Cybersécurité
Analyser les risques Mettre en œuvre les solutions

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

6e édition

DUNOD

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

Illustration de couverture :
© dszc-IStock

11, rue Paul Bert 92240 Malakoff
www.dunod.com
ISBN 978-2-10-079054-8

Table des matières

Avant-propos XI

Chapitre 1 • Sécurité informatique et cybersécurité 1

1.1 Objectifs de sécurité 1
1.1.1 Cybersespace 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 6
1.2.2 Sécurité logique, applicative et de l'information 6
1.2.3 Sécurité de l'exploitation 7
1.2.4 Sécurité des réseaux de télécommunication 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 22

Chapitre 2 • Cybercriminalité 27

2.1 Comprendre la menace d'origine criminelle pour une meilleure sécurité 27
2.1.1 Origine des menaces 27
2.1.2 Le cyberespace, 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

2.3 Les 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 36
2.3.5 Guerre sémantique et cyberhacktivisme 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
2.4.4 Coûts directs et indirects 45
2.5 Principales caractéristiques des cyberattaques 46
2.5.1 Étapes de réalisation d'une cyberattaque 46
2.5.2 Attaques actives et passives 47
2.5.3. Leurrer, détourner, exploiter 49
2.6 Faire face à la cybercriminalité 53
2.6.1 Développer une culture de la cybersécurité et disposer de mesures de sécurité 53
2.6.2 Diminuer le risque d'origine cybercriminelle 53
2.6.3 Lutter contre la cybercriminalité, un enjeu majeur 55
Exercices 57
Solutions 58

Chapitre 3 • Gouvernance et stratégie de sécurité 65
3.1 Gouverner la sécurité 65
3.1.1 Contexte 65
3.1.2 Principes de base de la gouvernance de la sécurité 66
3.2 Gérer le risque informationnel 68
3.2.1 Définitions 68
3.2.2 Projet d'entreprise et culture de sécurité 68
3.3 Connaître les risques pour les maîtriser 69
3.4 Vision stratégique de la sécurité 72
3.4.1 Fondamentaux 72
3.4.2 Mission de sécurité 73
3.4.3 Principes de base 74
3.4.4 Conditions de succès 75
3.4.5 Approche pragmatique 75
3.4.6 Bénéfices 76
3.4.7 Aspects économiques 76
3.5 Définir une stratégie de sécurité 78
3.5.1 Stratégie générale 78
3.5.2 Compromis et bon sens 79
3.5.3 Nouveaux risques, nouveaux métiers 80
3.5.4 Acteurs et compétences 81
3.6 Organiser et diriger 83
3.6.1 Organisation structurelle 83

3.7 Prise en compte des besoins juridiques 84
3.7.1 Responsabilités et obligations de moyens 84
3.7.2 La confiance passe par le droit, la conformité et la sécurité 86
3.8 Prise en compte des besoins d'intelligence économique 87
Exercices 90
Solutions 92

Chapitre 4 • Politique de sécurité 99
4.1 De la stratégie à la politique de sécurité 99
4.2 Propriétés d'une politique de sécurité 101
4.3 Méthodes et normes contribuant à la définition d'une politique de sécurité 102
4.3.1 Principales méthodes françaises 102
4.3.2 Normes internationales ISO de la série 27000 104
4.3.3 Méthodes et bonnes pratiques 115
4.3.4 Modèle formel de politique de sécurité 116
4.4 De la politique aux mesures de sécurité 116
4.4.1 Classification des ressources 116
4.4.2 Mesures de sécurité 117
4.5 Continuité des activités et gestion de crises 119
4.5.1 Définitions et objectifs 119
4.5.2 Démarche de déploiement d'un plan de continuité 119
4.5.3 Plans de continuité et de reprise 120
4.5.4 Dispositifs de secours et plan de secours 122
4.5.5 Plan d'action 126
4.5.6 Gestion de crise et dispositif de gestion de crise 126
4.6 Audit des systèmes d'information et audit de sécurité 127
4.6.1 Principes de base de l'audit des systèmes d'information 127
4.6.2 Référentiel CobiT 129
4.7 Mesurer l'efficacité de la sécurité 131
4.7.1 Métriques de sécurité 131
4.7.2 Modèle de maturité 132
4.8 Certification des produits de sécurité 134
4.8.1 Critères communs 134
4.8.2 Acteurs concernés par les critères communs 135
4.8.3 Principales limites des critères communs 135
4.8.4 Principes de base des critères communs 136
Exercices 137
Solutions 140

