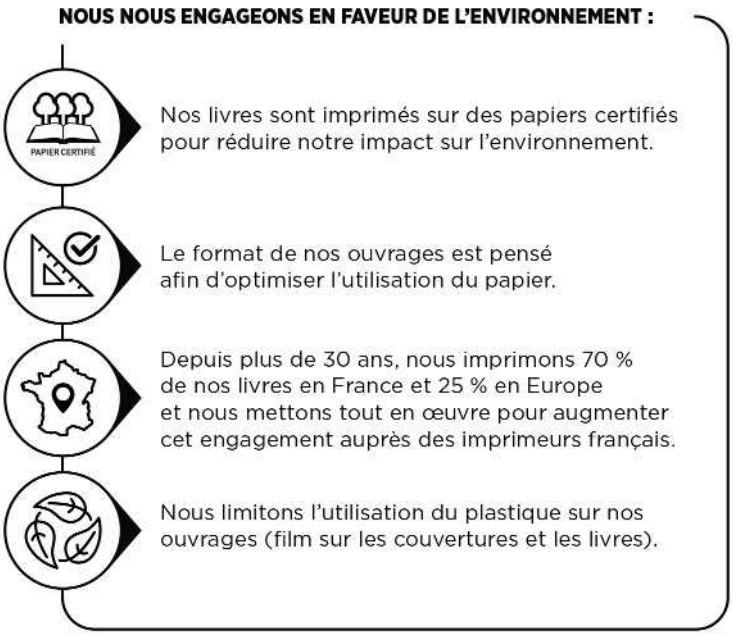
Cybercriminalité

Comprendre, prévenir, réagir

Solange Ghernaouti
Experte internationale en cybersécurité
cyberdéfense et lutte contre la cybercriminalité
Professeure de l'Université de Lausanne
Membre de l'Académie suisse des sciences techniques

DUNOD

Mise en pages : Nord Compo



11 rue Paul Bert, 92240 Malakoff
www.dunod.com
ISBN 978-2-10-085869-9

AVANT-PROPOS

Ce livre offre une **synthèse** des problématiques liées à la **cybercriminalité** afin de comprendre ce phénomène complexe en pleine expansion pour mieux le prévenir, s'en prémunir et réagir. Il permet d'apprécier la manière dont les technologies du numérique favorisent l'expression de nouveaux crimes et délits tout en étant au service de la performance criminelle. La cybercriminalité est considérée en mettant en perspective l'évolution de la criminalité informatique dans ses **dimensions civilisationnelle, politique et économique**.

Les divers modes d'expression de la cybercriminalité sont analysés sous l'angle des profils des **victimes** et des **criminels** ainsi qu'au travers des modes opératoires et outils mis en œuvre pour réaliser cette cybercriminalité.

Il s'agit, ni d'un livre de droit sur la cybercriminalité ou le droit du numérique, ni d'un livre technique. Il est conçu comme un pont entre les ouvrages juridiques et ceux concernant les technologies qui sont par conséquent réservés à un lectorat spécialisé. Ce livre permet l'acquisition de **connaissances transversales**, issues de différents champs disciplinaires et d'une certaine expérience du terrain nécessaires à la compréhension des exigences de la **lutte contre la cybercriminalité**. Par une approche intégrée, il traite de manière complémentaire des aspects incontournables permettant de développer une **vision globale** des problématiques et des moyens requis pour la maîtrise de la cybercriminalité.

Les dix **chapitres** qui structurent ce livre sont **indépendants**, ils peuvent être abordés dans l'ordre présenté mais aussi au gré des intérêts de chacun. Des figures et des exemples issus de situations concrètes les illustrent, un résumé les conclut. Afin de contribuer à renforcer l'apprentissage des connaissances, vérifier l'acquisition des fondamentaux comme le développement d'un **esprit de discernement**, des **exercices corrigés** et des **questions de réflexion** sont proposés en fin de chapitre. Ainsi, plus de 200 exercices et éléments de discussion sont traités, constituant ainsi une base de connaissance unique en son genre.

Un certain relief est apporté au texte pour faciliter la lecture et la compréhension par des termes mis en **gras** pour souligner leur importance, par la traduction anglaise du vocabulaire spécifique et par des paragraphes mis en évidence.

Ce livre est entièrement **« fait main – fait maison »**, c'est-à-dire sans recours à l'intelligence artificielle.

Guide de lecture et objectifs des chapitres

Le chapitre 1 présente la **terminologie** liée à la cybercriminalité et les principaux **concepts** qui permettent de comprendre comment les pratiques criminelles se sont transformées du fait d'Internet et du numérique.

Le chapitre 2 offre un **panorama** de la manière dont les technologies de l'information et des communications permettent la réalisation de crimes et de délits. Comprendre les **facteurs facilitateurs** de la cybercriminalité contribue à l'identification des **leviers d'actions** à activer pour lutter contre.

Le chapitre 3 explore les conséquences de la cybercriminalité sur les personnes, les organisations, les États et la population **victimes** de cybercriminels.

