

Table des matières

Introduction	1
Daniel VENTRE et Hugo LOISEAU	
Chapitre 1. Évolutions du cybercrime durant la crise de la Covid-19.	21
Daniel VENTRE	
1.1. Introduction.	21
1.2. Observer l'évolution de la cybercriminalité.	25
1.2.1. Exploiter des données annuelles : le cas de l'Inde.	28
1.2.2. Exploiter des données mensuelles	31
1.2.2.1. Le cas de la Malaisie.	31
1.2.2.2. Le cas du Brésil.	38
1.2.3. Exploiter des données hebdomadaires : le cas de la Chine.	41
1.3. Observer l'évolution de la géographie mondiale des cyberattaques.	48
1.4. Conclusion	54
1.5. Annexes	58
1.5.1. Des outils du cybercrime : les <i>malwares</i>	58
1.5.2. Les CVSS comme indicateurs du niveau des vulnérabilités	59
1.5.3. Hétérogénéité et complexité des typologies du cybercrime	60
1.5.4. Attitude des entreprises face aux risques cyber : le cas du Royaume-Uni	65
1.6. Bibliographie.	65

Chapitre 2. La crise pandémique de SARS-CoV-2 et l'évolution de la cybercriminalité aux États-Unis et au Canada 69

Hugo LOISEAU

2.1. Introduction 69

2.2. Les impacts de la pandémie du SARS-CoV-2 70

2.3. Cybercriminalité et SARS-CoV-2 72

 2.3.1. Cibles et victimes 73

 2.3.2. Acteurs malveillants 76

 2.3.3. Le cyberspace, un environnement propice à la cybercriminalité. 78

2.4. L'évolution du cybercrime en Amérique du Nord durant la pandémie 80

 2.4.1. Le cas des États-Unis. 81

 2.4.2. Le cas du Canada 88

2.5. Discussion 90

2.6. Conclusion 93

2.7. Remerciements. 94

2.8. Bibliographie. 95

Chapitre 3. Radicalisation en ligne et cybercriminalité : le militantisme américain pendant la Covid-19 101

Joseph FITSANAKIS et Alexa MCMICHAEL

3.1. Introduction 101

3.2. Une nouvelle typologie de la cybercriminalité 102

3.3. Connectivité internet et militantisme violent 105

3.4. Le paysage des menaces nationales avant la pandémie 106

3.5. Le paysage de la menace pandémique domestique. 108

3.6. Accélérationnisme pandémique 111

3.7. De la criminalité virtuelle à la criminalité réelle 112

3.8. Radicalisation en ligne pendant la Covid-19 114

3.9. Un nouveau paradigme méthodologique pour la radicalisation en ligne ? 118

3.10. Conclusion 119

3.11. Bibliographie 121

Chapitre 4. Cybercriminalité au Brésil : évaluation des politiques post-Covid de coopération internationale en matière d'enquêtes et de poursuites 129

Alexandre VERONESE et Bruno CALABRICH

4.1. Introduction. 129

4.2. La cybercriminalité dans la littérature et le cas brésilien 132

4.3. Un modèle théorique de coopération internationale	135
4.4. L'évolution de la cybercriminalité au Brésil	139
4.5. L'évolution du système juridique brésilien concernant la cybercriminalité et son lien avec le régime international	146
4.6. Gérer la coopération internationale sans disposer des meilleurs outils . .	154
4.7. Difficultés à coopérer : joints, mortaises et encoches	158
4.8. Conclusion	161
4.9. Annexe : liste des entretiens et des questions	163
4.10. Bibliographie	163

Chapitre 5. Impacts de la crise de Covid-19 sur la peur et la victimisation liées au vol d'identité en ligne au Portugal . . . 169

Inês GUEDES, Joana MARTINS, Samuel MOREIRA et Carla CARDOSO

5.1. Introduction.	169
5.2. L'impact de la pandémie Covid-19 sur la cybercriminalité.	170
5.3. Évolution de la cybercriminalité au Portugal	173
5.4. Vol d'identité en ligne (VIL)	175
5.4.1. Définition et <i>modus operandi</i>	175
5.4.2. La théorie des activités routinières (TAR) appliquée au cyberspace	176
5.4.2.1. Théorie des activités routinières et cybercriminalité	177
5.4.3. Variables individuelles et victimisation par le vol d'identité en ligne.	179
5.5. Peur de la criminalité en ligne.	180
5.5.1. Déterminants de la peur du crime en ligne	180
5.6. La présente étude	182
5.6.1. Instruments de mesure	182
5.6.2. Résultats	185
5.6.3. Variables associées à la victimisation en ligne et à la peur du vol d'identité.	189
5.7. Conclusion	190
5.8. Bibliographie	191

Chapitre 6. Une perspective sud-africaine sur la cybercriminalité pendant la pandémie 197

Brett VAN NIEKERK, Trishana RAMLUKAN et Anna COLLARD

6.1. Introduction.	197
6.1.1. Contexte de l'Afrique du Sud et de la pandémie.	198
6.1.2. Méthodologie	199
6.2. Classements internationaux	200

6.3. Cybercriminalité et législation connexe	203
6.4. Incidents de cybersécurité	205
6.4.1. Rançongiciel	205
6.4.2. Escroqueries et fraudes.	207
6.4.3. Intrusions dans les systèmes et violations de données	209
6.4.4. Désinformation et communications malveillantes.	211
6.4.5. Autres.	215
6.5. Discussion	216
6.6. Conclusion	218
6.7. Bibliographie.	218
Liste des auteurs.	229
Index	231