Chapitre 5 • La sécurité par le chiffrement 149
5.1 Principes généraux 149
5.1.1 Vocabulaire 149
5.1.2 Algorithmes et clés de chiffrement 150

5.2 Principaux systèmes cryptographiques 151
5.2.1 Système de chiffrement symétrique 151
5.2.2 Système de chiffrement asymétrique 153
5.2.3 Quelques considérations sur la cryptanalyse 156
5.2.4 Cryptographie quantique 157
5.2.5 Principaux algorithmes et techniques 160
5.3 Services offerts par la mise en œuvre du chiffrement 161
5.3.1 Optimisation du chiffrement par une clé de session 161
5.3.2 Vérifier l'intégrité des données 163
5.3.3 Authentifier et signer 164
5.3.4 Rendre confidentiel et authentifier 166
5.3.5 Offrir un service de non-répudiation 166
5.4 Infrastructure de gestion de clés 166
5.4.1 Clés secrètes 166
5.4.2 Objectifs d'une infrastructure de gestion de clés 167
5.4.3 Certificats numériques 168
5.4.4 Organismes de certification 170
5.4.5 Exemple de transaction sécurisée par l'intermédiaire d'une PKI 171
5.4.6 Limites des solutions basées sur des PKI 173
5.5 Apport de la blockchain 174
Exercices 177
Solutions 140

Chapitre 6 • La sécurité des infrastructures de télécommunication 183
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 188
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 194
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 204
6.4.3 Rôle et responsabilité d'un fournisseur d'accès dans le contrôle d'accès 205

6.4.5 Certificats numériques et contrôles d'accès 206
6.4.6 Gestion des autorisations d'accès via un serveur de noms 207
6.4.7 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 211
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 cloud computing 213
Exercices 218
Solutions 219

Chapitre 7 • La sécurité des réseaux sans fil 225
7.1 Mobilité et sécurité 225
7.2 Réseaux cellulaires 227
7.3 Sécurité des réseaux GSM 227
7.3.1 Confidentialité de l'identité de l'abonné 228
7.3.2 Authentification de l'identité de l'abonné 229
7.3.3 Confidentialité des données utilisateur et de signalisation 230
7.3.4 Limites de la sécurité GSM 230
7.4 Sécurité des réseaux GPRS 231
7.4.1 Confidentialité de l'identité de l'abonné 231
7.4.2 Authentification de l'identité de l'abonné 232
7.4.3 Confidentialité des données de l'utilisateur et de signalisation 232
7.4.4 Sécurité du cœur du réseau GPRS 234
7.5 Sécurité des réseaux UMTS 234
7.5.1 Confidentialité de l'identité de l'abonné 234
7.5.2 Authentification mutuelle 235
7.5.3 Confidentialité des données utilisateurs et de signalisation 237
7.5.4 Intégrité des données de signalisation 238
7.5.5 Évolutions à long terme et réseau 5G 239
7.6 Réseaux locaux sans fil 802.11 241
7.6.1 Principes de base 241
7.6.2 Sécurité 802.11 242
7.6.3 Renforcer la sécurité (norme 802.11i) 244
7.7 Réseaux personnels sans fil 249
Exercices 252
Solutions 253

Chapitre 8 • La sécurité par pare-feu et la détection d'incidents 257
8.1 Sécurité d'un intranet 257
8.1.1 Risques associés 257
8.1.2 Éléments de sécurité d'un intranet 258
8.2 Principales caractéristiques d'un pare-feu 260
8.2.1 Fonction de cloisonnement 260

8.2.2 Fonction de filtre 262
8.2.3 Fonctions de relais et de masque 264
8.2.4 Critères de choix d'un pare-feu 265
8.3 Positionnement d'un pare-feu 266
8.3.1 Architecture de réseaux 266
8.3.2 Périmètre de sécurité 267
8.4 Système de détection d'intrusion et de prévention d'incidents 268
8.4.1 Définitions 269
8.4.2 Fonctions et mode opératoire 269
8.4.3 Attaques contre les systèmes de détection d'intrusion 273
Exercices 274
Solutions 275

