

# Cybersécurité

**Analyser les risques  
Mettre en œuvre les solutions**

**Solange Ghernaoui**

Experte internationale en cybersécurité,  
cyberdéfense et lutte contre la cybercriminalité  
Professeure de l'Université de Lausanne

7<sup>e</sup> édition

**DUNOD**

Toutes les marques citées dans cet ouvrage  
sont des marques déposées par leurs propriétaires respectifs.

Illustration de couverture : © VideoFlow – Shutterstock

<p>Le pictogramme qui figure ci-contre mérite une explication. Son objet est d'alerter le lecteur sur la menace que représente pour l'avenir de l'écrit, particulièrement dans le domaine de l'édition technique et universitaire, le développement massif du photocopillage.</p> <p>Le Code de la propriété intellectuelle du 1<sup>er</sup> juillet 1992 interdit en effet expressément la photocopie à usage collectif sans autorisation des ayants droit. Or, cette pratique s'est généralisée dans les établissements</p>		<p>d'enseignement supérieur, provoquant une baisse brutale des achats de livres et de revues, au point que la possibilité même pour les auteurs de créer des œuvres nouvelles et de les faire éditer correctement est aujourd'hui menacée.</p> <p>Nous rappelons donc que toute reproduction, partielle ou totale, de la présente publication est interdite sans autorisation de l'auteur, de son éditeur ou du Centre français d'exploitation du droit de copie (CFC, 20, rue des Grands-Augustins, 75006 Paris).</p>
--	--	--

© Dunod, 2022

11 rue Paul Bert, 92240 Malakoff

[www.dunod.com](http://www.dunod.com)

ISBN 978-2-10-084149-3

Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L. 122-5, 2° et 3° a), d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (art. L. 122-4).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

# AVANT-PROPOS

Ce livre offre une synthèse des problématiques et des éléments de solution pour réaliser la cybersécurité des systèmes d'information. Il traite de l'analyse des risques, de la cybercriminalité, des questions de gouvernance, de gestion stratégique et opérationnelle de la sécurité. Il présente les principales mesures organisationnelles, managériales et techniques de la sécurité des environnements numériques qui permettent de satisfaire leurs besoins de sécurité.

- Le **chapitre 1** introduit les **principes fondamentaux** et les domaines d'application de la sécurité des systèmes d'information qui doivent être appréhendés de manière systémique. Il constitue la base nécessaire à la compréhension globale des différents aspects et dimensions de la cybersécurité.
- Le **chapitre 2** offre un panorama des **cyberrisques** et des différentes formes d'expression de la **cybercriminalité** et de ses impacts. Il identifie les vulnérabilités inhérentes au monde numérique, à **Internet** et au **cyberespace** ainsi que leur exploitation à des fins malveillantes. Il identifie les divers leviers d'action qui contribuent à produire de la sécurité et à lutter contre la cybercriminalité.
- Le **chapitre 3** traite des aspects liés à la **maîtrise des risques**, à la **gestion stratégique** et à la **gouvernance** de la sécurité mais aussi des questions d'**intelligence économique** en lien avec la cybersécurité. Les **dimensions politique, juridique, managériale et socio-économique** dans lesquelles s'inscrivent la sécurité informatique et les besoins de **cyberrésilience** sont identifiées pour insister sur la nécessité de doter les individus, les organisations et les États de moyens suffisants à leur cybersécurité et cyberdéfense. Les métiers relatifs à la sécurité numérique, les acteurs, les compétences comme les notions d'organisation, de responsabilité et de mission de sécurité sont présentés.
- Le **chapitre 4** concerne les **outils méthodologiques**, les **normes**, les **méthodes**, les bonnes pratiques, les démarches à disposition pour identifier les besoins de sécurité, **définir une politique de sécurité**, mettre en place des mesures, **auditer, mesurer, évaluer, certifier** la sécurité. Ce chapitre traite également de la **gestion de crise**, des **plans de secours, de reprise et de continuité** des activités.
- Le **chapitre 5** est consacré aux principes fondamentaux de la **cryptographie** (chiffrement) mis en œuvre dans des environnements d'informatique distribuée pour offrir des services de confidentialité, d'authentification, d'intégrité, d'imputabilité et de non-répudiation. Une analyse critique des différents mécanismes de cryptographie, qui tient compte des dernières évolutions du domaine, est réalisée. Une introduction à la **cryptographie quantique** ainsi qu'une présentation des avantages, inconvénients et limites des **systèmes de chiffrement** sont proposées. Les concepts et les mécanismes de signature numérique, de certificats numériques,

d'infrastructures de gestion de clés (PKI), de tiers de confiance, d'autorité de certification et de **blockchain** sont illustrés.

- Le **chapitre 6** traite des problématiques et des mesures de **sécurité des infrastructures de télécommunication** Internet. Il présente notamment la mise en œuvre de protocoles cryptographiques pour offrir des services de sécurité Internet (IPv6, IPSec). Les principes de sécurité liés au routage, à la gestion des noms, au contrôle d'accès, à des **réseaux privés virtuels** (VPN), à l'externalisation et au **cloud computing** sont étudiés.
- Le **chapitre 7** est dédié à la sécurité des **réseaux sans fil** et à la **mobilité**. Les technologies de la sécurité des réseaux cellulaires **GSM, GPRS, UMTS, 5G** sont présentées comme celles des **réseaux locaux sans fil 802.11** et des **réseaux personnels**.
- Faisant suite à la présentation des protocoles cryptographiques implantés dans des infrastructures réseaux filaires et sans fil, le **chapitre 8** se focalise sur des mesures permettant de renforcer la sécurité des environnements par des **systèmes pare-feu** et de **protection contre les incidents**.
- Le **chapitre 9** est dédié à la protection des contenus et à la sécurité des principaux services applicatifs d'Internet (sécurité de la **messagerie électronique**, de la **téléphonie sur Internet**, de la **navigation web**, du **commerce électronique**, des **paiements en ligne**, des **documents XML**). Sont également abordées la notion de protection des documents par **tatouage électronique**, la gestion des droits numériques (**DRM**), les problématiques de sécurité liées à l'usage de l'informatique personnelle (**BYOD**) et des **réseaux sociaux** en entreprise, ainsi que les problématiques de la **confiance** et de la **désinformation**.
- Le **chapitre 10** traite de la **gestion de réseau** comme outil de cohérence et d'**intégration des mesures** de sécurité et des savoir-faire managérial et technologique.

Les chapitres sont indépendants. Chacun comprend, entre autres, une présentation de ses objectifs, un résumé et des exercices corrigés. Ces derniers permettent de vérifier la bonne compréhension des concepts présentés et renforcent l'apprentissage des connaissances. Un certain relief est introduit dans le texte par des **termes** mis en gras pour souligner leur importance, par la traduction anglaise du vocabulaire de la sécurité (*security vocabulary*) et par des encarts.

Un glossaire et un index concluent cet ouvrage.

En traitant de manière complémentaire du management et de l'ingénierie de la cybersécurité, ce livre, par une **approche globale et intégrée**, permet d'appréhender toute la **complexité de la cybersécurité** et de développer les compétences nécessaires à sa maîtrise.

### Ressources numériques

Cette édition revue et augmentée propose **plus de 200 exercices corrigés** ainsi que des compléments en ligne **téléchargeables** sur la page associée à l'ouvrage du site des éditions Dunod :

<https://www.dunod.com/ean/9782100841493>

## Dédicace

Ce livre est le fruit de mes activités de recherche, d'enseignement et de conseil développées depuis plus d'une vingtaine d'années. Il est aussi celui de mes premiers ouvrages entièrement consacrés à la sécurité informatique et des télécommunications : *Stratégie et ingénierie de la sécurité des réseaux* (InterÉditions, 1998) et *Sécurité Internet, stratégies et technologies* (Dunod, 2000).

Je dédie cet ouvrage à ceux qui désirent apprendre, comprendre et agir, à mes étudiants, assistants et doctorants d'hier et d'aujourd'hui, à mes proches présents et lointains, à A. L. et S. qui m'accompagnent depuis toujours.

