

SOMMAIRE

Introduction.....	13
Le monde de demain et l'optimisme du désespoir.....	14
Rencontres et résistances : pour un optimisme de combat.....	15
Rencontres et résonances : vers un optimisme créatif	16
Des textes alertes	16

PARTIE 1. MANAGEMENT DE L'INCERTITUDE AU TEMPS DU CYBER

Chapitre 1. Gouverner l'incertitude : une cyberattaque en temps de crise	21
---	-----------

Fabien Rech

Introduction.....	22
Un château fort mal gardé : prémices d'un basculement.....	22
La faille humaine, chaînon manquant de la résilience	23
Ce que l'incident révèle : enseignements d'un chaos évitable	24
Cybersouveraineté : le dilemme stratégique.....	26
Conclusion	27

Chapitre 2. L'odyssée du cyberspace ? Une lecture stratégique des cyberrisques.....	31
--	-----------

Christian Foussard et Wim Van Wassenhove

Introduction.....	32
Définir le risque cyber : une cartographie technique	33
Ce qui fait spécificité : un risque inclassable	35
Le cyber dans l'espace analytique du danger : faits, modèles, finalités	37
Le cyber dans l'espace métaphysique du danger : règles, valeurs, finalités	39

Zones de dissonance stratégique.....	42
Conclusion : un appel à la lucidité stratégique	44

Chapitre 3. Bugs et organisations en silos : comment les risques cyber appellent de nouvelles pratiques managériales.....47

John Kingston et Dina Dajani Daoudi

Introduction	48
Les origines d’une crise organisationnelle et les questions posées ...	49
Les propositions de réponses via le Decision Model Canvas (DMC) .	53
Conclusion et ouvertures.....	54

PARTIE 2. CYBER AU CŒUR DES ORGANISATIONS

Chapitre 4. Lutte contre la cybercriminalité : focus sur les collectivités et les entreprises.....59

Marc Boget et Rémy Février

Introduction	60
La cybercriminalité : une forme de délinquance en plein essor – un fléau pour nos collectivités !.....	60
La cybercriminalité : nos entreprises en danger !.....	65
Conclusion	68

Chapitre 5. Développer une stratégie cyber antifragile : les leçons du GIGN..... 71

François Cazals et Ghislain Réty

Introduction	72
Dans un monde BANI, les technologies de l’information changent la donne stratégique	72
Une organisation antifragile : le GIGN	75
Développer une stratégie cyber antifragile	79
Conclusion	80

Chapitre 6. La perception du risque cyber en entreprise83*Emilie Peneloux, Cécile Godé et Philippe Lépinard*

Introduction	84
Le risque cyber : un objet en construction	85
Un cyberscore pour agir sur la perception du risque cyber	88
Conclusion	90

PARTIE 3. CYBER COMME FACTEUR STRATÉGIQUE

Chapitre 7. Enjeux informationnels du cyber : fonctions sociales et défis techniques95*Alexandre Kahn*

Introduction	96
Les réseaux sociaux comme vecteurs de l'action	97
Investir le risque	102

Chapitre 8. Entre contrôle et ouverture : sécurité des API à l'ère de l'IA103*François Acquatella et Christian Chung*

Introduction	104
Forks et fragmentation : entre opportunité et menace	105
Sécurisation dynamique des API.....	107
Arbitrage entre ouverture et contrôle	109
Conclusion	110

Chapitre 9. Le cybercrime et les stratégies innovantes.....111*Christine Dugoin-Clément*

Introduction	112
Quelques considérations théoriques sur l'innovation	112
D'Aramco en Arabie saoudite aux <i>wipers</i> du début de l'invasion de l'Ukraine	112
L'intégration du volet humain dans l'attaque pour maximiser l'effet.....	114

PARTIE 4. ACTEURS DU CYBER

Chapitre 10. Quand les pirates deviennent corsaires : alerte numérique et recomposition des pouvoirs119

Jean-Philippe Denis et Hugo Gaillard

Introduction. L'alerte numérique comme mise en crise institutionnelle.....	120
Une économie instable : l'influence comme secteur, promesse et trouble	121
D'une cible à l'autre : trajectoire d'alerte, effets en chaîne	123
Trois lectures pour penser l'alerte : entrepreneuriat institutionnel, hypercompétition et <i>whistleblowing</i>	126
Agir dans un monde d'expositions croisées : quelques repères stratégiques	128
Prolongements : quand l'alerte déborde ses cibles.....	130
Conclusion	131

Chapitre 11. La Gendarmerie nationale, acteur clé de la cyberprévention des PME dans un contexte de guerre hybride 135

Cyprien Ronze-Spilliaert

Introduction	136
La vulnérabilité des PME face aux cyberattaques et les failles du dispositif national de cybersécurité entraînent des risques systémiques.....	137
Par ses actions de cyberprévention au profit des PME, la Gendarmerie nationale complète le dispositif national de cybersécurité.....	141

PARTIE 5. CYBER ET COMBINAISON RÉSILIENTE

Chapitre 12. Une mise en perspective du couplage cybersécurité / gestion de crise au travers du stress lié à une attaque *wiper*149

Morgane Lucas, Christine Dugoin-Clément et Marc Bidan

Introduction et mise en contexte : de la diversification à la vulnérabilité	150
--	-----

Phase 1 : La cyberattaque ou l'inquiétude entre rançongiciel et <i>wiper</i>	151
Phase 2 : Les réactions en cascade ou la recherche de la coordination en temps de crise	151
Phase 3 : Les enjeux stratégiques ou le lien entre géopolitique et imagerie médicale	153
Phase 4 : Que pourrions-nous retenir de cette séquence ?	155
Chapitre 13. Risque cyber et erreurs comportementales à l'heure de l'IA : l'enjeu de la formation	159
<i>Cédric Denis-Rémis, Yann Bonnet et Jean-Fabrice Lebraty</i>	
Introduction	160
Risque cyber et erreurs comportementales.....	160
Envisager la cybersécurité dans le cadre de la responsabilité numérique des entreprises	163
Remédier par la formation	165
Chapitre 14. Quand tout s'effondre : leçons stratégiques et organisationnelles d'une cyberattaque universitaire	169
<i>Jean-Philippe Denis et Pascal Corbel</i>	
Introduction	170
Récit d'un effondrement... finalement évité	170
L'anticipation du risque et ses limites.....	174
Des équilibres délicats	178
Conclusion	184
Conclusion.....	189
Présentation des auteurs	193