Chapitre 9 • La sécurité des applications et des contenus 281
9.1 Messagerie électronique 281
9.1.1 Une application critique 281
9.1.2 Risques et besoins de sécurité 282
9.1.3 Cas particulier du spam 283
9.2 Protocoles de messagerie sécurisés 284
9.2.1 S/MIME 285
9.2.2 PGP 286
9.2.3 Recommandations pour sécuriser un système de messagerie 287
9.3 Sécurité de la téléphonie Internet 288
9.3.1 Contexte et éléments d'architecture 288
9.3.2 Éléments de sécurité 289
9.4 Mécanismes de sécurité des applications Internet 291
9.4.1 Secure Sockets Layer (SSL) – Transport Layer Security (TLS) 291
9.4.2 Secure-HTTP (S-HTTP) 293
9.5 Sécurité du commerce électronique et des paiements en ligne 294
9.5.1 Contexte du commerce électronique 294
9.5.2 Risques particuliers 294
9.5.3 Sécuriser la connexion entre l'acheteur et le vendeur 295
9.5.4 Sécurité des paiements en ligne 296
9.5.5 Sécuriser le serveur 298
9.5.6 Notions de confiance et de contrat dans le monde virtuel 298
9.6 Sécurité des documents XML 300
9.6.1 Risques et besoins de sécurité liés à l'usage de documents XML 300
9.6.2 Signatures XML 300
9.6.3 Chiffrement/déchiffrement XML 302
9.7 Marquage de documents et droits numériques 303
9.7.1 Tatouage numérique 303
9.7.2 Gestion des droits numériques 304
9.8 BYOD, réseaux sociaux et sécurité 306
9.9 Désinformation et mesures de confiance 308
9.9.1. Fabriquer le faux 308

9.9.2 Le faux au service de la rentabilité 309
9.9.3 L'ère de l'opinion et de la post-vérité 309
9.9.4 Mesures pour renforcer la confiance 310
Exercices 312
Solutions 313

Chapitre 10 • La sécurité par la gestion opérationnelle 319
10.1 Intégration des mesures de sécurité 319
10.1.1 Interopérabilité et cohérence globale 319
10.1.2 Une question d'investissement 320
10.1.3 Externalisation 321
10.2 Gestion de systèmes et réseaux 323
10.3 Gestion du parc informatique 324
10.3.1Objectifs et fonctions 324
10.3.2 Quelques recommandations 324
10.4 Gestion de la qualité de service réseau 326
10.4.1 Indicateurs de qualité 326
10.4.2 Évaluation et efficacité 327
10.5 Gestion comptable et facturation 328
10.6 Gestion opérationnelle d'un réseau 329
10.6.1 Gestion des configurations 329
10.6.2 Surveillance et optimisation 330
10.6.3 Gestion des performances 331
10.6.4 Maintenance et exploitation 331
10.6.5 Supervision et contrôle 334
10.6.6 Documentation 334
10.7 Gestion de systèmes par le protocole SNMP 335
10.8 Concilier gouvernance et gestion opérationnelle 337
Exercices 339
Solutions 340

QCM 349

Glossaire 363

Index 385

AVANT-PROPOS

Ce livre offre une synthèse des problématiques et des éléments de solution pour la réalisation de la cybersécurité des systèmes d'information. Il traite de la compréhension des cyberrisques, de la maîtrise de la cybercriminalité et des questions de gouvernance, de gestion stratégique et opérationnelle de la sécurité. Il analyse les principales mesures techniques de la sécurité informatique et des réseaux qui permettent de réaliser des services et des fonctions de la sécurité informatique.