Solange GHERNAOUTI

Professeure de l'Université de Lausanne

Docteure en informatique de l'Université Paris VI

Ancienne auditrice de l'IHEDN

Directrice du *Swiss Cybersecurity Advisory & Research Group*

Associée fondatrice de la société genevoise *Digital Risk Management & Security*

Présidente de la Fondation SGH – Institut de recherche Cybermonde

Membre de l'Académie suisse des sciences techniques

Chevalier de la Légion d'honneur

[www.scarg.org](http://www.scarg.org)



# TABLE DES MATIÈRES

<b>Avant-propos</b>	III
<b>Chapitre 1 • Sécurité informatique et cybersécurité</b>	1
1.1 Objectifs de sécurité	1
1.1.1 Cyberspace et sécurité	1
1.1.2 Disponibilité	2
1.1.3 Intégrité	3
1.1.4 Confidentialité	3
1.1.5 Fonctions additionnelles	3
1.2 Domaines d'application	5
1.2.1 Sécurité matérielle, physique et environnementale	5
1.2.2 Sécurité de l'exploitation	6
1.2.3 Sécurité des réseaux de télécommunication	7
1.2.4 Sécurité logicielle, applicative et de l'information	8
1.2.5 Cybersécurité	9
1.3 Multiples facettes de la cybersécurité	10
1.3.1 Cybermenace et cyberrisque	10
1.3.2 Des cyberrisques globaux	13
1.3.3 Développer un écosystème numérique cyberrésilient	15
1.4 Différents besoins de la cybersécurité	15
1.4.1 Piloter la sécurité	15
1.4.2 Importance du juridique dans la sécurité des systèmes d'information	17
1.4.3 Éthique et formation	17
1.4.4 Architecture de sécurité et approche holistique	18
Exercices	21
Solutions	21
<b>Chapitre 2 • Cybercriminalité</b>	27
2.1 Comprendre la menace d'origine criminelle	27
2.1.1 Origine des menaces	27
2.1.2 Le cyberspace, champ d'action de la criminalité	28
2.2 Infrastructure Internet et vulnérabilités exploitées à des fins criminelles	29
2.2.1 Éléments de vulnérabilité	29
2.2.2 Internet, facteur de performance du monde criminel	30
2.2.3 Internet au cœur des stratégies criminelles	32

## Cybersécurité, analyser les risques, mettre en œuvre les solutions

2.3	Cyberrisques	33
2.3.1	Principaux risques pour les individus	33
2.3.2	Principaux risques pour les organisations	35
2.3.3	Principaux risques pour la nation et la société	35
2.3.4	Guerre sémantique et cyberhactivisme	38
2.4	Crime informatique et cybercriminalité	39
2.4.1	Éléments de définition	40
2.4.2	Écosystème cybercriminel	42
2.4.3	Marchés noirs de la cybercriminalité	43
2.5	Principales caractéristiques des cyberattaques	43
2.5.1	Étapes de réalisation d'une cyberattaque	43
2.5.2	Attaques actives et passives	45
2.5.3	Leurrer, détourner, exploiter	46
2.6	Faire face à la cybercriminalité	50
2.6.1	Développer une culture de la cybersécurité et disposer de mesures de sécurité	50
2.6.2	Diminuer le risque d'origine cybercriminelle	51
2.6.3	Lutter contre la cybercriminalité, un enjeu majeur	52
	Exercices	54
	Solutions	55
	<b>Chapitre 3 • Gouvernance et stratégie de sécurité</b>	<b>63</b>
3.1	Gouverner la sécurité	63
3.1.1	Contexte	63
3.1.2	Principes de base de la gouvernance de la sécurité	64
3.2	Gérer le risque informatique et informationnel	66
3.2.1	Définitions	66
3.2.2	Projet d'entreprise et culture de sécurité	66
3.3	Connaître les risques pour les maîtriser	67
3.4	Vision stratégique de la sécurité	69
3.4.1	Fondamentaux	69
3.4.2	Mission de sécurité	71
3.4.3	Principes de base	71
3.4.4	Conditions de succès	72
3.4.5	Approche pragmatique	73
3.4.6	Bénéfices	73
3.4.7	Aspects économiques	74
3.5	Définir une stratégie de sécurité	75
3.5.1	Stratégie générale	75
3.5.2	Compromis et bon sens	76
3.5.3	Nouveaux risques, nouveaux métiers	77
3.5.4	Acteurs et compétences	79
3.6	Organiser et diriger	80
3.7	Prise en compte des besoins juridiques	81
3.7.1	Responsabilités et obligations de moyens	81
3.7.2	La confiance passe par le droit, la conformité et la sécurité	83



3.8	Prise en compte des besoins d'intelligence économique	84
	Exercices	88
	Solutions	89
	<b>Chapitre 4 • Politique de sécurité</b>	<b>97</b>
4.1	De la stratégie à la politique de sécurité	97
4.2	Propriétés d'une politique de sécurité	99
4.3	Méthodes et normes contribuant à la définition d'une politique de sécurité	100
4.3.1	Principales méthodes françaises	100
4.3.2	Normes internationales ISO de la série 27000	102
4.3.3	Méthodes et bonnes pratiques	112
4.3.4	Modèle formel de politique de sécurité	113
4.4	De la politique aux mesures de sécurité	113
4.4.1	Classification des ressources	113
4.4.2	Mesures de sécurité	114
4.5	Continuité des activités et gestion de crise	116
4.5.1	Définitions et objectifs	116
4.5.2	Démarche de déploiement d'un plan de continuité	116
4.5.3	Plans de continuité et de reprise	117
4.5.4	Dispositifs de secours et plan de secours	120
4.5.5	Plan d'action	123
4.5.6	Gestion de crise et dispositif de gestion de crise	124
4.6	Audit des systèmes d'information et audit de sécurité	124
4.6.1	Principes de base de l'audit des systèmes d'information	124
4.6.2	Référentiel CobiT	126
4.7	Mesurer l'efficacité de la sécurité	128
4.7.1	Métriques de sécurité	128
4.7.2	Modèle de maturité	130
4.8	Certification des produits de sécurité	132
4.8.1	Critères communs	132
4.8.2	Acteurs concernés par les critères communs	133
4.8.3	Principales limites des critères communs	133
4.8.4	Principes de base des critères communs	134
	Exercices	137
	Solutions	138
	<b>Chapitre 5 • La sécurité par le chiffrement</b>	<b>151</b>
5.1	Principes généraux	151
5.1.1	Vocabulaire	151
5.1.2	Algorithmes et clés de chiffrement	152
5.2	Principaux systèmes cryptographiques	153
5.2.1	Système de chiffrement symétrique	153
5.2.2	Système de chiffrement asymétrique	155
5.2.3	Quelques considérations sur la cryptanalyse	158

## Cybersécurité, analyser les risques, mettre en œuvre les solutions

5.2.4	Cryptographie quantique	159
5.2.5	Principaux algorithmes et techniques	162
5.3	Services offerts par la mise en œuvre du chiffrement	163
5.3.1	Optimisation du chiffrement par une clé de session	163
5.3.2	Vérifier l'intégrité des données	165
5.3.3	Authentifier et signer	165
5.3.4	Rendre confidentiel et authentifier	167
5.3.5	Offrir un service de non-répudiation	167
5.4	Infrastructure de gestion de clés	167
5.4.1	Clés secrètes	167
5.4.2	Objectifs d'une infrastructure de gestion de clés	168
5.4.3	Certificats numériques	169
5.4.4	Organismes de certification	170
5.4.5	Exemple de transaction sécurisée par l'intermédiaire d'une PKI	172
5.4.6	Limites des solutions basées sur des PKI	173
5.5	Apport de la <i>blockchain</i>	175
	Exercices	177
	Solutions	178
	<b>Chapitre 6 • La sécurité des infrastructures de télécommunication</b>	<b>183</b>
6.1	Protocole IPv4	183
6.2	Protocoles IPv6 et IPSec	185
6.2.1	Principales caractéristiques d'IPv6	185
6.2.2	Principales caractéristiques d'IPSec	187
6.2.3	En-tête d'authentification (AH)	187
6.2.4	En-tête de confidentialité-authentification (ESP)	187
6.2.5	Association de sécurité	187
6.2.6	Implantation d'IPSec	189
6.2.7	Gestion des clés de chiffrement	190
6.2.8	Modes opératoires	191
6.2.9	Réseaux privés virtuels	192
6.3	Sécurité du routage	193
6.3.1	Contexte	193
6.3.2	Principes généraux d'adressage	193
6.3.3	Gestion des noms	195
6.3.4	Principes généraux de l'acheminement des données	200
6.3.5	Sécurité des routeurs et des serveurs de noms	202
6.4	Sécurité et gestion des accès	203
6.4.1	Degré de sensibilité et accès aux ressources	203
6.4.2	Principes généraux du contrôle d'accès	203
6.4.3	Rôle et responsabilité d'un fournisseur d'accès dans le contrôle d'accès	205
6.4.4	Certificats numériques et contrôles d'accès	205
6.4.5	Gestion des autorisations d'accès <i>via</i> un serveur de noms	207
6.4.6	Contrôle d'accès basé sur des données biométriques	208
6.5	Sécurité des réseaux	210
6.5.1	Protection de l'infrastructure de transmission	210