Le chapitre 4 met en évidence l'évolution de la **cybercriminalité** en rapport avec les **nouvelles possibilités numériques** et leurs usages (cryptomonnaies, univers virtuels, objets connectés, villes intelligentes, intelligence artificielle…). Il aborde également la problématique écologique et **environnementale** ainsi que les **dérives** liées aux capacités de surveillance concomitantes aux pratiques numériques.

Le chapitre 5 permet de comprendre les **motivations** et l'état d'esprit des personnes impliquées dans des actions cybercriminelles. Une typologie est proposée pour mieux les distinguer en fonction de caractéristiques communes afin de faciliter l'analyse d'une réalité multiforme.

Le chapitre 6 a pour objectifs de présenter les invariants de la réalisation de **cyberattaques** afin de comprendre les outils conceptuels et pratiques utilisés par les cybercriminels pour parvenir à leurs fins.

Le chapitre 7 présente la manière dont les cybercriminels organisent leurs activités en tirant parti des caractéristiques d'Internet. Il traite en particulier des **marchés noirs de la cybercriminalité** (Darknets), des services offerts et de la manière dont ils contribuent à la performance criminelle.

Le chapitre 8 est consacré au fait qu'une démarche intégrée de **cybersécurité** peut contribuer à répondre à certains besoins de la lutte contre la cybercriminalité. En mettant l'accent sur la nécessité de **gérer les risques** pour être à l'abri des dangers et en facilitant la compréhension que la cybersécurité n'est pas uniquement une question de technique. Ce chapitre présente les principaux instruments de la **maîtrise des risques informatiques d'origine criminelle**. La démarche complète de sécurisation des systèmes d'information est traité dans cet ouvrage complémentaire : *Cybersécurité. Analyser les risques, mettre en œuvre les solutions* (S. Ghernaouti, Dunod, 2022, 7e éd.).

Le chapitre 9 propose les outils conceptuels et pratiques à mettre en œuvre pour **enquêter** et réaliser des **investigations informatiques** afin de pouvoir collecter des **traces numériques** et recueillir des **preuves** admissibles auprès d'un tribunal**.**

Le chapitre 10 est consacré à la **dimension stratégique** de la lutte contre la cybercriminalité et à ses conditions de succès aux niveaux national et international.

***

« Il n'y aura pas de changement de société sans changement humain et pas de changement humain sans changement de chacun ». Pierre Rabhi, paysan philosophe, *La convergence des consciences*, 2016.

Ce livre est le fruit de mes activités d'enseignement, de recherche et de conseil au sein d'institutions privées, gouvernementales et internationales qui s'inscrivent dans la durée. Il est dédié à ceux qui ont envie de comprendre pour agir, pour que demain soit différent mais en mieux.

Solange GHERNAOUTI
Docteure en Informatique de l'Université Paris-Sorbonne.
Ancienne auditrice de l'Institut des hautes études de défense nationale (IHEDN).
Directrice du *Swiss Cybersecurity Advisory & Research Group* (www.scarg.org).
Associée fondatrice de la société Heptagone *Digital Risk Management & Security.*
Présidente de la Fondation SGH – Institut de recherche Cybermonde.
Professeure de l'Université de Lausanne.
Membre de l'Académie suisse des sciences techniques.
Médaille d'Or du Progrès.
Chevalier de la Légion d'honneur.

Table des matières

Avant-propos III

Chapitre 1 • Transformation numérique de la criminalité 1

1.1 Une évolution civilisationnelle 1
1.1.1 Le cyberespace 1
1.1.2 De nouvelles pratiques criminelles 3
1.2 Caractéristiques 3
1.2.1 Terminologie 3
1.2.2 Interprétation 4
1.3 Une question juridique 6
1.3.1 Comportement illégal 6
1.3.2 La Convention européenne sur la cybercriminalité 6
1.4 Une question culturelle 7
1.4.1 Le lieu et le temps 7
1.4.2 Les limites de l'éthique 7
1.5 Une question technique 9
1.5.1 Des attaques informatiques 9
1.5.2 Des atteintes aux critères de sécurité informatique 9
1.5.3 La disponibilité 9
1.5.4 L'intégrité 10
1.5.5 La confidentialité 11
1.5.6 Les problèmes de sécurité n'ont pas forcément une origine criminelle 11
Exercices 13
Solutions 13

Chapitre 2 • Des pratiques numériques au service du crime 17

2.1 Des opportunités criminelles 17
2.1.1 Le contexte d'Internet 17
2.1.2 Des facilités et une certaine impunité 18
2.2 Une couche d'isolation protectrice 20
2.2.1 Un marché mondial 20
2.2.2 Des investigations difficiles 20
2.2.3 Des conditions optimales 21
2.3 Des vulnérabilités propices à la cybercriminalité 22
2.3.1 Des technologies faillibles 22
2.3.2 Des informations publiques 24
2.3.3 Des failles critiques de sécurité 24
2.3.4 Des situations propices à la cybercriminalité 25

2.3.5 Des outils de la vengeance interpersonnelle 26
2.3.6 Des risques pour la réputation des personnes et des organisations 27
Exercices 29
Solutions 30