- Le **chapitre 1** introduit les **principes fondamentaux** et les domaines d'application de la sécurité informatique 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'inscrit la sécurité informatique et les besoins de **cyberésilience** sont identifiées pour insister sur la nécessité de doter les individus, les organisations et les États, de moyens suffisants et nécessaires à leur cybersécurité et cyberdéfense. Les métiers de la sécurité informatique, les acteurs, les compétences comme les notions d'organisation, de responsabilité et de mission de sécurité sont présentées.
- 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 numé-

riques, 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** 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 les notions de protection des documents par **tatouage électronique**, la gestion des droits numériques (**DRM**) et les problématiques de sécurité liées à l'usage de l'informatique personnelle (**BYOD**) et des **réseaux sociaux** en entreprise, 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. 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. De nombreuses références, un glossaire des principaux termes ou encore le **corrigé des exercices** contribuent à une meilleure assimilation des thèmes abordés.

Un index conclut 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 **près de 200 exercices corrigés** ainsi que des compléments en ligne **téléchargeables** sur la page associée à l'ouvrage sur le site des éditions Dunod :
www.dunod.com/contenus-complementaires/9782100747344

Remerciements et dédicace

Ce livre est le fruit de mes activités de recherche, d'enseignement et de conseil développées depuis plus d'une trentaine d'années. Il est aussi celui de mes premiers ouvrages entièrement consacrés à la sécurité informatique, à savoir : *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, sans oublier A. L. H. et S. qui m'accompagnent depuis toujours.

Solange GHERNAOUTI
Chevalier de la Légion d'honneur
Docteure 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
Professeure de l'université de Lausanne
Associate fellow, Geneva Center for Security Policy
Membre de l'Académie suisse des sciences techniques
Membre de l'association des réservistes du chiffre et de la sécurité de l'information
www.scarg.org

1 Sécurité informatique et cybersécurité

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.
- Comprendre les champs d'application, les différents aspects et la dimension interdisciplinaire de la cybersécurité.
- Aborder la notion d'architecture de sécurité et d'approche holistique.

1.1 Objectifs de sécurité

1.1.1 Cybersespace 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 cyberespace (l'ensemble des infrastructures numériques, des données et des services mis en réseaux) 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 cyberespace est une pure création de l'être humain qui ne relève pas de la nature.

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, par le mathématicien Norman Wiener aux États-Unis 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 la sécurité informatique, celle de l'information et la sécurité des réseaux, des environnements connectés à Internet. La sécurité des systèmes accessibles *via* le cyberespace peut être mise en défaut, entre autres, par des **cyberattaques**. Ainsi, du fait de l'usage extensif d'Internet, de nouvelles menaces sont apparues générant des risques additionnels dont les impacts, de niveaux d'importance variables, peuvent affecter les individus, les organisations ou 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). Ces critères de base (critères *DIC*) sont réalisés par la mise en œuvre de fonctions et services de sécurité, tels que ceux de contrôle d'accès ou de détection d'incidents par exemple. Des services de sécurité liés à **l'authentification** (notions de authenticité et de véracité) ou encore à la **non-répudiation, à l'imputabilité**, ou à la **traçabilité** contribuent à protéger des infrastructures numériques (figure 1.1).

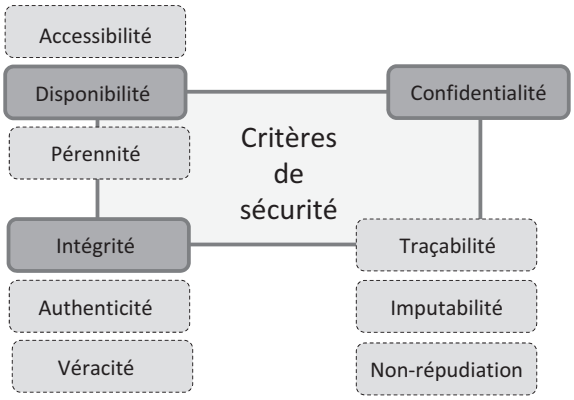

Figure 1.1 – Critères de sécurité.

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 destruction 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 ou si il y a malveillance. Une **politique de sauvegarde** ainsi qu'un arbitrage entre le coût de la sauvegarde et celui du risque d'indisponibilité, supportable par l'organisation doivent être préalablement établis pour que la mise en œuvre des mesures techniques soit efficient.