6.5.2 Protection du réseau de transport	210
6.5.3 Protection des flux applicatifs et de la sphère de l'utilisateur	211
6.5.4 Protection optimale	212
6.5.5 Sécurité du <i>cloud computing</i>	213
6.5.6 Souveraineté et <i>cloud computing</i>	216
Exercices	219
Solutions	220
<b>Chapitre 7 • La sécurité des réseaux sans fil</b>	<b>225</b>
7.1 Mobilité et sécurité	225
7.2 Réseaux cellulaires	226
7.2.1 Concepts de base	226
7.2.2 Principes de sécurité des réseaux GSM	227
7.2.3 Principes de sécurité des réseaux GPRS	229
7.2.4 Principes de sécurité des réseaux UMTS	230
7.2.5 Réseaux 5G	231
7.3 Réseaux locaux sans fil 802.11	234
7.3.1 Concepts de base	234
7.3.2 Principes de sécurité 802.11	234
7.3.3 Sécurité renforcée (norme 802.11i)	236
7.4 Réseaux personnels sans fil	238
Exercices	240
Solutions	240
<b>Chapitre 8 • La sécurité par pare-feu et la détection d'intrusion</b>	<b>243</b>
8.1 Sécurité d'un intranet	243
8.1.1 Risques associés	243
8.1.2 Éléments de sécurité	244
8.2 Principales caractéristiques d'un pare-feu	246
8.2.1 Fonction de cloisonnement	246
8.2.2 Fonction de filtre	248
8.2.3 Fonctions de relais et de masque	249
8.2.4 Critères de choix d'un pare-feu	251
8.3 Positionnement d'un pare-feu	251
8.3.1 Architecture de réseaux	251
8.3.2 Périmètre de sécurité	252
8.4 Système de détection d'intrusion et de prévention d'incidents	254
8.4.1 Définitions	254
8.4.2 Fonctions et mode opératoire	255
8.4.3 Attaques contre les systèmes de détection d'intrusion	259
Exercices	260
Solutions	260
<b>Chapitre 9 • La sécurité des applications et des contenus</b>	<b>265</b>
9.1 Messagerie électronique	265

## Cybersécurité, analyser les risques, mettre en œuvre les solutions

9.1.1 Une application critique	265
9.1.2 Risques et besoins de sécurité	266
9.1.3 Cas particulier du spam	266
9.2 Protocoles de messagerie sécurisés	268
9.2.1 S/MIME	269
9.2.2 PGP	269
9.2.3 Recommandations pour sécuriser un système de messagerie	271
9.3 Sécurité de la téléphonie Internet	271
9.3.1 Contexte et éléments d'architecture	271
9.3.2 Éléments de sécurité	273
9.4 Mécanismes de sécurité des applications Internet	275
9.4.1 <i>Secure Sockets Layer (SSL) – Transport Layer Security (TLS)</i>	275
9.4.2 <i>Secure-HTTP (S-HTTP)</i>	277
9.5 Sécurité du télétravail	277
9.6 Sécurité du commerce électronique et des paiements en ligne	278
9.6.1 Contexte du commerce électronique	278
9.6.2 Risques particuliers	278
9.6.3 Sécuriser la connexion entre l'acheteur et le vendeur	279
9.6.4 Sécurité des paiements en ligne	280
9.6.5 Sécuriser le serveur	282
9.6.6 Notion de contrat dans le monde virtuel	282
9.7 Sécurité des documents	283
9.7.1 Documents XML	283
9.7.2 Marquage de document et tatouage numérique	284
9.7.3 Gestion des droits numériques	285
9.8 Byod et réseaux sociaux	286
9.9 Désinformation et mesures de confiance	287
9.9.1 Fabriquer le faux	287
9.9.2 Le faux au service de la rentabilité	288
9.9.3 L'ère de l'opinion et de la post-vérité	289
9.9.4 Mesures pour renforcer la confiance	289
Exercices	292
Solutions	293
<b>Chapitre 10 • La sécurité par la gestion opérationnelle</b>	<b>299</b>
10.1 Intégration des mesures de sécurité	299
10.1.1 Interopérabilité et cohérence globale	299
10.1.2 Une question d'investissement	300
10.1.3 Une question d'outils de pilotage	301
10.2 Gestion de système et de réseau	302
10.2.1 Principes généraux	302
10.2.2 Gestion des systèmes par le protocole SNMP	303
10.3 Gestion du parc informatique	305
10.3.1 Objectifs et fonctions	305
10.3.2 Quelques recommandations	306

## Table des matières

10.4	Gestion de la qualité de service réseau	307
10.4.1	Indicateurs de qualité	307
10.4.2	Évaluation et efficacité	308
10.5	Gestion comptable et facturation	309
10.6	Gestion opérationnelle d'un réseau	310
10.6.1	Gestion des configurations	310
10.6.2	Surveillance et optimisation	311
10.6.3	Gestion des performances	312
10.6.4	Maintenance et exploitation	312
10.6.5	Supervision et contrôle	315
10.6.6	Documentation	316
10.7	Concilier gouvernance et gestion opérationnelle	317
	Exercices	318
	Solutions	319
	<b>QCM</b>	329
	<b>Glossaire</b>	342
	<b>Index</b>	363



# SÉCURITÉ INFORMATIQUE ET CYBERSÉCURITÉ

# 1

PLAN

- 1.1 Objectifs de sécurité
- 1.2 Domaines d'application
- 1.3 Multiples facettes de la cybersécurité
- 1.4 Différents besoins de la cybersécurité


OBJECTIFS

- Présenter le contexte, les enjeux et les principes généraux de la cybersécurité.
- Identifier les critères et les principales caractéristiques de la sécurité informatique et de la cybersécurité.
- Comprendre les champs d'application, les différents aspects et la dimension interdisciplinaire de la cybersécurité.
- Aborder les notions d'architecture de sécurité et d'approche holistique.

## 1.1 OBJECTIFS DE SÉCURITÉ

### 1.1.1 Cyberspace et sécurité

Le préfixe « cyber » est relatif à l'environnement informatique et aux activités rendues possibles par les technologies du numérique et de l'Internet. Le cyberspace (l'ensemble des infrastructures numériques, des données et des services mis en réseau) est une extension de notre espace naturel qui reflète notre société avec ses réalités politique, économique, sociale et culturelle. Mais contrairement à la terre, à la mer, à l'air et à l'espace extra-atmosphérique, le cyberspace est une pure création de l'être humain qui ne relève pas de la nature, il est une construction issue d'un contexte géopolitique et économique particulier.



La racine « **cyber** » provient du mot **cybernétique**, qui avait été formé en français en 1834 pour désigner la « science du gouvernement », à partir du grec *Kubernêtiké*, signifiant « diriger, gouverner ». Terme repris en 1948, aux États-Unis, par le mathématicien Norman Wiener à l'origine de la **cybernétique** (*cybernetics*), science constituée par l'ensemble des théories relatives au contrôle, à la régulation et à la communication entre l'être vivant et la machine.

La **cybersécurité** concerne des environnements numériques connectés à Internet, la sécurité informatique, celle de l'information et celle des réseaux de télécommunication. La sécurité des systèmes et services accessibles *via* le cyberspace peut être mise en défaut, entre autres, par des **cyberattaques**. Ainsi, du fait de l'usage d'Internet, de nouvelles menaces existent générant des risques d'origine cyber de niveau d'importance variable, pouvant affecter les individus, les organisations privées et publiques et les États.

