

Table des matières

Préface	3
Avant-propos	13
Chapitre 1. L'espace numérique	19
Introduction: un nouveau domaine d'opportunités... et de menaces	19
I. Réseaux informatiques, Internet, cyberspace	20
1. Quelques rappels fondamentaux	20
2. Brève histoire d'Internet	21
3. Gouvernance technique d'Internet	24
4. Le « <i>deep</i> » et le « <i>dark</i> »	25
II. Topologie du cyberspace	26
1. Couches, frontières, centres de gravité, pentes	26
2. Acteurs en présence	28
3. Caractéristiques et propriétés	29
III. Les données numériques	33
1. De quoi parle-t-on?.....	33
2. Quelques représentations en cycles de vie	34
3. Enjeux de valeur et de sensibilité	35
4. Aparté sur l'intelligence artificielle	36
IV. Ce qu'il se passe dans le numérique	38
1. Plusieurs grands aspects d'une transformation globale	38
2. Cognition: accès à la connaissance, apprentissage, esprit critique.....	39
3. Relations sociales.....	45
4. Enjeux économiques	47
5. Enjeux sociétaux de régulation.....	49
6. Une source croissante de conflictualité stratégique	51

V. Enjeux de souveraineté.....	54
1. De la souveraineté classique à la souveraineté numérique.....	54
2. Acception classique du concept de souveraineté	54
3. Souveraineté numérique?	56
Chapitre 2. La menace d'origine cyber	61
Introduction: une menace élevée, croissante et protéiforme	61
I. Comprendre la menace cyber.....	62
1. Les sources de menace: les attaquants	62
2. Les motivations et finalités des attaquants.....	64
3. Les cibles: des entités, des systèmes, des données	68
4. Les vulnérabilités	73
a. Des vulnérabilités de différentes natures.....	73
b. Le cycle de vie d'une vulnérabilité technique	74
c. Les vulnérabilités « 0-day ».....	76
d. Économie générale de la recherche de vulnérabilités.....	77
e. Responsabilités des éditeurs et des utilisateurs	78
f. Enjeux de politique publique.....	80
5. Les modes opératoires, outils et infrastructures.....	82
II. Tendances générales associées à la menace d'origine cyber.....	89
III. Quelques exemples récents d'attaques informatiques	91
1. Estonie (2007)	91
2. <i>Olympic Games</i> et <i>Stuxnet</i> (2010).....	92
3. <i>Shamoon</i> (2012).....	92
4. <i>Sony Pictures Entertainment</i> (2014).....	93
5. <i>Office of Personnel Management</i> (2014-2015).....	94
6. <i>TV5 Monde</i> (2015)	94
7. <i>Ashley Madison</i> (2015)	95
8. <i>SWIFT</i> (2015-2016).....	95
9. <i>The Shadow Brokers</i> (2016-2017).....	96
10. <i>Mirai</i> (2016).....	96

11. Vault 7 (2017).....	97
12. WannaCry (2017).....	97

Chapitre 3. La cybersécurité.....99

Introduction : la difficile quête d'un état optimal de cybersécurité.....99

I. Le risque cyber : un risque stratégique qu'il faut « gouverner ».....101

1. Remarques préliminaires.....	101
2. La nécessaire complémentarité entre les approches « par la conformité » et l'analyse des risques.....	102
3. Un risque stratégique et systémique: une préoccupation pour les dirigeants.....	103
4. Le besoin d'une gouvernance holistique.....	105
5. Une attention particulière sur la conformité.....	106
6. Des textes de référence issus de différentes sphères.....	108

II. Un processus itératif pour animer la gouvernance du risque cyber..... 109

1. Une méthode en fil rouge: EBIOS <i>Risk Manager</i>	109
2. Délimiter le périmètre, comprendre le contexte.....	112
3. Identifier et évaluer des risques et des scénarios.....	112
4. Décider, en pleine conscience, d'une façon de traiter les risques.....	113

**III. La réduction des risques grâce aux mesures de protection,
de défense et de résilience115**

1. Généralités.....	115
a. Types et fonctions.....	115
b. Principes.....	116
2. Décourager les attaquants.....	117
3. Protéger les SI.....	119
4. Détecter les attaques.....	120
a. Au niveau d'une organisation.....	120
b. La détection en France en bref.....	126
c. Les centres de réponse aux incidents informatiques: les CSIRT et les CERT.....	128

5. Réagir à une attaque	130
a. Au niveau d'une organisation ou d'un individu	130
b. Dispositif étatique de réponse à une attaque cyber	138

Chapitre 4. Le modèle français..... 147

Introduction : la sécurité numérique, une politique publique interministérielle..... 147

I. Organisation et gouvernance..... 150

1. Organisation générale	150
2. L'ANSSI	152
3. D'autres acteurs incontournables	154
4. Quatre chaînes opérationnelles	156
5. Quelques enceintes de gouvernance de la cyberdéfense française.....	157
6. Atouts du modèle	160