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 sont l'objet de mesures de sécurité. Ainsi, se prémunir contre l'altération des données et avoir la certitude qu'elles n'ont pas été modifiées collabore à 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 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 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 signé 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 (notion de contrôle d'accès) ;

- 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 permettent 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, d'éviter que des erreurs ne se répètent ou d'identifier des fautifs. Cela autorise par exemple d'analyser le comportement du système et des utilisateurs à des fins d'optimisation, de gestion des incidents et des performances ou encore d'audit. L'enregistrement des actions et événements permet également d'enrichir les bases de données qui permettent de développer des applications de **surveillance**, **de détection et de réaction aux incidents**, en particulier à l'aide des techniques issues de **l'inteligence artificielle**.

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 telle que, par exemple, un mot de passe ou une empreinte biométrique.

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.

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 infrastcrutures 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 règlementations 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 sécurité informatique. En fonction de son domaine d'application, celle-ci peut se décliner en (figure 1.2) :

- sécurité matérielle, physique et environnementale ;
- sécurité logique, sécurité applicative et sécurité de l'information ;
- sécurité de l'exploitation ;
- sécurité des réseaux de télécommunication ;
- cybersécurité.

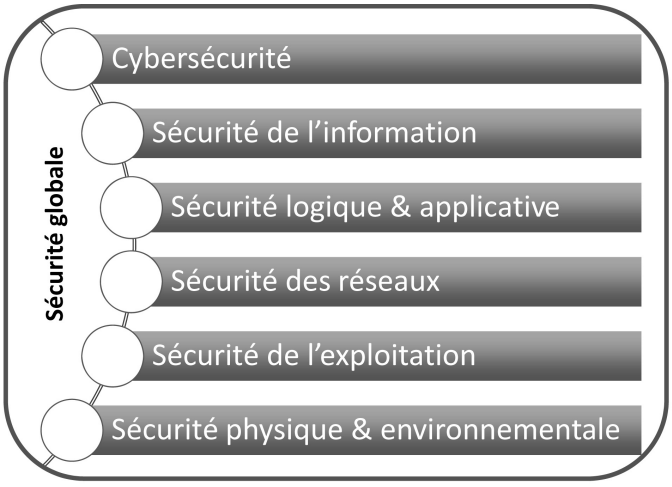

Figure 1.2 – Domaines d'application de la sécurité.

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, nous retiendrons que la sécurité physique repose essentiellement sur :

- la **fiabilité** des matériaux (éléments matériels constitutifs des systèmes) et usage d'équipements qui possèdent un bon degré de **sûreté de fonctionnement**, de fiabilité et de **robustesse** ;
- 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 le retrouver ;
- 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 logique, applicative et de l'information

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

- la qualité 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 logiciels malveillants, de détection d'intrusions et d'incidents ;
- mais aussi sur un dimensionnement suffisant des ressources, une certaine redondance ainsi que sur 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 (***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 ;
- la sécurité des progiciels (choix des fournisseurs, interface sécurité, etc.) ;
- l'élaboration et la gestion des contrats (les relations avec des sous-traitants éventuels comprenant des clauses d'engagement de responsabilité) ;
- un plan de migration des applications critiques ;
- la validation et l'audit des programmes ;
- la qualité 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***).

1.2.3 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 ;

- 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 celles 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 service et à sa facturation.

1.2.4 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 plates-formes 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 **récursivité de la sécurité**).

La sécurité des télécommunications est peu différente de celle que l'on doit mettre en œuvre pour protéger les ordinateurs. Les réseaux télécommunication ne sont pas plus vulnérables que les systèmes d'extrémité ou que les personnes qui les conçoivent, les gèrent ou les utilisent.