La notion de **sécurité informatique** fait référence à des propriétés d'un système informatique qui s'expriment en termes de **disponibilité** (D), d'**intégrité** (I) et de **confidentialité** (C). La mise en œuvre de fonctions et de services particuliers de sécurité autorise la réalisation de ces critères de base (critères DIC), comme ceux additionnels liés à l'**authentification** (notions d'authenticité) ou encore à la **non-répudiation**, à l'**imputabilité**, ou à la **traçabilité** (figure 1.1).

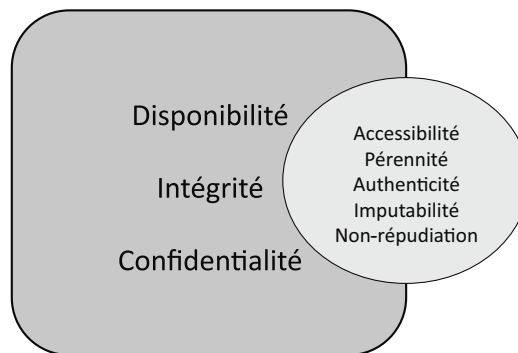


Figure 1.1 - Critères de sécurité.

### 1.1.2 Disponibilité

La **disponibilité** d'une ressource est relative à la période de temps pendant laquelle le service qu'elle offre est opérationnel. Le volume potentiel de travail susceptible d'être pris en charge durant la période de disponibilité d'un service détermine la **capacité** d'une ressource à être utilisée.

Il ne suffit pas qu'une ressource soit disponible, elle doit pouvoir être utilisable avec des temps de réponse acceptables. Sa disponibilité est indissociable de sa capacité à être **accessible** par l'ensemble des ayants droit (**notion d'accessibilité**).

La disponibilité des services, systèmes et données est obtenue par un **dimensionnement approprié** et une certaine redondance ainsi que par une **gestion opérationnelle** et une **maintenance efficaces** des ressources.

Un service nominal doit être assuré avec le minimum d'interruption, il doit respecter les clauses de l'engagement de service établies sur des indicateurs dédiés à la mesure de la **continuité de service**. Des pertes ou destructions de données, donc une indisponibilité de celles-ci, sont possibles si les procédures de sauvegarde et de restitution ainsi que les supports de mémorisation associés ne sont pas gérés correctement. Cela peut égale-



ment résulter d'actions malveillantes ou de cyberattaques. Une **politique de sauvegarde** ainsi qu'un arbitrage entre le coût de la sauvegarde et celui du risque d'indisponibilité supportable par l'organisation (désormais un grand nombre de cyberattaques visent à porter atteinte à la disponibilité des ressources informatiques des organisations) doivent être préalablement établis pour que la mise en œuvre des mesures techniques soit efficiente.

### 1.1.3 Intégrité

Le critère d'**intégrité** des ressources physiques et logiques (équipements, données, traitements, transactions, services) est relatif au fait qu'elles sont demeurées intactes, qu'elles n'ont pas été détruites ou modifiées à l'insu de leurs propriétaires tant de manière intentionnelle qu'accidentelle. Préserver l'intégrité des ressources et s'assurer que des ressources sont intègres font l'objet de mesures de sécurité. Ainsi, se prémunir contre l'altération des données, avoir la certitude qu'elles n'ont pas été modifiées, contribuent à assurer la qualité des prises de décision basées sur celles-ci.

Si, en télécommunication, l'intégrité des données relève essentiellement de problématiques liées au transfert de données, elle dépend également des aspects purement informatiques de traitement de l'information (logiciels d'application, systèmes d'exploitation, environnements logiciel et matériel d'exécution, procédures de sauvegarde, de reprise et de restauration des données). Des contrôles d'intégrité, par la mise en œuvre de mécanismes cryptographiques peuvent être effectués pour s'assurer que les données n'ont pas été modifiées lors de leur transfert par des cyberattaques.

### 1.1.4 Confidentialité

La notion de **confidentialité** est liée au maintien du **secret**, elle est réalisée par la protection des données contre une divulgation non autorisée (notion de protection en lecture).

Il existe deux types d'actions complémentaires permettant d'assurer la confidentialité des données :

- limiter et contrôler leur accès afin que seules les personnes habilitées à les lire ou à les modifier puissent le faire ;
- les rendre inintelligibles en les chiffrant de telle sorte que les personnes qui ne sont pas autorisées à les déchiffrer ne puissent les utiliser.



Des mesures complémentaires permettant de réaliser la disponibilité, l'intégrité et la confidentialité des ressources contribuent à leur protection.

### 1.1.5 Fonctions additionnelles

Identifier l'auteur présumé d'un tableau est une chose, s'assurer que le tableau est authentique en est une autre. Il en est de même en informatique, où des procédures d'**identification** et d'**authentification** peuvent être mises en œuvre pour contribuer à réaliser des mesures de sécurité assurant :

- la **confidentialité** et l'**intégrité des données** : seuls les ayants droit identifiés et authentifiés sont habilités à accéder aux ressources ;

- la **non-répudiation** et l'**imputabilité** : seules les entités identifiées et authentifiées ont pu réaliser une certaine action (notion de preuve, preuve de l'origine d'un message, etc.).

L'identification et l'authentification des ressources et des utilisateurs permettent d'associer la réalisation d'une action à une entité qui pourra en être tenue **responsable** et éventuellement en rendre compte.

L'enregistrement des activités, actions et transactions permet la **traçabilité** des événements et leur analyse. Garder la mémoire des actions survenues permet notamment de reconstituer et de comprendre ce qui s'est passé lors d'incidents afin d'améliorer la sécurité de l'environnement concerné, d'éviter que des erreurs ou des incidents ne se répètent ou encore d'identifier des personnes à l'origine des incidents de sécurité. Analyser le comportement du système et des utilisateurs à des fins d'optimisation des performances ou d'audit contribue à réaliser un processus continu de gestion de la sécurité. De plus, l'enregistrement des événements permet d'enrichir les bases de données de support aux applications de **surveillance**, de collecte et de traitement des alertes, **de détection et de réaction aux incidents**, des **plateformes de sécurité** (SOC, *Security Operation Center*) de supervision et d'administration à distance de la sécurité des systèmes d'information, ainsi que l'apprentissage nécessaire au développement des techniques d'**intelligence artificielle** appliquée à la cybersécurité.

L'**authentification** permet de vérifier l'identité d'une entité afin de s'assurer de son authenticité. Pour cela, l'entité devra prouver son identité, le plus souvent en donnant une information spécifique qu'elle est censée être seule à détenir.

Tous les mécanismes de contrôle d'accès logique aux ressources informatiques nécessitent de gérer l'identification, l'authentification des entités et la gestion des droits et permissions associés. C'est également sur la base de l'identification des personnes et des accès aux ressources que s'établissent des fonctions de facturation et de surveillance.

La **non-répudiation** est le fait de ne pouvoir nier ou rejeter qu'un événement (action, transaction) a eu lieu. À ce critère de sécurité peuvent être associées les notions d'imputabilité, de traçabilité ou encore parfois d'auditabilité (caractère de ce qui est vérifiable).

Attribuer une action à une entité déterminée (ressource ou personne) relève de l'**imputabilité**, qui peut être réalisée par un ensemble de mesures garantissant l'enregistrement fiable d'informations pertinentes relatives à un événement.

La **traçabilité** permet de reconstituer une séquence d'événements à partir des données numériques laissées dans les systèmes lors de leurs réalisations. Cette fonction comprend l'enregistrement des opérations, de la date de leur réalisation et leur imputation. Elle permet, par exemple, de retrouver l'adresse IP d'un système à partir duquel des données ont été envoyées. Afin de garder la trace d'événements, on recourt à des solutions qui permettent de les enregistrer (de les journaliser), à la manière d'un journal de bord, dans des fichiers (*log*).

L'**auditabilité** d'un système se définit par sa capacité à garantir la présence d'informations nécessaires à une analyse, postérieure à la réalisation d'un événement (courant ou exceptionnel), effectuée dans le cadre de procédures de contrôle et

d'**audit**. L'audit peut être mis en œuvre pour diagnostiquer ou vérifier l'état de la sécurité d'un système, pour déterminer s'il y a eu ou non violation de la politique de sécurité, quelles sont les ressources compromises, ou encore par exemple pour déceler et examiner les événements susceptibles de constituer des menaces de sécurité.