Chapitre 3 • Les conséquences de la cybercriminalité 33
3.1 Des atteintes aux personnes 33
3.1.1 Des escroqueries 33
3.1.2 Des intermédiaires douteux 36
3.1.3 Le smartphone, un facilitateur de cybernuisances 36
3.1.4 Faux sentiment de sécurité et prédateurs 37
3.1.5 Exemple d'une impossible confiance 38
3.1.6 Criminalité identitaire 39
3.2 Des atteintes aux entreprises 41
3.2.1 La déstabilisation de l'économie 41
3.2.2 Manipulation des marchés financiers 42
3.2.3 Monnaies virtuelles, portefeuille électronique 43
3.2.4 Guerre économique, espionnage, fuite et pillage de données 45
3.3 Des atteintes aux organisations publiques et à l'État 46
3.3.1 Des retombées sur la population 46
3.3.2 Cyberactions visant à nuire à un État et à la société 48
3.3.3 Cyberactions visant à nuire à l'environnement 49
3.3.4 Constat 49
3.3.5 Urgences environnementale, énergétique et numérique 50
3.3.6 Perspectives et leviers d'actions possibles 54
Exercices 55
Solutions 57

Chapitre 4 • Nouveaux crimes liés à l'évolution technologique et dérives 65
4.1 Objets connectés et cybercriminalité 65
4.1.1 Tout ce qui est connectable à Internet est piratable 65
4.1.2 Insécurité par conception 65
4.1.3 Des cyberattaques facilitées par la voix 66
4.1.4 Voitures autonomes 67
4.1.5 Villes intelligentes 67
4.2 Crimes liés au métaverse et aux NFT 68
4.2.1 Les méta univers virtuels 68
4.2.2 Les jetons non fongibles 69
4.3 Quelques problèmes liés à l'intelligence artificielle 70
4.3.1 Boîte noire et obscurité des algorithmes 71
4.3.2 Une logique de pouvoir 71
4.3.3 Une question de vision, de responsabilité et de croyance 72
4.4 Une cybersécurité à risque, des menaces persistantes 74
4.4.1 Cyberattaques contre des chaînes d'approvisionnement 74
4.4.2 Menaces persistantes 76
4.4.3 Une logique d'informatisation questionnable 78

4.5 Désinformation et *deep fakes* 79
4.5.1 Un phénomène qui évolue 79
4.5.2 Une logique de post-vérité 80
4.6 Dérives, ce que la surveillance informatique fait à l'humain 81
4.6.1 La reconnaissance faciale, une violence invisible 81
4.6.2 Facteurs aggravants 82
4.6.3 Transparence des observés, obscurité des observants et des algorithmes 83
Exercices 86
Solutions 88

Chapitre 5 · Les acteurs de la cybercriminalité 97
5.1 Le piratage informatique 97
5.1.1 Origine 97
5.1.2 Des hackeurs et des experts en sécuritédu numérique 98
5.2 Classification des cybercriminels 98
5.2.1 Des professionnels et des amateurs 98
5.2.2 Des personnes aux motivations multiples 99
5.2.3 Des personnes au service des gouvernements 100
5.2.4 Des mercenaires 100
5.2.5 Des crackers, des *nerds* et des *script kiddies* 101
5.2.6 Des intermédiaires et des mules 101
5.2.7 Des personnes à la recherche de défis et de la valorisation de soi 102
5.2.8 Des adeptes de concours de hacking 102
5.2.9 Des personnes à la recherche de reconnaissance 104
5.2.10 Des personnes à la recherche de profit, de pouvoir et de puissance 104
5.2.11 Le *hacking* inspiré par une motivation politique 105
5.2.12 Du *hacking* inspiré par la revendication 106
5.2.13 Des profils variés 106
5.2.14 Le *hacking* inspiré par le terrorisme 107
5.3 Des personnes aux compétences et motivations diverses 109
5.3.1 Chevaliers blancs et justiciers 109
5.3.2 Ombre et lumière 110
5.3.3 Convergence d'intérêts 110
5.4 L'esprit hackeur 110
5.4.1 Devenir hackeur 110
5.4.2 L'art de la manipulation 112
5.4.3 Des passages à l'acte facilités par l'intelligence artificielle 113
Exercices 114
Solutions 115

Chapitre 6 · La boîte à outils des cybercriminels 123
6.1 Des instruments au service de la cybercriminalité 123
6.1.1 Du spam et de l'hameçonnage 123
6.1.2 Des facilités pour obtenir des paramètres de connexion 125
6.1.3 Des logiciels malveillants 128

6.2 Des cyberattaques pour nuire, soumettre et conquérir 131
6.2.1 Attaques actives et passives 131
6.2.2 Méthodologie pour cyberattaquer 131
6.2.3 Attaques par déni de service 134
6.2.4 Attaques par défiguration 136
6.2.5 Attaque par utilisation détournée des protocoles de communication 136
Exercices 137
Solutions 138