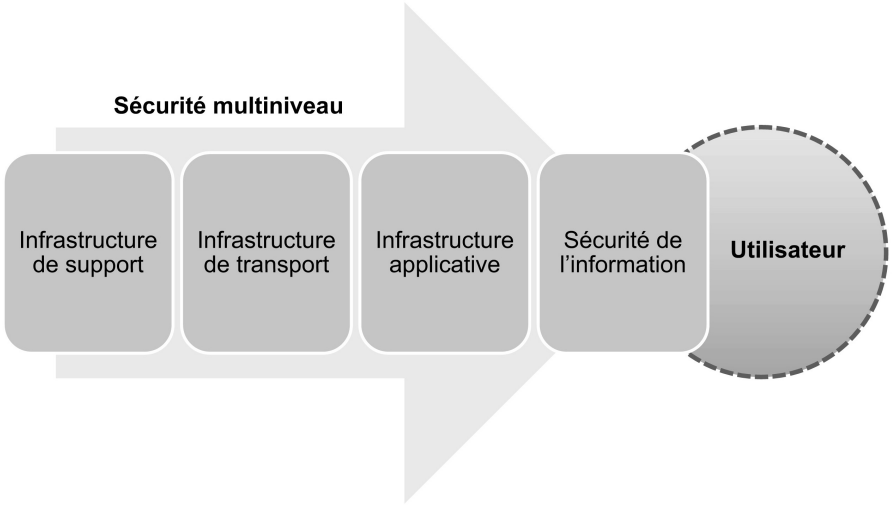

Figure 1.3 – Sécurité des infrastructures de télécommunication.

Un environnement informatique et de télécommunication sécurisé implique la sécurisation de tous les éléments qui le composent. La **sécurité globale** est toujours celle du maillon le plus faible. 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 plates-formes matérielles et logicielles non correctement sécurisées.

L'implantation de mesures de sécurité doit répondre à des besoins de sécurité clairement identifiés à la suite d'une **analyse des risques** spécifiquement encourus par une organisation. Les besoins s'expriment en termes d'exigences de sécurité à satisfaire dans la **politique de sécurité**. De plus, un système 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 au contrôle imposés par le caractère stratégique des enjeux économiques et politiques que doivent satisfaire les systèmes d'information.

La confiance qu'une personne peut accorder à une entité relève du sentiment qui fait qu'elle peut se fier, à tord ou à raison, à cette dernière. **La confiance n'exclut pas le contrôle** ! La sécurité, en tant que propriété d'un système, peut être qualifiable (notion d'assurance de sécurité qui fait référence à la quantification de la qualité de la sécurité).

1.2.5 Cybersécurité

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

Désormais, toutes les activités de la société intègrent un élément de traitement informatisé dont il faut assurer le bon fonctionnement, la cohérence, la sûreté de fonctionnement, la fiabilité, la sécurité et la résilience (figure 1.4).

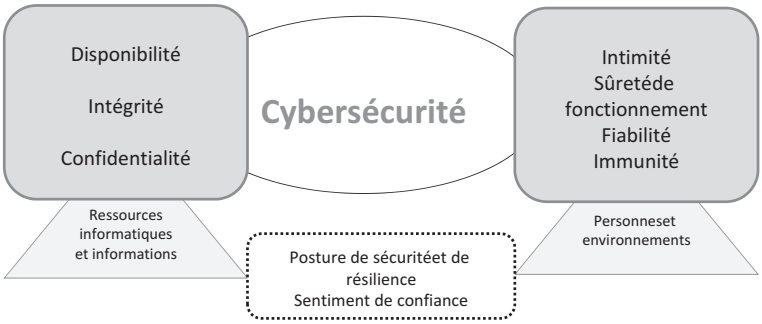

Figure 1.4 – Cybersécurité, posture de sécurité et de résilience.

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 possède un comportement fiable, prévisible, auquel on peut se fier. Sûreté et fiabilité sont des composantes de la sécurité des systèmes qui devraient être immunisés contre des programmes malveillants. Protégés et robustes, les systèmes interconnectés peuvent offrir des services aux utilisateurs, dont les programmes et données sont traités en toute innocuité (qualité de ce qui n'est pas nuisible). Cela permet d'atteindre un certain état de sécurité et de développer la confiance des usagers envers les infrastructures numériques.

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 cyberespace, qui peut toucher tout système connecté à Internet. Sa concrétisation par une **cyberattaque**, 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 à l'usage malveillant des technologies Internet et à la **cybercriminalité**. 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 l'apparition de cybermenaces, 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 conséquences préjudiciables. Toutefois, un risque peut également être porteur d'opportunités et générer des bénéfices pour l'entité qui l'assume.