II. Les documents fondateurs 163

1. 2008: le <i>Livre blanc sur la défense et la sécurité nationale</i>	163
2. 2009: le décret de création de l'ANSSI	165
3. 2011: la première stratégie nationale de défense et de sécurité des systèmes d'information.....	166
4. 2013: le <i>Livre blanc sur la défense et la sécurité nationale</i>	167
5. 2013: la loi de programmation militaire 2014-2019.....	168
6. 2015: la <i>Stratégie nationale pour la sécurité du numérique</i>	173
7. 2018: la <i>Revue stratégique de cyberdéfense</i>	174
8. 2018: la loi de programmation militaire 2019-2025	178
9. 2019: éléments de doctrine cyber du ministère des Armées.....	180

III. Réglementation nationale de cybersécurité..... 182

1. Considérations générales sur le cadre réglementaire français	182
2. Protection des systèmes et informations sensibles.....	183
3. Réglementation sur la cryptologie	186
4. Administration et commerce électronique	189
5. La « loi Godfrain »	193

IV. Aspects industriels	195
1. Quels besoins technologiques et industriels?	196
2. Comment faire émerger, structurer et rendre lisible un marché de la cybersécurité?	197
a. La certification de sécurité	199
b. La qualification	200
c. L'agrément.....	200
d. La labellisation	201
e. Les Visas de sécurité ANSSI.....	202
3. Quid de l'échelon européen et de l'international?	202

Chapitre 5. Les enjeux internationaux205

Introduction : pourquoi parler d'enjeux internationaux en matière de sécurité numérique ? 205

I. Quelques grands acteurs	207
1. Les États-Unis d'Amérique.....	208
a. Une lente prise en compte des enjeux cyber sur les quatre dernières décennies.....	208
b. L'organisation fédérale actuelle de cybersécurité.....	212
c. Quelques éléments saillants	213
2. La Fédération de Russie	215
a. Généralités.....	215
b. Organisation et doctrine	217
3. La République populaire de Chine	219
a. Généralités.....	219
b. Evolutions récentes de la doctrine et de l'organisation chinoises en matière de cybersécurité	222
II. La coopération internationale	225
1. Rappels de relations internationales et de droit international	225
2. Alliances et coopérations bilatérales	226
a. « Alliances traditionnelles » et « alliances cyber »	226
b. Établir une coopération bilatérale en matière de cybersécurité	228

3. Organisations internationales.....	231
a. L'Organisation des Nations unies (ONU).....	232
b. L'Union européenne (UE).....	235
c. L'Organisation du traité de l'Atlantique Nord (OTAN).....	244
d. L'Organisation de coopération et de développement économiques (OCDE).....	250
III. Paix, sécurité et stabilité stratégique du cyberspace	252
1. Régulation internationale du cyberspace: de quoi parle-t-on?	252
2. La séquence onusienne: droit international et cyberspace	254
a. Faut-il un « traité du cyberspace »?.....	254
b. Le traitement du sujet à l'ONU	255
c. Les travaux du GGE	256
3. La convention de Budapest: coopération internationale et cybercriminalité.....	262
4. L'arrangement de Wassenaar: contrôle des exportations et sécurité numérique.....	263
5. Perspectives actuelles et futures	265
a. Acteurs: au-delà des États, une implication croissante du secteur privé	265
b. Sujets: continuer à construire le cadre juridique et à renforcer la coopération internationale.....	266
c. Des enceintes multilatérales variées	266
 Chapitre 6. Une brève histoire de la sécurité numérique en France	 271
 Introduction: « celui qui ne sait pas d'où il vient ne peut savoir où il va »	 271
I. Cadrage de l'exercice: jusqu'à quand remonter?.....	272
II. Les temps anciens: de l'invention de l'imprimerie à la fin du XIX^e siècle	275
III. L'ère contemporaine « pré-électronique »	276
1. De 1870 à la Première Guerre mondiale.....	276
2. La Première Guerre mondiale	278
3. Conclusions intermédiaires.....	280

4. L'entre-deux-guerres.....	281
5. La Seconde Guerre mondiale.....	284
IV. La deuxième partie du XX^e siècle et la numérisation	289
1. Les années 1950 et 1960.....	289
2. Les années 1970	294
3. Les années 1980 et 1990.....	295
4. Des années 2000 à nos jours.....	299
5. Conclusions finales du chapitre	301
Remerciements.....	303
Glossaire des acronymes et sigles	305
Références.....	313
I. Livres.....	313
1. Sur la sécurité numérique ou fortement connexes	313
2. Pour lire l'histoire de la sécurité numérique	314
3. Sur d'autres sujets	315
II. Textes officiels.....	316
1. Textes réglementaires français	316
a. Arrêtés.....	316
b. Constitution.....	316
c. Décrets.....	316
d. Instructions interministérielles	317
e. Lois.....	318
f. Ordonnance.....	318
2. Textes réglementaires internationaux.....	319
a. Divers.....	319
b. États-Unis d'Amérique.....	319
c. Organisation des Nations unies	319
d. Union européenne.....	321

3. Textes doctrinaux et rapports divers.....	322
a. France	322
b. International.....	324
III. Articles, publications et références web	324
1. France	324
2. International.....	326