Chapitre 7 • Marchés noirs de la cybercriminalité 145
7.1 Une structure organisée 145
7.1.1 Des marchés noirs 145
7.1.2 Une logique de marché 148
7.1.3 L'indispensable e-commerce 148
7.1.4 Des Darknets en libre-service accessibles à tous, ou pas 151
7.2 Des services à usage dual 151
7.2.1 *Crimeware as a service* 151
7.2.2 Accéder à un Darknet 152
7.2.3 Les incontournables outils de communication 154
7.2.4 Cryptomonnaie et plateforme d'échange 154
Exercices 157
Solutions 158

Chapitre 8 • Apports de la cybersécurité à la lutte contre la cybercriminalité 163
8.1 Différentes facettes de la lutte contre la cybercriminalité 163
8.2 La cybersécurité 165
8.2.1 Contexte et finalités 165
8.2.2 L'essentielle appréciation des risques 166
8.2.3 L'anticipation 169
8.3 Le partage d'information 170
8.3.1 Les besoins 170
8.3.2 Différents types d'information et d'environnements de partage 171
8.3.3 La sensibilisation et la formation 172
8.3.4 Le développement d'une culture de la cybersécurité 172
8.3.5 L'élaboration de normes dans le domaine de la cybersécurité 172
8.3.6 La maîtrise des vulnérabilités et des incidents de sécurité 173
8.3.7 Des centres de partage et d'analyse d'information 173
8.3.8 Solidarité et réciprocité 175
8.3.9 Conditions de succès d'une démarche de partage d'information 176
8.4 Quelques initiatives européennes liées à la cybersécurité 177
8.4.1 Des structures organisationnelles 177
8.4.2 Quelques aspects législatifs 177
Exercices 179
Solutions 180

Chapitre 9 • Criminalistique informatique et investigation numérique 187
9.1 Investiguer un cybercrime 187
9.1.1 La notion d'enquête 187
9.1.2 Les objectifs de l'investigation 188
9.1.3 Spécificités numériques 189
9.1.4 L'adresse IP 190
9.2 La scène du crime informatique 192
9.2.1 En amont de l'investigation, quelques préalables 192
9.2.2 La recherche de traces et de preuves numériques 192
9.3 Concepts fondamentaux relatifs aux enquêtes en cybercriminalité 194
9.3.1 La chaîne de maîtrise de l'intégrité des preuves 194
9.3.2 Méthodologie d'enquête 195
9.4 Enquêter des cybercrimes au sein des organisations 197
9.4.1 Le contexte général 197
9.4.2 Des contraintes et des injonctions contradictoires 197
9.4.3 Des comportements et des procédures 198
9.4.4 De la trace à la preuve 200
9.5 Des approches complémentaires 203
9.5.1 Enquêtes sous pseudonyme 203
9.5.2 Le recueil d'information par sources ouvertes 204
Exercices 205
Solutions 206

Chapitre 10 • Stratégie de lutte contre la cybercriminalité 211
10.1 Contexte de la lutte contre la cybercriminalité 211
10.1.1 Un continuum de sécurité 211
10.1.2 Un écosystème global 211
10.1.3 Un paradoxe 213
10.2 Prérequis à la lutte contre la cybercriminalité 214
10.2.1 Estimation de l'ampleur du phénomène 214
10.2.2 Un cadre propice 215
10.2.3 Des bases légales 215
10.3 Défis de la lutte contre la cybercriminalité 217
10.3.1 Une urgence à réagir 217
10.3.2 Le renforcement des capacités 218
10.4 Une question de volonté et de moyens 220
10.4.1 Principales structures organisationnelles internationales et européennes 220
10.4.2 Concevoir une stratégie 223
Exercices 227
Solutions 228

Index 241

1 TRANSFORMATION NUMÉRIQUE DE LA CRIMINALITÉ

PLAN

1.1 Une évolution civilisationnelle
1.2 Caractéristiques
1.3 Une question juridique
1.4 Une question culturelle
1.5 Une question technique

1.1 UNE ÉVOLUTION CIVILISATIONNELLE

1.1.1 Le cyberespace

Internet et l'ensemble des équipements informatiques, données et services mis à disposition des utilisateurs, forment le **cyberespace**. Ce cyberespace constitue un nouvel espace d'interactions et de réalisations d'activités basé sur le traitement de données numériques.

Le cyberespace peut être vu comme un **nouveau territoire** construit par l'humain, superposable au monde réel où les frontières temporelles et géographiques traditionnelles sont transcendées par la quasi-instantanéité des échanges et une connectivité des systèmes et des personnes à l'échelle mondiale.

En constante **évolution**, il est difficile de recenser tous les équipements, tous les réseaux, toutes les applications, toutes les données ainsi que toutes les interactions que le cyberespace autorise. La matérialité du cyberespace est celle de ses **infrastructures physiques** localisées dans des territoires géographiques déterminés sur terre (serveurs, ordinateurs, centres de données, réseaux de télécommunications, objets connectés, téléphones…), dans la mer (câbles sous-marins…) et dans l'espace (satellites de communication…). Les frontières géographiques traditionnelles s'estompent au profit d'un **environnement virtuel** où tous les services semblent être de proximité, où tout le monde peut, a priori, communiquer avec tout le monde, n'importe quand, n'importe où. Cette proximité est renforcée du fait d'une communication immédiate et par la possibilité d'effectuer des actions à distance.