Un **risque** est un danger plus ou moins prévisible relatif à des menaces et à des vulnérabilités.

L'évaluation d'une menace tient compte de l'ampleur et de l'importance des dégâts qu'elle peut occasionner si elle devient réalité. Cela s'exprime le plus souvent 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, ce qui est parfois difficile. 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. Entre dans cette catégorie, la réception de messages publicitaires, de lettres d'information envoyées sans le consentement initial de l'internaute, de spams (pourriels), surchargeant la boîte aux lettres électronique des usagers, qui se trouvent alors contraints de trier les messages non sollicités de ceux qui les concernent vraiment, de les effacer ou d'effectuer éventuellement des demandes de désabonnement, etc. Cela entraîne des pertes de temps et d'énergie et divers désagréments avec parfois la perte de messages pertinents du fait qu'ils ont été noyés parmi les spams. Le 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 réagir après incident. C'est le cas, par exemple, lorsque des programmes nuisibles se sont installés dans la machine de l'utilisateur et dont la charge de malveillance ne s'est pas encore déclenchée. Il peut s'agir par exemple d'un « cheval de Troie » : une fois installé dans la machine, ce virus permet à des entités externes et hostiles de prendre le contrôle de l'ordinateur infecté pour espionner, voler, détruire des données ou lancer des cyberattaques sur d'autres systèmes.

La réalisation d'une menace de **niveau élevé** de dangerosité entraîne des dysfonctionnements, des dégâts et des coûts fortement préjudiciables au fonctionnement des organisations et de la société.

La figure 1.5 présente un récapitualtif des cybermenaces pouvant porter atteinte au bon fonctionnement d'un pays et de la société.

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

Cybermenaces relatives à :	Impacts potentiels sur :
Des systèmes informatiques contrôlant les infrastructures critiques	Population Économie 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 Le champ de bataille 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
La manipulation de l'information constituant des stratégies d'influence et de guerre phycologique	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, rassemblement, atteinte au moral des troupes, …) Déstabilisation des services de renseignement Atteintes à la démocratie, ingérence étrangère

Figure 1.5 – Exemples de cybermenaces pour un pays.

parfois être anticipée s'il existe une bonne connaissance du contexte, des valeurs à protéger et de leurs vulnérabilités.

Les systèmes informatiques sont vulnérables, du fait de l'existence de failles qui peuvent être exploitées pour effectuer des actions malveillantes. 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. Des logiciels antivirus, même à jour, ne détectent que les virus connus. Ils ne sont d'aucune utilité pour de nouveaux virus.

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 alors nécessaire de pouvoir définir le paramètre de **probabilité d'occurrence** en classant cette probabilité en différents niveaux comme :

- la menace ne devrait pas se concrétiser ;
- la menace pourrait bien se concrétiser ;
- la menace devrait se concrétiser ;
- la menace va se concrétiser et se concrétiser à plusieurs reprises.

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, télécom et téléphonie, stockage, services, intelligence artificielle, etc.). Certains fournisseurs sont devenus des géants incontournables de l'Internet ou 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 et à leurs capacités à pouvoir réaliser des actions d'intelligence économique, de surveillance, d'espionnage ou encore de « manipulation » des échanges et cela à l'échelle mondiale.

L'assujetissement et la grande dépendance d'un pays à des fournisseurs et infrastrcutures numériques étrangers posent des problèmes liés à sa **perte de 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**. Il est vrai que cette question de 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 **cyberespionnage** 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, etc.) qui peuvent relever de **phénomène d'addiction**.

Lutter contre l'illettrisme numérique ou contre les différentes formes de domination culturelles et économiques qui s'imposent au travers du cyberespace est nécessaire. 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 devrait être par exemple, accompagné par des enseignements issus des sciences politique, économique, juridique et sociale. Décoder ce qui se passe derrière l'écran est tout aussi primordial, voire plus important que d'apprendre à coder ou d'apprendre à utiliser un équipement informatique. Seule une éducation de qualité, qui traite également des questions éthiques et philosophiques, 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'enjeux est majeur car, *in fine*, il s'agit de s'assurer que l'humain ne devienne pas un robot de chair et de sang, dépossédé de ses capacités mentales,