
Contents

Introduction	ix
Daniel VENTRE, Hugo LOISEAU and Hartmut ADEN!	
Chapter 1. The “Science” of Cybersecurity in the Human and Social Sciences: Issues and Reflections	1
Hugo LOISEAU!	
1.1. Introduction.	1
1.2. A method?	4
1.3. Data?.	11
1.4. One or more definition(s)?	16
1.5. Conclusion	20
1.6. References	21
Chapter 2. Definitions, Typologies, Taxonomies and Ontologies of Cybersecurity	25
Daniel VENTRE!	
2.1. Introduction.	25
2.2. Definition	27
2.2.1. What is a definition?	27
2.2.2. Usefulness of definitions	29
2.2.3. Rules for constructing definitions	29
2.2.4. Definitions of cybersecurity.	32
2.3. Typology	43
2.3.1. What is a typology?	44
2.3.2. Usefulness of typologies.	44
2.3.3. Rules for the construction of typologies	45
2.3.4. Cybersecurity typologies	46

2.4. Taxonomy.	48
2.4.1. What is a taxonomy?	48
2.4.2. Usefulness of taxonomy	49
2.4.3. Rules for the construction of taxonomies	49
2.4.4. Taxonomies of cybersecurity	50
2.5. Ontologies	51
2.5.1. What is ontology?	52
2.5.2. Usefulness of ontologies.	53
2.5.3. Rules for construction of ontologies	53
2.5.4. Cybersecurity ontologies	54
2.6. Conclusion	56
2.7. References	57
Chapter 3. Cybersecurity and Data Protection – Research Strategies and Limitations in a Legal and Public Policy Perspective	67
Hartmut ADEN!	
3.1. Introduction.	67
3.2. Studying the complex relationship between cybersecurity and data protection: endangering privacy by combating cybercrime?	68
3.2.1. Potential tensions between cybersecurity and data protection.	69
3.2.2. Potential synergies between cybersecurity and data protection	72
3.3. Methodological approaches and challenges for the study of cybersecurity – legal and public policy perspectives	74
3.3.1. Legal interpretation and comparison as methodological approaches to the study of cybersecurity	74
3.3.2. Public policy approaches to the study of cybersecurity.	77
3.3.3. Transdisciplinary synergies between legal and public policy perspectives	78
3.4. Conclusion and outlook.	80
3.5. References	81
Chapter 4. Researching State-sponsored Cyber-espionage	85
Joseph FITSANAKIS!	
4.1. Defining cybersecurity and cyber-espionage	85
4.2. Taxonomies of cyber-threats.	87
4.3. The structure of this chapter	88
4.4. The significance of state-sponsored cyber-espionage	90
4.5. Research themes in state-sponsored cyber-espionage	94
4.6. Theorizing state-sponsored cyber-espionage in the social sciences	98
4.7. Research methodologies into state-sponsored cyber-espionage	104

4.8. Intellectual precision and objectivity in state-sponsored cyber-espionage research	106
4.9. Detecting state actors in cyber-espionage research.	110
4.10. Identifying specific state actors in cyber-espionage research.	112
4.11. Conclusion: researching a transformational subject	116
4.12. References.	118

Chapter 5. Moving from Uncertainty to Risk: The Case of Cyber Risk ! 123!

Michel DACOROGNA and Marie KRATZ!

5.1. Introduction.	123
5.2. The scientific approach to move from uncertainty to risk.	124
5.3. Learning about the data: the exploratory phase.	126
5.4. Data cleansing	128
5.5. Statistical exploration on the various variables of the dataset	130
5.6. Univariate modeling for the relevant variables	134
5.7. Multivariate and dynamic modeling	139
5.7.1. A fast-changing environment: time dependency.	140
5.7.2. Causal relations	143
5.7.3. Models for prediction	147
5.8. Conclusion	149
5.9. Acknowledgments.	151
5.10. References.	151

Chapter 6. Qualitative Document Analysis for Cybersecurity and Information Warfare Research 153

Brett VAN NIEKERK and Trishana RAMLUKAN!

6.1. Introduction.	153
6.1.1. Previous research	154
6.2. Information warfare and cybersecurity.	154
6.3. Researching information warfare and cybersecurity.	156
6.4. Qualitative research methodologies for information warfare and cybersecurity	157
6.4.1. Clustering of documents.	159
6.4.2. Clustering of words.	159
6.4.3. Word frequencies and word clouds	159
6.4.4. Text search and word trees	159
6.4.5. Example use cases of qualitative document analysis	160
6.5. An analysis of national cybersecurity strategies	161
6.5.1. Selection process for the documents.	161
6.5.2. Analysis	162

6.5.3. Discussion	167
6.6. An analysis of the alignment of South Africa’s Cybercrimes Bill to international legislation	169
6.6.1. Background to the documents	169
6.6.2. Analysis	170
6.6.3. Discussion	174
6.7. An analysis of the influence of classical military philosophy on seminal information warfare texts	176
6.8. Reflections on qualitative document analysis for information warfare and cybersecurity research	177
6.9. Conclusion	179
6.10. References.	180
Chapter 7. Anti-feminist Cyber-violence as a Risk Factor: Analysis of Cybersecurity Issues for Feminist Activists in France	185
Elena WALDISPUEHL!	
7.1. Introduction.	185
7.2. Localization of an online field.	187
7.2.1. Online ethnographic work and empathy	192
7.2.2. Cybersecurity issues of an online field	193
7.3. Online–offline continuum	194
7.4. Continuum between security and insecurity.	199
7.5. Conclusion	204
7.6. References	205
List of Authors	211
Index	213