 Non–state actors 171
7.2.4 Critical infrastructures 172
7.3 Characterization of Advanced Threat Actors 173
7.3.1 Low level observables 175
7.3.2 Tactics, techniques and procedures 177
7.3.3 Goals and strategy 179
7.3.4 Attribution 180
7.4 Detection of Advanced Threat Actors 181
7.4.1 The role of intelligence 182
7.4.2 Indicators of Compromise 185
7.4.3 The detection process 187

8 Conclusions 191

A Acronyms 195

Bibliography 199