Notre manière de vivre et de faire société est largement influencée par les technologies du numérique, qu'il s'agisse de technologies de l'information, des télécommunications ou de l'intelligence artificielle, c'est en réalité **l'informatisation de la société** dont il est question. Cela révolutionne la façon de penser et de réaliser les échanges tant politiques, économiques que sociaux ou culturels. Nos habitudes, nos manières d'agir et d'être au monde sont bouleversées par **l'usage extensif de l'informatique** et du fait de la dématérialisation. **Internet** et sa panoplie d'outils et de services influencent la manière dont chacun perçoit le monde et interagit avec lui, ce qui modifie notre manière d'agir dans le monde réel. De nouveaux comportements, modes de fonctionnement, d'interaction et d'échange entre les personnes, mais aussi entre les objets, les institutions publiques, les organisations privées et les États, en découlent. Cela concerne tous les domaines d'activités (économie, santé, politique, culture, éducation…) que cela soit dans la sphère privée, professionnelle ou publique et cela à l'échelle planétaire.

La **dématérialisation** consiste à traiter informatiquement des données qui représentent une certaine réalité. Les produits dématérialisés sont téléchargeables instantanément alors que les produits physiques sont livrés toujours plus rapidement par des acteurs logistiques globalisés.

Connectant personnes et systèmes informatiques à l'échelle mondiale, Internet, permet de mettre quasi-instantanément en relation toutes sortes d'entités, qu'elles soient bienveillantes ou malveillantes, qu'elles défendent leurs intérêts de façon loyale ou déloyale, de manière licite ou illicite (figure 1.1).

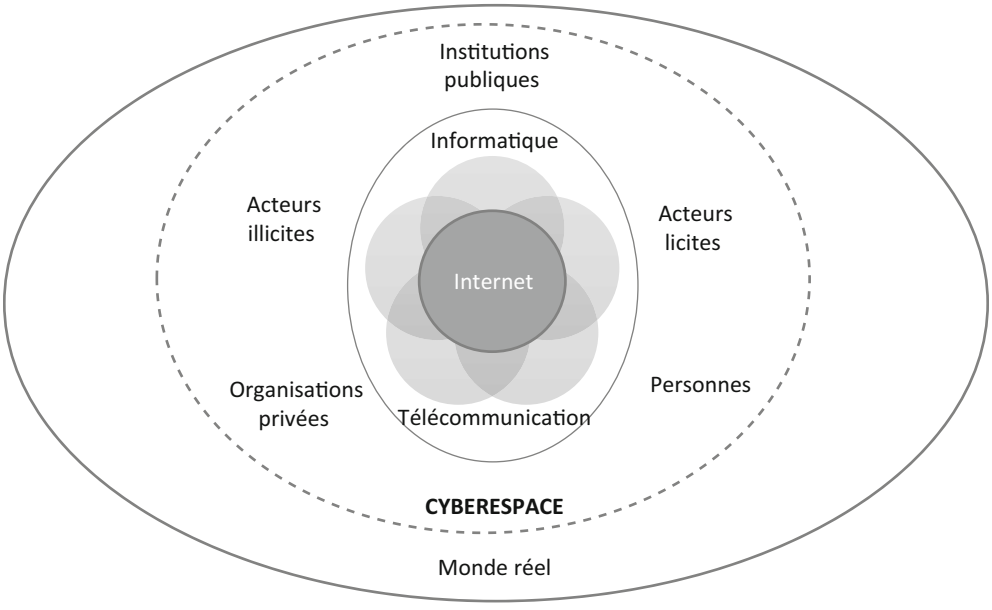


Figure 1.1 – **Internet et le cyberespace.**

La racine **cyber** provient du mot cybernétique, formé en français en 1834 pour désigner la « science du gouvernement », à partir du grec *kubermêtiké*, féminin de

kubermêtikos, dérivé de *kuberman*, signifiant diriger, gouverner. Le terme est repris en 1948 par Norman Wiener aux États-Unis (*cybernetics*) et donne naissance à la **cybernétique**, science constituée par l'ensemble des théories relatives au contrôle, à la régulation et à la communication au sein de l'être vivant et de la machine. Un *cyborg* est un organisme cybernétique, dans lequel des parties électroniques et biologiques coexistent. Le préfixe *cyber* est devenu courant pour indiquer toutes activités réalisables par Internet.

La révolution informationnelle conduit à des changements d'une ampleur sans précédent, que ce soit à l'échelle locale ou internationale. L'urbanisation numérique et **l'économie du numérique** sont des acteurs et des vecteurs de la mondialisation qui favorisent l'instauration d'un nouvel ordre numérique.

Urbanisation numérique : concentration croissante des activités et des services réalisés via l'informatique, des données numériques et des plateformes détenues par des acteurs hégémoniques de l'Internet.