Les coûts liés à la journalisation et à l'analyse des données n'étant pas négligeables et la capacité mémoire des journaux n'étant pas infinie (même s'il y a recours à des infrastructures de stockage dans le *cloud*), l'administrateur système ou le responsable sécurité ont tout intérêt à identifier les **événements pertinents**, qui pourront faire l'objet d'analyse ultérieure lors de la survenue d'incidents, de procédures d'audit ou d'actions en justice.

La **durée de rétention** des informations contenues dans ces journaux peut être fixée par des réglementations sectorielles ou par la loi. C'est le cas par exemple pour les fournisseurs d'accès et de services Internet, qui doivent garder toutes les données de connexion des internautes, durant une période variable selon les réglementations auxquelles ils sont soumis (généralement entre 6 mois et 2 ans).

## 1.2 DOMAINES D'APPLICATION

Toutes les sphères d'activité de l'informatique et des réseaux de télécommunication sont concernées par la cybersécurité (figure 1.2).

### 1.2.1 Sécurité matérielle, physique et environnementale

La **sécurité matérielle, physique et environnementale** concerne tous les aspects liés à la sécurité des composants, équipements et systèmes et de l'environnement dans lequel ils se situent.

Sans vouloir être exhaustif, la sécurité physique repose essentiellement sur :

- la **fiabilité** des matériaux (éléments matériels constitutifs des systèmes) et l'usage d'équipements qui possèdent un bon degré de **sûreté de fonctionnement**, de fiabilité et de **robustesse** ;
- la protection des sources énergétiques et de la climatisation (alimentation électrique, refroidissement, etc.) ;
- la protection de l'environnement (mesures *ad hoc* notamment pour faire face aux risques d'incendie, d'inondation ou encore de tremblement de terre, pour respecter les contraintes liées à la température, à l'humidité, etc.) ;
- des mesures de gestion et de contrôle des accès physiques aux locaux, équipements et infrastructures (avec entre autres la traçabilité des entrées et une gestion rigoureuse des clés d'accès aux locaux et des personnes qui y accèdent) ;
- la redondance physique des infrastructures et des sources énergétiques ;
- le marquage des matériels pour notamment contribuer à dissuader le vol de matériel et éventuellement contribuer à le retrouver ;

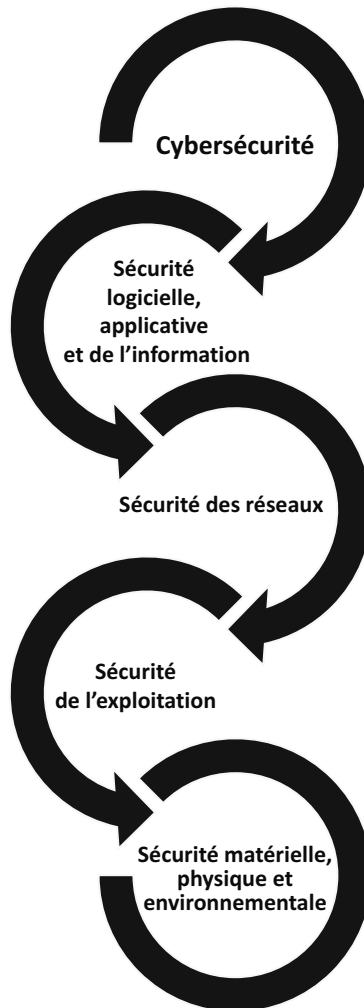


Figure 1.2 - Domaines d'application de la sécurité.

- le plan de maintenance préventive (tests, etc.) et corrective (pièces de rechange, etc.) des équipements, ce qui relève également de la sécurité de l'exploitation des environnements.

### 1.2.2 Sécurité de l'exploitation

La **sécurité de l'exploitation** doit permettre un bon fonctionnement opérationnel des systèmes informatiques et des réseaux de télécommunication. Cela comprend la mise en place d'outils et de procédures relatifs aux méthodologies d'exploitation, de maintenance, de test, de diagnostic, de gestion des performances, de gestion des changements et des mises à jour.

La sécurité de l'exploitation dépend fortement de son **degré d'industrialisation**, qui est qualifié par le niveau de supervision des applications et l'automatisation des tâches de maintenance. Bien que relevant de la responsabilité de l'exploitation, ces conditions concernent directement la conception et la réalisation des applications elles-mêmes et leur intégration dans un système d'information.

Les points clés de la sécurité de l'exploitation sont les suivants :

- gestion du parc informatique ;
- gestion des configurations et des mises à jour y compris de sécurité ;
- gestion des incidents et suivi jusqu'à leur résolution ;
- gestion des performances ;
- gestion des sauvegardes, des secours et de la continuité ;
- gestion de la maintenance et des contrats de maintenance ;
- gestion des logs et des fichiers de journalisation.

La **maintenance** doit être préventive et régulière, et selon les besoins conduire à des actions de réparation ou de remplacement des éléments défectueux.

Au-delà du coût d'une panne entraînant le remplacement des équipements, le **risque d'exploitation** se traduit par une interruption de service ou une perte de données qui peuvent avoir des conséquences préjudiciables pour l'entreprise. Cela peut aussi comprendre l'usage abusif, détourné ou criminel des outils et procédures d'administration des systèmes.

La sécurité de l'exploitation peut, dans une certaine mesure, rejoindre celle des télécommunications, car c'est au niveau des procédures d'exploitation que sont fixés les paramètres servant à la facturation de l'utilisation des ressources. Toutefois, ceci est plus spécifiquement relatif à la gestion de la comptabilité et à la maîtrise du risque financier. C'est également lors de l'exploitation des ressources que l'on vérifie l'adéquation du niveau de service offert, par rapport à celui spécifié dans un contrat de services et à sa facturation.

### 1.2.3 Sécurité des réseaux de télécommunication

La **sécurité des télécommunications** consiste à offrir à l'utilisateur final et aux applications communicantes une connectivité fiable de bout en bout. Cela passe par la réalisation d'une **infrastructure réseau** sécurisée au niveau des accès au réseau et du transport de l'information (sécurité de la gestion des noms et des adresses, sécurité du routage, sécurité des transmissions à proprement parler). Cela s'appuie sur des mesures architecturales adaptées, l'usage de plateformes matérielles et logicielles sécurisées et une gestion de réseau de qualité.

La sécurité des télécommunications ne peut à elle seule garantir la sécurité des informations. Elle ne constitue qu'un maillon de la chaîne sécuritaire car il est également impératif de sécuriser l'**infrastructure informatique** dans laquelle s'exécutent les programmes. Pris au sens large, cela comprend la sécurité physique et environnementale des systèmes (figure 1.3).

Pour que les infrastructures informatiques et télécoms soient cohérentes, performantes et sécurisées de manière optimale, l'**infrastructure de sécurité** (outils,

procédures, mesures) et la gestion de la sécurité doivent être réalisées de manière sécurisée. Les solutions de sécurité doivent être également sécurisées (notion de **récurtivité de la sécurité**). Implanter des mécanismes de chiffrement pour rendre les données transférées confidentielles est de peu d'utilité si d'aucuns peuvent y accéder lorsqu'elles sont manipulées par des plateformes matérielles et logicielles non correctement sécurisées.



La sécurité des télécommunications est peu différente de celle que l'on doit mettre en œuvre pour protéger les ordinateurs, les applications et les informations. Les réseaux de télécommunication comme les entités qu'ils mettent en relation peuvent être des sources d'insécurité et des vecteurs de propagation de programmes malveillants. La cohérence des mesures de sécurité est un facteur clé de succès.

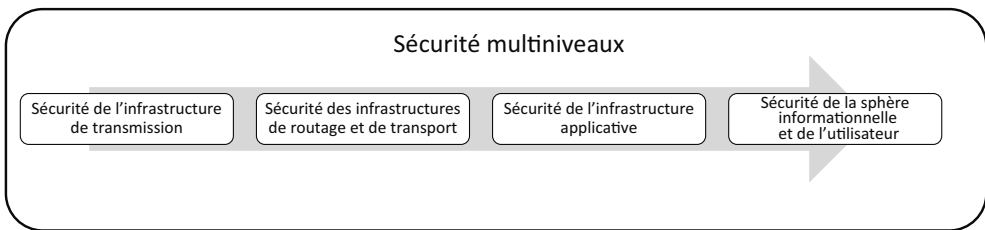


Figure 1.3 - Sécurité des infrastructures de télécommunication.

