

Sommaire

Préface	7
Préambule	9
Introduction	11
PARTIE I - CONCEPTS ET LÉGISLATION	13
Titre I - Phénomène de la cybercriminalité	15
Chapitre 1 - Historique de la cybercriminalité	15
Chapitre 2 - Terminologie liée à la cybercriminalité	21
<i>Section 1 • Appréhension de la terminologie</i>	21
<i>Section 2 • Flou terminologique et critères communs</i>	23
Titre II - Cybercriminalité et outils juridiques	25
Chapitre 1 - Qualification des infractions et situation actuelle en droit belge ..	26
<i>Section 1 • Qualification des infractions</i>	26
Sous-section 1 ■ Typologie des infractions :	26
brève analyse d'une hétérogénéité	
Sous-section 2 ■ Actes répréhensibles :	28
exposé des difficultés de qualification	
<i>Section 2 • Situation actuelle en droit belge</i>	31
Sous-section 1 ■ Faux en informatique	31
Sous-section 2 ■ Fraude informatique	33
Sous-section 3 ■ Infractions contre la confidentialité, l'intégrité et	37
la disponibilité des systèmes informatiques et	
des données qui sont stockées, traitées ou	
transmises par ces systèmes	
Sous-section 4 ■ Sabotage des données et sabotage informatique	45
Chapitre 2 - Adaptation de la procédure pénale et des méthodes	47
de recherche des infractions à la réalité des réseaux	
et des systèmes informatiques	
<i>Section 1 • Situation belge particulière : la Computer Crime Unit</i>	50
<i>Section 2 • Recherche sur les réseaux informatiques</i>	51
<i>Section 3 • Obligation d'informer et de collaborer</i>	56
<i>Section 4 • Saisie de données</i>	61
<i>Section 5 • Écoutes téléphoniques et interception des télécommunications</i>	63
<i>Section 6 • Réquisitions informatiques</i>	66
<i>Section 7 • Obligation d'enregistrer et de conserver</i>	70
<i>les données de télécommunication</i>	

Section 8. Repérage informatique et localisation de l'origine ou de la destination de télécommunications	73
Section 9. Infiltration dans un système informatique	76
Section 10. Observation sur internet	77
Section 11. Future mesure : identification des détenteurs des cartes de téléphonie prépayées	79
Chapitre 3 - Preuves électroniques	80
PARTIE II - MISE EN PERSPECTIVES DES CONCEPTS	83
Titre I - Les anonymous	85
Chapitre 1 - Historique des Anonymous	86
Chapitre 2 - Exposé de différents « faits » des Anonymous	88
Titre II - Entreprises et cybercriminalité	90
Chapitre 1 - Premier type de risque : les menaces provenant de l'intérieur	92
Section 1. Agissements imprudents des travailleurs	92
Section 2. Téléchargements illicites	92
Section 3. Sabotage informatique de bases de données	94
Section 4. Divulgence du know-how	95
Section 5. Lignes de prévention	95
Chapitre 2 - Deuxième type de risque : les menaces provenant de l'extérieur	99
Section 1. Vol des outils de travail informatiques des travailleurs	99
Section 2. Botnets	100
Section 3. Programmes malveillants	100
Section 4. Pollution de site web	101
Section 5. Lignes de prévention	102
Chapitre 3 - Facteurs aggravant les risques de menace	103
Section 1. Mobilité informatique et cloud computing	103
Section 2. Évolution des systèmes d'information	104
Section 3. Dépendance technologique	104
Section 4. Banalisation de la monétique	105
Section 5. Équipements privés utilisés dans le domaine professionnel	105
Chapitre 4 - Forme particulière de cybercriminalité : le « cyberparasitisme économique »	106
Conclusion	110