1.1.2 De nouvelles pratiques criminelles

Nouvelle valeur de civilisation, « or » du XXIe siècle, les données informatiques, traitées, sauvegardées et communiquées via des ordinateurs et des réseaux de télécommunication, constituent le patrimoine numérique des individus, des organisations et des États. Elles font l'objet de toutes les convoitises. La dématérialisation des transactions et des services autorise des formes d'organisation et d'activités économiques innovantes, ce dont les organisations criminelles savent tirer parti.

1.2 Caractéristiques

1.2.1 Terminologie

La **cybercriminalité** recouvre toute activité criminelle réalisée par le biais d'Internet et des technologies du numérique. Elle englobe toute forme de **malveillance** effectuée à l'aide de l'informatique, d'équipements électroniques et des réseaux de télécommunication. La notion d'activité criminelle décrit toute activité illégale, irrégulière ou contraire à la loi.

Certains acteurs à la recherche de **profit** ou de **pouvoir** se sont accaparés Internet et le cyberespace, pour atteindre leurs objectifs. La criminalité, organisée ou non, exploite l'informatique et Internet pour accroître la performance de ses activités.

La **cybercriminalité** recouvre une large gamme de forfaits et la majorité des délits existants peuvent désormais être réalisés via Internet. Les technologies du numérique permettent également l'expression de **nouvelles formes de criminalité**.

Les systèmes informatiques, les réseaux de télécommunications, les programmes et les données sont à la fois des **cibles** de la malveillance et des **moyens** pour la réaliser et commettre des délits (figure 1.2).

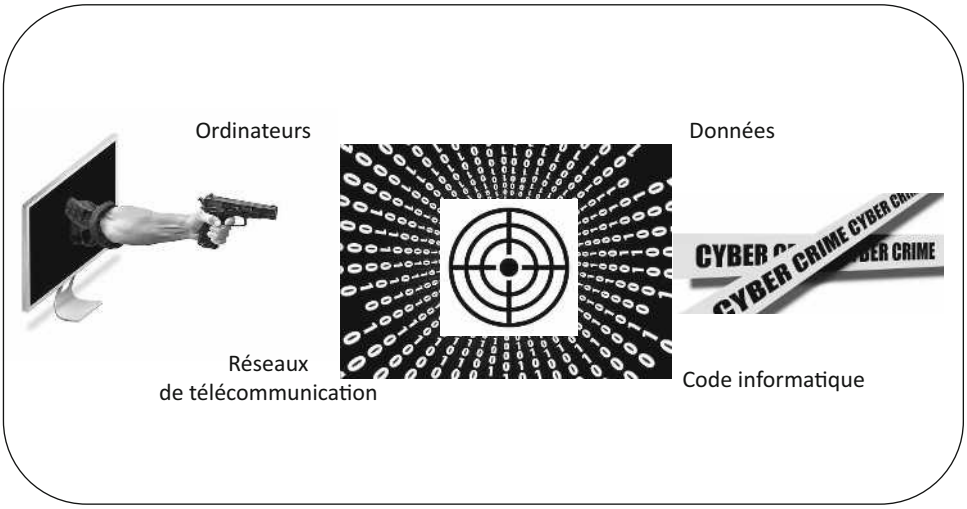


Figure 1.2 – **Les systèmes informatiques et les réseaux de communication sont les objets et les moyens du cybercrime.**

Dans le cas d'une intrusion non autorisée, via Internet, dans le système d'information d'une banque, le code informatique et le réseau permettent d'effectuer un délit (ils constituent le moyen du crime pour réaliser ce type de cyberattaque). Le système ciblé et les données sont la cible et l'objet du crime. Le mobile et la finalité de cette attaque sont fonction de la motivation et du résultat escompté par son commanditaire.

1.2.2 Interprétation

L'usage du préfixe **cyber** est communément utilisé pour créer des termes qui font spécifiquement référence à la criminalité perpétrée par des outils numériques et grâce à la connectivité. Cette dernière autorise la **mise en relation** des acteurs criminels avec leurs potentielles victimes. Ainsi de nombreux termes sont entrés dans le langage courant comme cyberattaque, cybermalveillance, cyberdélinquance, cyberviolence, cyberescroquerie, cyberfraude, cyberextorsion, cyberespionnage, cyberguerre, etc.

Le **cyberespace** étend le champ de la criminalité tout en offrant de nouvelles opportunités criminelles.

Au-delà de la question de la terminologie, le nouveau vocabulaire, lié à la criminalité à travers le cyberespace, traduit l'apparition de comportements malveillants tirant parti de l'existence et des caractéristiques d'Internet. Il peut s'agir de crimes classiques réalisés par les technologies du numérique comme le blanchiment d'argent, la fraude financière, le crime économique, l'atteinte au droit d'auteur, etc. ou de nouveaux délits rendus possibles par les technologies de l'information comme l'accès indu à un système, le vol de données, le piratage de logiciel, ou le verrouillage de ressources pour ne citer que quelques exemples.

Un **cybercrime** peut avoir des effets immédiats ou à retardement. Il peut être perpétré à distance, au-delà des frontières et des lieux géographiques où les objets du crime sont touchés.

Quelle que soit la terminologie employée, le cybercrime est un crime assisté par ordinateur qui englobe tous les délits réalisables via l'informatique et les télécommunications (figure 1.3).