### 1.2.4 Sécurité logicielle, applicative et de l'information

La **sécurité logique** fait référence à la protection des données et à la réalisation de mécanismes de sécurité par logiciel contribuant au bon fonctionnement des programmes et des services offerts. Elle s'appuie généralement sur :

- la qualité et la sécurité des développements logiciels et des tests de sécurité ;
- une mise en œuvre adéquate de la **cryptographie** pour assurer intégrité et confidentialité ;
- des procédures de **contrôle d'accès logique** et d'authentification ;
- des procédures de détection de logiciel malveillant, de détection d'intrusion et d'incident ;
- mais aussi un dimensionnement suffisant des ressources, une certaine redondance ainsi que des procédures de **sauvegarde** et de restitution des informations sur des supports fiables, éventuellement spécialement protégés et conservés dans des lieux sécurisés pour les applications et données critiques.

La sécurité logique fait également référence à la **sécurité applicative**, qui doit tenir compte des besoins de sécurité dans le développement et l'implémentation des logiciels, et satisfaire à des exigences de sécurité et de qualité (sécurité par conception [*security by design*]).

La **sécurité applicative** comprend le développement pertinent de solutions logicielles (ingénierie, qualité du logiciel, développé sans vulnérabilité) ainsi que leur

intégration et exécution harmonieuses dans des environnements opérationnels. Elle repose essentiellement sur l'ensemble des facteurs suivants :

- une méthodologie de développement (en particulier le respect des normes de développement propres à la technologie employée et aux contraintes de sécurité et d'exploitabilité) ;
- la robustesse des applications ;
- des contrôles et des jeux de tests ;
- l'intégration de mécanismes de sécurité, d'outils d'administration et de contrôle de qualité dans les applications ;
- le choix des fournisseurs et sous-traitants ;
- l'élaboration et la gestion des contrats, les relations avec les fournisseurs comprenant des clauses d'engagement de responsabilité, y compris pour les solutions d'informatique en nuage (*cloud computing*) ;
- un plan de migration des applications critiques ;
- la validation et l'audit des programmes ;
- la qualité, la véracité et la pertinence des données.

Bien **protéger l'information**, c'est avant tout comprendre son rôle, son importance stratégique dans l'impact des décisions et des actions qu'elle permet de prendre et d'effectuer. C'est également assurer son **exactitude** et sa **pérennité** pour le temps nécessaire à son exploitation et à son archivage. Une **classification des données** permet de qualifier leur **degré de sensibilité** (normale, confidentielle, etc.) et de les protéger en fonction de ce dernier. Ainsi, à partir d'un tableau mettant en relation le type de données et leur degré de sensibilité, la nature et le nombre de protections peuvent être déterminés et des mesures de sécurité *ad hoc* développées. Par ailleurs, du point de vue de l'utilisateur, une bonne sécurité doit lui assurer le respect de son intimité numérique et la protection de ses données personnelles (*privacy by default*).

### 1.2.5 Cybersécurité

L'objet de la cybersécurité est de maîtriser les risques liés à l'usage du numérique et du cyberspace. Cela concerne toutes les infrastructures, tous les systèmes d'information, services et données ainsi que tous les acteurs qui les utilisent.

Pour une organisation, la réalisation de mesures de sécurité doit répondre à des besoins de sécurité clairement identifiés à la suite d'une **analyse des risques** spécifiquement encourus dans le cadre d'une **politique de sécurité** établie. Un système d'information sécurisé, mobilisant d'importants moyens sécuritaires, aussi pertinents soient-ils, ne pourra être efficace que s'il s'appuie sur des personnes intègres et sur un code d'utilisation adéquat des ressources informatiques pouvant être formalisé par une **charte** de sécurité. Souplesse et confiance réciproque ne peuvent se substituer à la rigueur et aux contrôles imposés par le caractère stratégique des enjeux économiques et politiques que doivent satisfaire les systèmes d'information.

Désormais, la grande majorité des activités humaines repose sur des traitements informatiques. La confiance envers ces derniers ne peut se construire qu'à condition

de pouvoir assurer et garantir leur bon fonctionnement, leur sûreté, leur fiabilité et leur sécurité (figure 1.4).

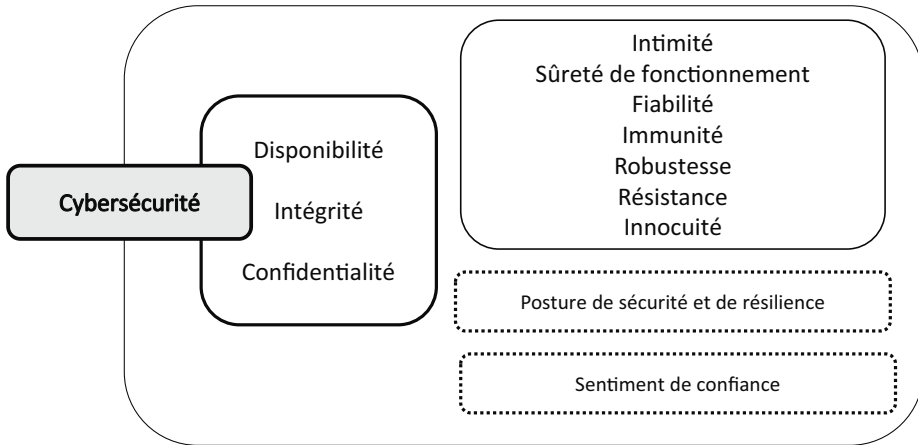


Figure 1.4 - Cybersécurité, posture de sécurité et de résilience.

La **sûreté de fonctionnement** (*safety*) caractérise un système qui est sûr et dont le bon fonctionnement peut être garanti. La **fiabilité** (*reliability*) est son aptitude à fonctionner sans incident pendant un temps donné. Le système qui possède un comportement prévisible, auquel on peut se fier, est qualifié de fiable. Sûreté et fiabilité sont des composantes de la sécurité des systèmes qui, en plus, devraient être immunisés contre des programmes malveillants. Conçues de manière robuste, spécialement protégées, résistantes aux cyberattaques et bien gérées, les infrastructures numériques peuvent offrir des services aux utilisateurs, dont les programmes et données sont traités en toute innocuité (qualité de ce qui n'est pas nuisible).



La confiance qu'une personne peut accorder à une entité relève du sentiment qui fait qu'elle peut se fier, à tort ou à raison, à cette dernière. **La confiance n'exclut pas le contrôle** ! La sécurité, en tant que propriété d'un système, peut contribuer à développer un sentiment de confiance s'il est possible de la qualifier et d'obtenir une assurance raisonnable d'un certain niveau de qualité des mesures de sécurité (notion d'assurance de sécurité).

Un environnement numérique sécurisé implique la sécurisation de tous les éléments qui le composent. Sa **sécurité globale** est toujours celle de son maillon le plus faible.

## 1.3 MULTIPLES FACETTES DE LA CYBERSÉCURITÉ

### 1.3.1 Cybermenace et cyberrisque

Une **menace** est un signe par lequel se manifeste ce que l'on doit craindre. Une **cybermenace** est une menace qui s'exprime *via* le cyberspace, qui peut toucher



tout système connecté à Internet. Sa concrétisation peut affecter le bon fonctionnement des ordinateurs, des réseaux de télécommunication et de tous les services et activités humaines qui en dépendent.

Les cybermenaces sont le plus souvent associées aux usages malveillants et détournés de l'Internet. Elles se concrétisent du fait de l'existence de vulnérabilités qui sont exploitées pour réaliser des **cyberattaques**. De nombreuses cyberattaques existent, elles recouvrent des réalités diverses en fonction des cibles touchées, de leurs impacts, finalités, origines et auteurs. Il est primordial de pouvoir identifier au plus tôt les indicateurs, y compris les signaux faibles, qui permettent d'anticiper les cyberattaques, afin d'empêcher leur réalisation ou de diminuer leur occurrence de survenue ou la gravité de leurs impacts.

