

Table des matières

Introduction. Étudier le cyberspace à l'international	1
Sébastien-Yves LAURENT	
Chapitre 1. Les États-Unis, les États et les faux-semblants de la fin de l'internet mondial	5
Sébastien-Yves LAURENT	
1.1. Introduction.	5
1.2. La création de l'internet et le développement du cyberspace par les États-Unis	6
1.2.1. Les premiers systèmes de télécommunications internationaux développés par l'ensemble des États	7
1.2.2. La création et le développement de l'internet par les États-Unis	7
1.2.3. Une gestion internationale contrôlée par les États-Unis	8
1.2.4. Un système sociotechnique porteur d'une idéologie composite d'origine étatsunienne	13
1.2.5. La fausse recomposition du système sociotechnique mondial : les sommets mondiaux sur la société de l'information	14
1.3. Un cyberspace transformé sous l'effet de l'arrivée en force des États	16
1.3.1. Les intentions des États dans les « stratégies nationales » : des discours marqués par l'approche globale	17
1.3.2. Les désaccords structurels russo-américains sur la sécurité de l'information et sur la cybersécurité	19
1.3.3. Les discussions sur la cybersécurité : la restauration internationale symbolique de l'État coercitif.	21

1.4. Praxis de la coercition d'État dans le cyberspace	23
1.4.1. Les activités de renseignement et de surveillance dans l'environnement numérique	24
1.4.2. Des opérations cyber non militaires	27
1.4.3. Conflits numériques interétatiques, secret et diplomatie coercitive	29
1.5. La fragmentation de l'internet mondial et la souveraineté numérique des États	32
1.5.1. La balkanisation linguistique : Babel numérique	32
1.5.2. La fragmentation politique : des internets alternatifs	34
1.6. La forte contrainte de coopération interétatique pour l'ensemble des États	36
1.6.1. Des accords interétatiques sur un embryon de droit international	36
1.6.2. La dépendance des États à la coopération internationale pour la cybersécurité	37
1.7. Conclusion	38
1.8. Bibliographie	38

Chapitre 2. De la cybersécurité en Amérique : l'appareil de sécurité nationale étatsunien face à la gestion de la cyberconflictualité

45

Frédéric GAGNON et Alexis RAPIN

2.1. Introduction.	45
2.2. Dynamiques sociétales et institutionnelles	47
2.3. Dynamiques organisationnelles et bureaucratiques	51
2.4. Dynamiques individuelles	55
2.5. Conclusion	59
2.6. Bibliographie.	60

Chapitre 3. Séparation des fonctions offensive et défensive : l'originalité du modèle de cyberdéfense française remis en cause ?

65

Alix DESFORGES

3.1. Introduction.	65
3.2. Un modèle pensé et élaboré en réaction aux menaces et enjeux du début des années 2010	68

3.2.1. Un modèle d'organisation reposant en apparence sur deux acteurs principaux	68
3.2.1.1. Un acteur défensif : l'Agence nationale de sécurité des systèmes d'information	68
3.2.1.2. Un acteur défensif et offensif dans les opérations militaires : le ministère de la Défense (hors services de renseignement)	70
3.2.1.3. Les services de renseignement : acteur discret mais fondamental du dispositif français en matière offensive.	70
3.2.2. Le choix assumé d'une séparation stricte offensif/défensif	72
3.2.2.1. Un modèle en opposition aux ambiguïtés du modèle anglo-saxon	72
3.2.2.2. Un modèle pour construire de la confiance, en particulier vis-à-vis du secteur privé	74
3.3. Une séparation stricte des fonctions et missions offensives et défensives : obstacle à une meilleure défense ?	77
3.3.1. Un contexte en forte évolution : une menace de plus en plus importante issue des États les plus avancés	78
3.3.2. Des limites devenues des entraves pour assurer les missions de la cyberdéfense	79
3.3.2.1. Prévenir, anticiper, protéger et détecter.	80
3.3.2.2. Une nécessité pour attribuer et réagir	81
3.3.2.3. Des nécessaires mutualisations des moyens	82
3.3.3. Un rapprochement institutionnalisé des acteurs des pôles défensif et offensif au nom des missions de cyberdéfense : de l'atténuation à l'effacement ?	84
3.4. Conclusion	86
3.5. Bibliographie.	87

Chapitre 4. La frontière entre la cybercriminalité et la cyberguerre : un *no man's land* incertain