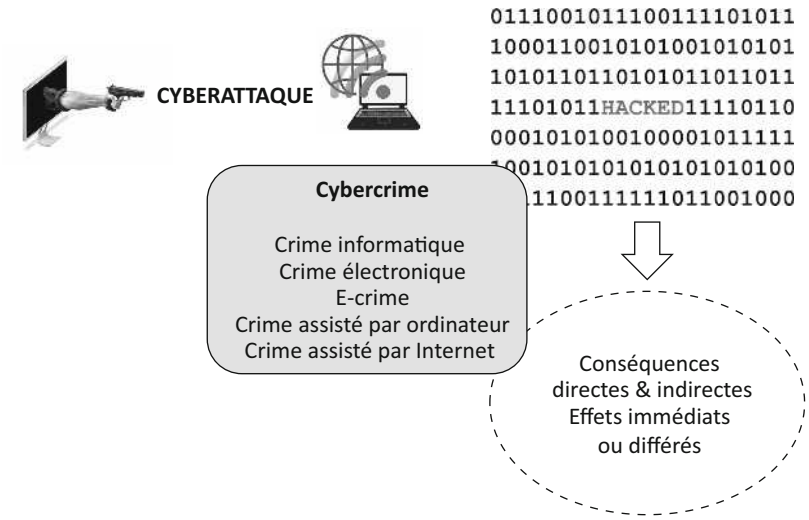


Figure 1.3 – **Le cybercrime, un crime assisté par ordinateur.**

Un cybercrime peut être de grande envergure et affecter simultanément un nombre considérable de cibles, comme c'est le cas lors de la propagation massive de virus informatiques (**cyberépidémie**).

Un cybercrime peut être commis par :

- L'exploitation des vulnérabilités relatives aux systèmes et à des personnes.
- La force (intrusion dans un système en cassant des barrières de sécurité).
- La fraude (usurpation de paramètres de connexion d'ayants droit).
- Le leurre (des personnes et des systèmes, détournement du mode de fonctionnement normal des technologies).

La réalisation d'activités délictueuses au travers du cyberespace peut se caractériser par le fait que les criminels agissent cachés derrière un écran et de **multiples intermédiaires techniques** mais aussi à distance de leurs victimes qui peuvent être dans des pays différents.

1.3 Une question juridique

1.3.1 Comportement illégal

Un crime est une action interdite par **la loi**. Les lois doivent donc préexister pour définir ce qui relève d'une activité licite ou non. La notion de cybercriminalité recouvre une vaste réalité et un concept sujet à de multiples définitions et interprétations selon les cultures juridiques des pays. Toutefois, c'est en 1983 que l'Organisation de coopération et de développement économiques (OCDE) a défini la notion d'**infraction informatique** comme étant « tout comportement illégal, immoral ou non autorisé qui implique la transmission et/ou le traitement automatique de données ». Cela ne concerne pas uniquement les activités Internet, mais s'étend à tout ce qu'il est possible de faire via l'informatique, les télécommunications, y compris la téléphonie fixe ou mobile, à tous les équipements qui intègrent un traitement électronique et informatique de données (cartes à puces, distributeurs de billets, capteurs, centres de contrôle, systèmes de navigation assistée, jeux électroniques, multimédia, etc.). Ainsi, tout élément et toute infrastructure informatique qui manipulent de l'information numérique, y compris les systèmes d'intelligence artificielle, sont concernés par le **crime informatique**.

1.3.2 La Convention européenne sur la cybercriminalité

Le fait que la criminalité et la délinquance relèvent du droit pénal des nations engendre de multiples définitions, caractéristiques ou typologies du crime informatique, lesquelles varient selon les pays. La Convention sur la cybercriminalité du **Conseil de l'Europe**, premier et encore seul instrument juridique de portée internationale, sans pour autant préciser explicitement le terme de cybercriminalité, n'en définit pas moins les infractions relevant de celle-ci. La convention, comme l'explicite son préambule, répond également à « la nécessité de mener, en priorité, une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale ; […] préoccupés par le risque que les réseaux informatiques et l'information électronique soient utilisés également pour commettre des infractions pénales et que les preuves de ces infractions soient stockées et transmises par le biais de ces réseaux » (source : Conseil de l'Europe – **STCE n° 185** – Budapest 23.XI.2001).

Le préambule de la convention délimite le pourtour de la cybercriminalité en inscrivant sa lutte dans le contexte de la **protection des droits fondamentaux**. Cette dernière inclut la protection des données personnelles et la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Il rappelle aussi : « la nécessité de garantir un équilibre adéquat entre les intérêts de l'action répressive et le respect des droits de l'homme fondamentaux, tels que garantis dans la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe (1950), dans le Pacte international relatif aux droits civils et

politiques des Nations unies (1966), ainsi que dans d'autres conventions internationales applicables en matière de droits de l'homme, qui réaffirment le droit à ne pas être inquiété pour ses opinions, le droit à la liberté d'expression, y compris la liberté de rechercher, d'obtenir et de communiquer des informations et des idées de toute nature, sans considération de frontière, ainsi que le droit au respect de la vie privée ».