Dès lors que des menaces et des vulnérabilités existent, il y a un risque relatif à l'éventualité qu'un événement non sollicité survienne et provoque des dommages.

Un **risque** est un danger plus ou moins prévisible relatif à des menaces et à des vulnérabilités. Les **cyberrisques** sont les risques inhérents à la vulnérabilité des environnements numériques, à l'usage d'Internet et à la réalisation de services au travers du cyberspace.

Les systèmes informatiques sont vulnérables, du fait de l'existence de failles et des défauts de sécurité qu'ils intègrent par conception et qui sont exploités pour effectuer des cyberattaques. Ainsi par exemple, il peut exister des :

- défaillances de conception, de mise en œuvre, de gestion ou d'utilisation des environnements informatiques ;
- déficits ou absences de comportement averti de l'utilisateur, d'hygiène informatique et sécuritaire ;
- failles techniques matérielles et logicielles, des carences ou limites des solutions de sécurité. C'est le cas par exemple des logiciels antivirus qui même à jour ne détectent que les virus connus. Ils sont d'aucune utilité pour de nouveaux virus.

L'**évaluation d'une menace** tient compte de l'ampleur et de l'importance des dégâts et dysfonctionnements qu'elle peut occasionner si elle devient réalité. Cela s'exprime par un **degré de dangerosité**, qui de manière habituelle peut se catégoriser en trois niveaux : faible, moyen et élevé.

Dans une **démarche de gestion de risques**, il est important de pouvoir identifier le plus correctement possible les menaces et leurs combinaisons. Prises isolément, des menaces de niveau faible ou moyen ne sont pas forcément graves. En revanche, associées et combinées entre elles dans des scénarios de réalisation particuliers de risques et d'interdépendances, elles peuvent devenir extrêmement préjudiciables.

Un **faible niveau** de dangerosité relève généralement de la nuisance. Un spam publicitaire pour des médicaments contrefaits n'est pas forcément grave, à moins qu'il n'entraîne la prise de produits inefficaces ou néfastes à la santé des personnes.

Les menaces de **niveau moyen** de dangerosité sont celles dont les impacts sont maîtrisables mais nécessitent des ressources pour diminuer leur survenue ou pour y

## Chapitre 1 • Sécurité informatique et cybersécurité

réagir. C'est le cas, par exemple, lorsque des programmes indésirables de type « cheval de Troie » sont installés dans des systèmes mais dont la charge de malveillance ne s'est pas encore déclenchée.

La réalisation d'une menace de **niveau élevé** de dangerosité entraîne forcément des préjudices importants.

La figure 1.5 présente un récapitulatif des cybermenaces pouvant porter atteinte au bon fonctionnement des organisations et de la société.

Cybermenaces relatives à :	Impacts potentiels sur :
Des systèmes informatiques contrôlant les infrastructures critiques	Population Economie Sécurité nationale Sûreté publique Centres d'alerte et de secours Fonctionnement du gouvernement, l'administration Diplomatie internationale
Des systèmes informatiques relatifs à la prise de décisions dans le secteur de la défense militaire et sur des systèmes d'armement (contrôle de missiles, drones, aviation militaire, équipement du soldat, ...)	Centres névralgiques nécessaires au commandement militaire et à l'opérativité de l'armée Altération des processus de prise de décisions La disponibilité et la qualité des informations nécessaires à la prise de décision pertinente Le commandement stratégique et opérationnel Les opérations militaires L'art de faire la paix et la guerre La manière de gérer les conflits, de les prévenir, de les traiter Invalidation des défenses de l'adversaire
L'information, manipulation de l'information, stratégies d'influence, guerre psychologique, guerre de l'opinion	Cyberinfluence Altération du sens Manipulation des prises de décision, de l'opinion publique, des dirigeants économiques et politiques La manipulation des foules, capacité à soulever des manifestations hostiles contre l'Etat (mouvements sociaux, activisme, terrorisme, atteinte au moral, ...) Déstabilisation des services de renseignement Atteintes à la démocratie, ingérence étrangère

Figure 1.5 - Exemples de cybermenaces pour un pays.

Il ne suffit pas de **cartographier** l'ensemble des cybermenaces envisageables, ni de se protéger des menaces les plus dangereuses et les plus probables. Il faut tenir compte de la corrélation et de l'interaction des menaces, dans des **scénarios de risques** possibles (approche combinatoire des risques). Bien qu'il soit toujours difficile de tout prévoir, la part d'imprévisibilité ou d'ingéniosité des malveillants peut parfois être anticipée s'il existe une bonne connaissance du contexte, des valeurs à protéger et de leurs vulnérabilités.

Si une menace a un fort degré de dangerosité mais qu'elle n'a qu'une chance infime de se concrétiser, ou si inversement une menace a de fortes chances de se réaliser mais à faible degré de dangerosité, elles ne sont pas à considérer avec autant de soucis que des menaces à degré moyen de dangerosité mais dont la probabilité d'occurrence est importante.

Il est donc nécessaire de pouvoir définir un paramètre de **probabilité d'occurrence** en classant cette probabilité en différents niveaux comme par exemple :

- la menace ne devrait pas se concrétiser ;
- la menace pourrait bien se concrétiser ;
- la menace devrait se concrétiser ;
- la menace va se concrétiser.

Ainsi, en combinant la probabilité d'occurrence d'une menace et sa dangerosité, il est possible d'attribuer un **degré d'importance** à une ressource pour mieux la protéger.

### 1.3.2 Des cyberrisques globaux

Les risques « cyber » s'inscrivent dans une problématique plus large des risques liés à la **dépendance** de toutes les activités humaines aux technologies du numérique et à des fournisseurs d'infrastructures matérielles et logicielles (capacités de traitement, télécoms et téléphonie, stockage, services, intelligence artificielle, *cloud*, etc.). Certains fournisseurs sont devenus des géants incontournables de l'Internet et de la téléphonie mobile et sont de véritables empires à la volonté hégémonique affichée.

La montée en puissance de certains groupes mondialisés induit de nouveaux risques notamment liés à leurs capacités à pouvoir réaliser des actions d'intelligence économique, de surveillance, d'espionnage ou encore de « manipulation » de l'information et cela à l'échelle mondiale.

L'assujettissement et la grande dépendance d'un pays à des fournisseurs et infrastructures numériques étrangers posent des problèmes liés à sa **perte de cyber-souveraineté** et d'autonomie en matière de numérique (figure 1.6). Dès lors, il pourrait devenir captif de fournisseurs étrangers dont ils subiraient la **colonisation numérique**. La dépendance à des équipementiers ou des fournisseurs de services étrangers est un problème crucial auxquels doivent faire face de nombreux pays. Cette prise de conscience est, pour beaucoup, consécutive aux révélations de **cyber-espionnage** et de **surveillance de masse**, rendues publiques par un ex-agent de l'agence de sécurité nationale (NSA – *National Security Agency*) des États-Unis d'Amérique en 2013, Edward Snowden.

Par ailleurs, au niveau individuel, certaines personnes développent des comportements et des habitudes de consommation du numérique (médias sociaux, divertissements, jeux d'argent, sexe, achats, etc.) qui peuvent relever d'un **phénomène d'addiction**.



**Lutter contre l'illettrisme numérique** ou contre les différentes formes de domination numériques, culturelles et économiques qui s'imposent au travers du cyberspace est un sujet de préoccupation. Force est de reconnaître que les champions mondiaux de l'économie du numérique ne sont ni européens ni francophones.

