

Table des matières

Introduction	1
Daniel VENTRE, Hugo LOISEAU et Hartmut ADEN	
Chapitre 1. La « science » de la cybersécurité en sciences humaines et sociales : problèmes et réflexions	7
Hugo LOISEAU	
1.1. Introduction	7
1.2. Une méthode ?	10
1.3. Des données ?	17
1.4. Une ou des définitions ?	22
1.5. Conclusion	26
1.6. Bibliographie	27
Chapitre 2. Définitions, typologies, taxonomies et ontologies de la cybersécurité	31
Daniel VENTRE	
2.1. Introduction	31
2.2. Les définitions	33
2.2.1. Objet des définitions	33
2.2.2. Utilité des définitions	35
2.2.3. Règles de construction des définitions	35
2.2.4. Définitions de la cybersécurité	38
2.3. Les typologies	50

2.3.1. Définition des typologies	51
2.3.2. Utilité des typologies	51
2.3.3. Règles de construction des typologies	51
2.3.4. Typologies de la cybersécurité	52
2.4. Les taxonomies.	55
2.4.1. Définition des taxonomies	55
2.4.2. Utilité des taxonomies	56
2.4.3. Règles de construction des taxonomies	56
2.4.4. Taxonomies de la cybersécurité	56
2.5. Les ontologies	59
2.5.1. Définition des ontologies	59
2.5.2. Utilité des ontologies	60
2.5.3. Règles de construction des ontologies	60
2.5.4. Ontologies de la cybersécurité	61
2.6. Conclusion	63
2.7. Bibliographie	64

Chapitre 3. Cybersécurité et protection des données : stratégies de recherche et limites dans une perspective juridique et de politique publique 75

Hartmut ADEN

3.1. Introduction.	75
3.2. Étudier la relation complexe entre la cybersécurité et la protection des données : mettre en danger la vie privée en luttant contre la cybercriminalité ?	76
3.2.1. Tensions potentielles entre la cybersécurité et la protection des données	77
3.2.2. Synergies potentielles entre la cybersécurité et la protection des données	81
3.3. Approches méthodologiques et défis pour l'étude de la cybersécurité – perspectives juridiques et de politique publique	82
3.3.1. Interprétation et comparaison juridiques comme approches méthodologiques pour l'étude de la cybersécurité	83
3.3.2. Approches de politique publique pour l'étude de la cybersécurité	85
3.3.3. Synergies transdisciplinaires entre les perspectives juridiques et de politique publique	87
3.4. Conclusion et perspectives	89
3.5. Bibliographie	90

Chapitre 4. La recherche sur le cyberespionnage commandité par l'État	93
Joseph FITSANAKIS	
4.1. Définition de la cybersécurité et du cyberespionnage	93
4.2. Taxonomies des cybermenaces	95
4.3. Structure du chapitre	96
4.4. Importance du cyberespionnage commandité par l'État.	98
4.5. Thèmes de recherche dans le domaine du cyberespionnage commandité par l'État	102
4.6. Théorisation du cyberespionnage commandité par l'État dans le domaine des sciences sociales	106
4.7. Méthodes de recherche sur le cyberespionnage commandité par l'État	111
4.8. Précision intellectuelle et objectivité dans la recherche sur le cyberespionnage commandité par l'État	114
4.9. Détecter les acteurs étatiques dans la recherche sur le cyberespionnage	118
4.10. Identifier les acteurs étatiques spécifiques dans la recherche sur le cyberespionnage	120
4.11. Conclusion : la recherche d'un sujet transformationnel	124
4.12. Bibliographie	126
Chapitre 5. Analyse qualitative de documents pour la recherche sur la cybersécurité et la guerre de l'information	131
Brett VAN NIEKERK et Trishana RAMLUKAN	
5.1. Introduction.	131
5.1.1. Recherches antérieures.	132
5.2. Guerre de l'information et cybersécurité.	132
5.3. Recherche sur la guerre de l'information et la cybersécurité	134
5.4. Méthodologies de recherche qualitative sur la guerre de l'information et la cybersécurité.	135
5.4.1. <i>Clustering</i> des documents	137
5.4.2. <i>Clustering</i> des termes	137
5.4.3. Fréquences de mots et nuages de mots	137
5.4.4. Recherche de texte et arbres de mots	137
5.4.5. Exemples de cas d'utilisation de l'analyse qualitative de documents	138
5.5. Une analyse des stratégies nationales de cybersécurité	139
5.5.1. Processus de sélection des documents	139

5.5.2. Analyse	140
5.5.3. Discussion	145
5.6. Une analyse de l’alignement de la loi sud-africaine sur la cybercriminalité sur la législation internationale	147
5.6.1. Contexte des documents	147
5.6.2. Analyse	148
5.6.3. Discussion	152
5.7. Une analyse de l’influence de la philosophie militaire classique sur les textes fondateurs de la guerre de l’information	154
5.8. Réflexions sur l’analyse qualitative des documents pour la recherche sur la guerre de l’information et la cybersécurité	156
5.9. Conclusion	157
5.10. Bibliographie	158

**Chapitre 6. Les cyberviolences antiféministes comme dispositif
d’insécurité : analyse des enjeux de cybersécurité
des activistes féministes en France 163**

Elena WALDISPUEHL

6.1. Introduction.	163
6.2. Localisation d’un terrain en ligne	165
6.2.1. Travail ethnographique en ligne et empathie	170
6.2.2. Enjeux de cybersécurité d’un terrain en ligne	171
6.3. <i>Continuum</i> en ligne et hors ligne	172
6.4. <i>Continuum</i> entre sécurité et insécurité	177
6.5. Conclusion	182
6.6. Bibliographie.	183

Liste des auteurs 189

Index 191