Marc WATIN-AUGOUARD

4.1. Introduction.	89
4.2. Le champ de la cybercriminalité jusqu'aux limites du plafond de verre	91
4.2.1. Le champ de la cybercriminalité : un essai de délimitation	92
4.2.2. La cybercriminalité, « criminalité du XXI ^e siècle »	94
4.2.3. La cyberconflictualité aux frontières du plafond de verre	95

4.3. Guerre dans le cyber, cyber dans la guerre	97
4.3.1. Le cyber dans la guerre, une réalité quotidienne.	98
4.3.2. La guerre autonome dans le cyber à l'épreuve du droit des conflits armés.	98
4.3.3. La cyberpersuasion numérique	101
4.4. Conclusion	103
4.5. Bibliographie.	103

Chapitre 5. La cyberdéfense, dimension numérique de la sécurité nationale 105

Bertrand WARUSFEL

5.1. Introduction.	105
5.2. La cyberdéfense dans le cadre politico-juridique de la sécurité numérique	106
5.2.1. Une définition de la cyberdéfense	106
5.2.2. Le rattachement de la cyberdéfense à la stratégie de sécurité nationale	107
5.3. L'émergence d'un régime juridique cohérent de la cyberdéfense	108
5.3.1. Les moyens juridiques de la posture permanente de cyberdéfense.	109
5.3.2. Les instruments exceptionnels de riposte à la crise	110
5.4. Conclusion	112
5.5. Bibliographie.	113

Chapitre 6. Omniprésence sans omnipotence : la puissance américaine contre Huawei à l'heure de la 5G 115

Mark CORCORAL

6.1. Introduction.	115
6.2. L'offensive unilatérale américaine contre Huawei : une campagne de nuisance provoquant d'importants dommages collatéraux	118
6.2.1. Huawei : une menace « rare et exceptionnelle » mettant en cause la place des États-Unis dans l'ordre international	118
6.2.2. Une offensive politique, juridique et économique contre Huawei provoquant d'importants dommages collatéraux	120
6.3. L'offensive diplomatique américaine : les limites de la coercition rhétorique américaine à l'égard de leurs partenaires et alliés	125

6.3.1. Éduquer plutôt que persuader : une tentative de coercition rhétorique des partenaires et alliés	126
6.3.2. Une mise à l'agenda réussie mais une coercition rhétorique au succès limité	128
6.3.3. La coercition rhétorique américaine dans la <i>special relationship</i>	131
6.4. L'offensive anti-Huawei : baromètre de la puissance américaine ? . . .	134
6.5. Bibliographie	135

Chapitre 7. L'enjeu des données personnelles et souveraines à l'aune d'un « droit international du renseignement » en formation

145

Fabien LAFOUASSE

7.1. Introduction	145
7.2. Les règles de droit invoquées à l'occasion du recueil de données personnelles et de données souveraines	148
7.2.1. Droit au respect de la vie privée <i>versus</i> surveillance générale des communications	149
7.2.2. Violation de la souveraineté territoriale <i>versus</i> cyberespionnage	151
7.3. La localisation des données à l'aune du droit international du renseignement	154
7.3.1. Fluidité des données <i>versus</i> stockage des données	154
7.3.2. Sphère des données <i>versus</i> droit international du renseignement	157
7.4. Conclusion	161
7.5. Annexe : les quadrants du droit du renseignement	162
7.6. Sources et bibliographie	162
7.6.1. Sources	162
7.6.2. Bibliographie	164

Chapitre 8. Les coopérations internationales de cybersécurité

167

Guillaume POUPARD

8.1. Les tendances actuelles des attaques	167
8.2. Les multiples voies des coopérations internationales	169
8.3. L'enjeu des attributions d'attaques	172

Chapitre 9. Cyberdéfense et politiques de régulation aux États-Unis : de l'échec de la politique globale au succès de l'approche sectorielle	175
Adrien MANNIEZ	
9.1. Introduction.	175
9.2. L'identification d'une nouvelle menace et l'impact du cyber sur la manière de concevoir les politiques de sécurité et de défense étatsuniennes.	176
9.3. De l'impact du cyber sur les politiques à l'impact de la politique sur le cyber.	180
9.4. De la politique cyber globale à l'approche sectorielle : le succès d'une politique de régulation non avouée.	189
9.5. Conclusion	194
9.6. Bibliographie.	195
 Liste des auteurs.	 197
 Index	 199