L'apprentissage de la technique informatique se doit d'être accompagné par des enseignements issus des sciences politique, économique, juridique et sociale. Décoder ce qui se passe derrière l'écran est tout aussi important que d'apprendre à coder ou à utiliser un équipement informatique. Seule une éducation de qualité, qui

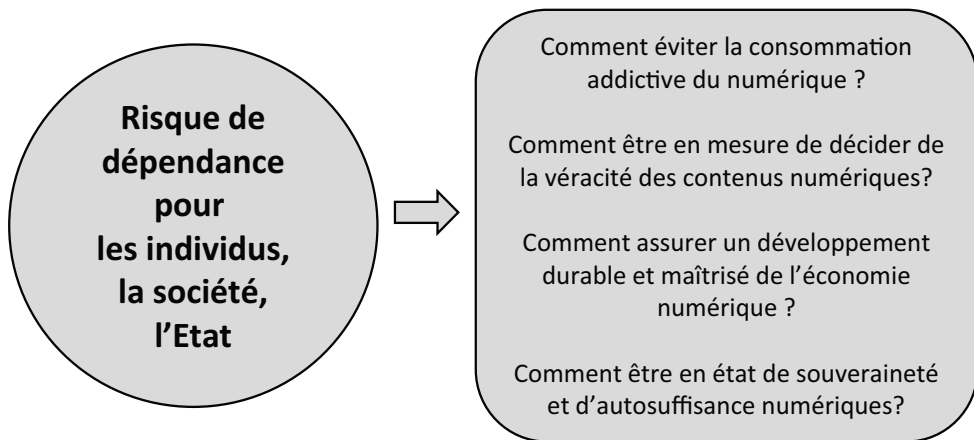


Figure 1.6 - Quelques impacts de la dépendance numérique.

traite également des questions philosophiques, écologiques, éthiques et des défis et des conséquences de la numérisation et de l'informatisation de la société, peut contribuer à éviter des aliénations et addictions numériques, à ce que l'humain ne soit pas seulement au service de la machine et de l'économie qu'elle dessert. L'enjeu est majeur car il s'agit de s'assurer que l'humain ne devienne pas un robot de chair et de sang, dépossédé de ses capacités mentales, émotionnelles ou cognitives, programmé pour répondre à des stimulations électroniques, ni ne devienne un mercenaire *hacker* au service du plus offrant.

La performance économique d'un pays dépend dans une large mesure du bon fonctionnement de son écosystème numérique et de sa cybersécurité. S'approprier le numérique pour un **développement durable de la société** passe par une certaine émancipation au regard des dépendances numériques, mais aussi par la maîtrise :

- des infrastructures de base, des ressources critiques de l'Internet et de la sécurité (y compris la sécurité énergétique) ;
- des données en vue de développer la nouvelle génération des services et des équipements basés sur l'intelligence artificielle ;
- des problématiques de financement et de fiscalité de l'économie du numérique ainsi que des transactions s'appuyant de plus en plus sur des modes de paiement dont les États tendent à perdre le contrôle (cryptomonnaies, etc.) ;
- de la recherche, de l'innovation, de l'éducation et de l'accompagnement des évolutions technologiques pour transformer ces dernières en progrès social pour tous.

Aux risques précédemment présentés il convient d'y associer ceux liés à l'**écologie du numérique**. Cela concerne en particulier les risques induits par la fabrication des systèmes, leur transport, la **consommation énergétique** nécessaire à leur fonctionnement et par l'**épuiement des ressources** naturelles, **les déchets électroniques** et la pollution qu'ils génèrent.

### 1.3.3 Développer un écosystème numérique cyberrésilient

Que ce soit dans le domaine de l'écologie, de la psychologie, du management, de l'informatique ou de l'économie par exemple, la **résilience** est relative à la capacité d'un « système » à pouvoir continuer à opérer si possible normalement, ou au moins en mode dégradé, après un incident, un choc, une perturbation, une panne. Parler de **cyberrésilience** aujourd'hui revient à admettre qu'il est impossible d'empêcher des cyberincidents d'advenir, que le cyberspace est un environnement fragile, instable et potentiellement hostile. Pour autant, faire de la cyberrésilience ne revient pas à accepter une relative impuissance à protéger correctement les infrastructures numériques, même si parfois il peut exister une certaine insuffisance de mesures de sécurité préventives efficaces.



La maîtrise des cyberrisques et la gestion de crise « cyber » doivent être efficaces pour développer la **cyberrésilience** des infrastructures numériques afin qu'en toutes circonstances, elles puissent continuer à fonctionner.

La **cybersécurité** ne doit pas s'inscrire uniquement dans une logique de réactivité qui permet d'être préparé à « survivre » à un cyberincident, d'origine intentionnelle ou non. Bien que cette capacité à résister soit fondamentale et absolument nécessaire, elle ne peut suppléer à un défaut d'une approche globale multi-acteurs, aux niveaux national et international, de l'appréhension du phénomène relevant pour l'essentiel de la **cybercriminalité** et de la réalité des cyberattaques. Le cyberspace et Internet modifient considérablement le paradigme de la protection car, contrairement au passé, il n'est plus possible de sécuriser un périmètre particulier fermé. De plus, la notion de coffre-fort électronique, représentée par la mise en œuvre de mécanismes cryptographiques, pour mettre à l'abri des données sensibles, ne permet pas de garantir la protection absolue de ces dernières.

## 1.4 DIFFÉRENTS BESOINS DE LA CYBERSÉCURITÉ

### 1.4.1 Piloter la sécurité

Que cela soit à l'échelle d'un pays ou d'une organisation, la cybersécurité doit s'appréhender d'une **manière globale et stratégique** et s'appuie sur :

- la définition d'une politique de sécurité ;
- la volonté, la motivation et la formation des acteurs impliqués ;
- la mise en place de mesures organisationnelles, procédurales, techniques et juridiques ;
- l'optimisation de l'usage des technologies numériques et des solutions de sécurité.

L'utilisation seule d'outils de sécurité (mesures techniques) ne peut pas résoudre les problèmes de cybersécurité d'une organisation. En aucun cas, ils ne se substituent à une **gestion cohérente** de l'appréhension des risques et des problématiques

de sécurité. Les besoins de sécurité doivent être clairement identifiés et constamment réévalués au regard des risques encourus et de leur évolution.



La prolifération désordonnée d'outils de sécurité non intégrés dans un processus continu de gestion ne peut qu'entraver l'usage, alourdir l'exploitation ou encore dégrader les performances d'un système d'information sans offrir un niveau de sécurité adapté aux besoins réels.

La gestion des risques « cyber » passe par une gestion rigoureuse des **ressources informatiques et humaines** ainsi que de celles liées aux locaux et à l'infrastructure environnementale. La **maîtrise de la sécurité informatique** est avant tout une question de management dont les outils, les technologies ou les solutions de sécurité (qui sont également à gérer de manière continue) constituent la partie liée à la réalisation opérationnelle des environnements numériques à sécuriser. Des outils comme ceux de chiffrement ou les pare-feu ne permettent pas de sécuriser correctement un environnement à protéger s'ils ne sont pas inscrits dans une démarche de gestion des risques et s'ils ne sont pas accompagnés de procédures de gestion qui régissent leurs configuration et utilisation. Ainsi, piloter la sécurité correspond à la volonté de **maîtriser les risques** liés à l'usage des technologies de l'information et à **maîtriser les coûts** engendrés par de l'insécurité et ceux relatifs au déploiement des mesures nécessaires pour se protéger des cybermenaces.



Pour une organisation, **gouverner** la sécurité informatique répond à une volonté politique de la direction pour maîtriser les cyberrisques, protéger ses valeurs et être compétitive. Cela s'inscrit dans une dimension humaine, organisationnelle, managériale et économique.

La cybersécurité repose sur la **complémentarité** et la **cohérence** des mesures prises au niveau stratégique et réalisées au niveau opérationnel. **Elle n'est jamais acquise définitivement**. La constante évolution des besoins, des environnements, des menaces ou des risques rend instable toute mesure de sécurité. Cela se traduit par un problème de gestion de la qualité constante et optimale de la sécurité dans un contexte dynamique et évolutif. *De facto*, la sécurité informatique ne peut s'appréhender que comme un **processus continu de gestion** afin de répondre de manière optimale (en termes de coût et de niveau de sécurité) aux besoins de production de l'organisation et de protection de ses actifs.

Pour beaucoup d'entreprises, l'outil informatique et le système d'information sont des leviers essentiels de leurs activités, de leur développement et de leur pérennité. Dans ce cas, l'indisponibilité de l'informatique ou son dysfonctionnement constituent un **risque majeur** qui peut être réduit par une gestion rigoureuse des ressources et par la mise en œuvre de mesures de cybersécurité spécifiques.

La démarche de sécurité informatique comme la démarche qualité participent à satisfaire aux exigences de **rentabilité** et de **compétitivité** des entreprises dont la performance peut être accrue par un système d'information correctement sécurisé. La finalité de celui-ci est de permettre à l'organisation qui le met en œuvre de réaliser des services ou des produits dont la qualité et les critères de sécurité sont garantis.