Outre les différents délits identifiés, la convention met l'accent notamment sur la nécessité de la coopération entre les États et l'industrie privée et sur l'entraide judiciaire internationale pour la lutte contre la cybercriminalité.

En 2003, un **premier Protocole additionnel** relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques est venu compléter la Convention (STE n° 189). Le Comité des ministres du Conseil de l'Europe a adopté en 2021 un **deuxième Protocole additionnel** à la Convention relatif au renforcement de la coopération et de la divulgation des **preuves électroniques** (STE n° 224).

1.4 Une question culturelle

1.4.1 Le lieu et le temps

La limite entre ce qui est légal et ce qui ne l'est pas est influencée par la situation historique, culturelle et temporelle dans laquelle la société se développe. La **morale** varie selon la culture et le contexte sociopolitique d'un pays et d'une époque. Les comportements identifiés comme déviants par rapport à la morale, à la normalité, ou encore par rapport à des coutumes relevant d'une culture particulière, peuvent être parfois, s'ils s'effectuent au travers d'Internet, considérés comme relevant de la cybercriminalité.

La morale est relative aux mœurs, aux habitudes, aux règles de conduites admises et pratiquées dans une société, ce qui peut être traduit ou non par des préceptes moraux. **Avoir un sens moral** est de disposer de capacités de discernement du bien et du mal, permettant de se comporter en être vertueux.

Un acte peut être **déviant** par rapport à la morale, sans pour autant être illégal. En revanche, la définition de ce qui est licite ou non dépend de la loi applicable dans le pays considéré. Cet ancrage territorial des lois pose d'ailleurs un problème lorsqu'il s'agit de crimes perpétrés par-delà les frontières géographiques d'un pays, comme c'est généralement le cas en matière de cybercriminalité.

1.4.2 Les limites de l'éthique

L'éthique est la science du bien et du mal, de la morale. Elle se concrétise en un ensemble de règles de conduites considérées comme bonnes. Ces règles et ces principes moraux peuvent sous-tendre une charte d'éthique ou de **déontologie**. Le serment d'Hippocrate que prêtent les médecins est un exemple bien connu de ce genre de code déontologique.

La science du bien et du mal est le fondement de la théorie de l'action humaine en tant qu'elle est soumise au devoir et a pour but le bien.

Une charte d'éthique n'a pas force de loi, et ne contraint que celles et ceux qui choisissent de s'y conformer. Si ce n'est pas le cas, les potentielles atteintes à l'image et à la réputation et le blâme public peuvent inciter des organisations ou des personnes à respecter *a minima* des règles d'éthique. Cette approche de dénonciation pour blâmer (*name and shame*) est facilitée par Internet (figure 1.4).

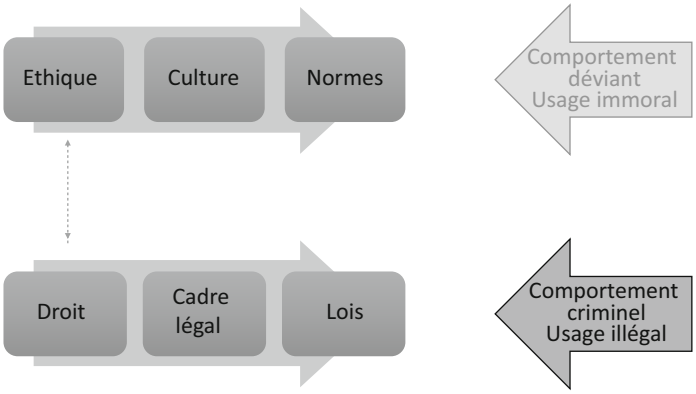


Figure 1.4 – **Au-delà de l'éthique, le droit applicable.**

L'éthique est souvent invoquée dans des stratégies de communication (marketing, publicité…) des entreprises sans pour autant s'appuyer sur la réalité des faits. Ses éléments de discours sur l'éthique existent à l'instar de ceux relatifs à l'environnement, à l'écologie (*green washing*) ou à l'égalité, la diversité et l'inclusion. Des vertus éthiques, comme la diversité, l'équité et l'inclusion, peuvent être avancées pour la forme, pour conforter un discours performatif, alors même qu'elles ne sont pas instanciées dans les pratiques, que les objectifs sont insuffisamment définis et que les moyens pour les atteindre ne sont pas alloués. Cela ne permet pas de développer des pratiques cohérentes au regard des vertus, valeurs et principes éthiques à respecter.

Le **lavage éthique** (*ethical washing*) est une pratique consistant à feindre une prise en considération des grands principes éthiques largement reconnus pour améliorer la manière dont une entité (organisations, universités, responsables économiques ou politiques...) est perçue.

Les discours sur l'éthique, non traduits en pratiques concrètes et vérifiables, créent un faux sentiment de prise en compte des besoins éthiques. Ils entretiennent l'illusion que les valeurs relevant de l'éthique sont prises en considération alors qu'ils ne sont là que pour justifier une manière de procéder qui peut être éloignée de l'éthique.