RÉPUBLIQUE
FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

CYBER EN JEUX

# Former à la cybersécurité

Livret enseignant

# SOMMAIRE

## Introduction

Le présent livret est constitué de 13 fiches thématiques, mises à disposition des enseignants en vue de les aider à acculturer les élèves aux enjeux de cybersécurité dans le cadre d'un temps de formation dédié, avant ou en parallèle de la phase de création de jeux. Ces fiches, destinées à un public adulte, peuvent être partagées, à la discrétion de l'enseignant, avec les élèves.

**Le contenu des fiches cybersécurité a été pensé pour synthétiser, simplifier et accélérer l'accès à des enjeux de la cybersécurité.**

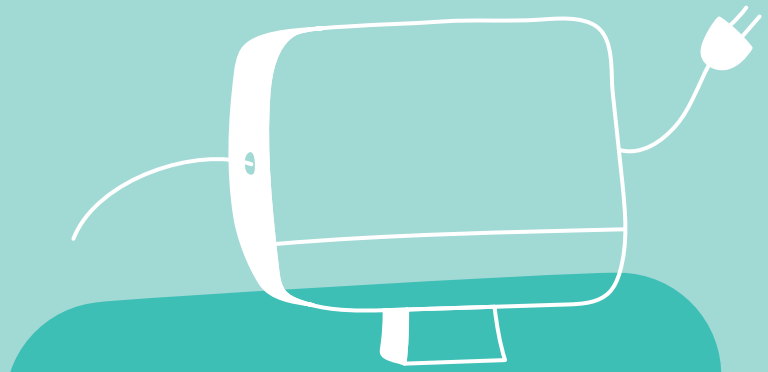
Chaque fiche pédagogique est déclinée en une carte « objectifs cybersécurité ». L'ensemble des cartes est destiné aux élèves en vue de les aider à choisir les thématiques des jeux qu'ils choisiront de créer.

2 cartes peuvent être, par exemple, tirées au hasard ou choisies par l'enseignant ou les élèves eux-mêmes. Un jeu ne devrait pas couvrir plus de deux à trois objectifs.



FICHE

1



# Le cyberespace

# 1 L'essor du numérique, vers l'infini et au-delà !

Parler de cybersécurité, c'est d'abord s'intéresser à ce qu'il faut protéger dans « l'espace numérique », que l'on pourrait résumer à l'ensemble des équipements (téléphones, ordinateurs, tablettes), infrastructures informatiques et réseaux à l'échelle de la planète, également appelé « cyberespace ».

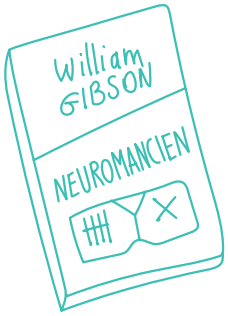
À partir des années 1960-1970, l'apparition des premiers réseaux à des fins militaires ou de recherche (*Arpanet* aux États-Unis, *Cyclades* en France) a conduit à l'émergence d'internet tel que nous le connaissons aujourd'hui.

**L'essor du numérique a depuis bouleversé le fonctionnement de nos sociétés et de l'économie, des usages et du quotidien, notamment à l'échelle :**

- **Individuelle, avec l'apparition des téléphones intelligents, des ordinateurs, des tablettes, etc.** Ces technologies permettent l'accès à la connaissance et à la culture, aux jeux, aux réseaux sociaux, aux films et aux séries, aux services publics en ligne, aux sites marchands, au *Cloud* et, de plus en plus, aux objets connectés (matériel sportif, balances, chauffage, etc.).
- **Des entreprises, avec le passage au « tout numérique »** (postes de travail, processus internes, relations clients, méthodes de production et de distribution, etc.), des plus petites et moyennes entreprises aux plus grands groupes, tous secteurs confondus. Parmi ces entreprises, certaines sont considérées comme « vitales » ou « critiques » pour le fonctionnement de la nation (télécommunications, énergie, santé, finance, etc.).
- **Des administrations, avec notamment l'essor du numérique** dans leur relation avec les citoyens, grâce aux services publics en ligne.



# 2 Le « cyberespace »




**Imaginé par l'auteur de science-fiction William Gibson dans son livre *Neuromancien* (1983), le concept de « cyberespace » est aujourd'hui utilisé pour décrire l'ensemble des infrastructures, des technologies et des services numériques de par le monde, dont le principal : le réseau internet.**

Il possède également une dimension fortement géopolitique. Pour certains États, le cyberespace est devenu un espace de confrontation à part entière pour les armées, à l'image d'autres espaces tels que la terre, la mer ou l'air.

D'un point de vue plus technique, le « cyberespace » est souvent représenté sous forme de couches.

**Une couche « sémantique »**

L'ensemble des informations, des contenus générés, stockés, partagés : photos, vidéos, mails, etc.

**Une couche « logicielle »**

Les systèmes d'exploitation permettant aux utilisateurs d'accéder aux fonctionnalités d'un ordinateur ou d'un téléphone, ainsi que l'ensemble des logiciels comme les applications mobiles.

**Une couche « matérielle »**

Les câbles sous-marins, terrestres, les infrastructures de l'internet mais aussi l'ensemble des équipements connectés (serveurs, ordinateurs, téléphones, tablettes, etc.).

FICHE

2

# Les systèmes et les données à protéger

# 1 Deux notions incontournables

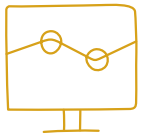
**Les systèmes d'information :** l'ensemble des ressources informatiques permettant de traiter et de diffuser de l'information dans le monde numérique. Un ordinateur, un téléphone, une montre connectée, un serveur, le réseau interne d'un établissement scolaire comme le réseau mondial d'une entreprise sont donc des systèmes d'information.
**Du concept de « systèmes d'information » découle celui de « sécurité des systèmes d'information » très proche de celui de cybersécurité.**

**Les données :** l'ensemble des informations numériques créées, traitées, stockées, sauvegardées, mais aussi accessibles, partageables, diffusables.

# 2 Ce qu'il faut protéger

Se poser la question des systèmes d'information et des données à protéger implique de s'interroger sur leur importance pour une entité ou une personne donnée. **On peut citer, par exemple :**

**Les données à caractère personnel** d'un individu (par exemple : nom, prénom, adresse, numéro de téléphone, email, conversations privées, photos, données bancaires, etc.) dont l'utilisation à des fins malveillantes ou simplement par négligence expose à de nombreux risques : utilisation abusive des données à des fins commerciales, atteinte à la réputation, fraude ou extorsion, usurpation d'identité, etc.



**Les systèmes d'information et les données des entreprises, des universités ou encore des collectivités, essentiels à leur fonctionnement et pouvant être sensibles.** Une atteinte aux systèmes et aux données pourrait porter préjudice à leur bon fonctionnement ou à la compromission de secrets. À la clé, l'interruption de tout ou partie de leur activité, parfois des pertes de chiffre d'affaires, une atteinte à la réputation…

**Les systèmes d'information des opérateurs publics et/ou privés d'infrastructures critiques**, gérant des installations jouant un rôle parfois vital dans le fonctionnement de la nation, comme dans les secteurs de l'énergie, des transports, des télécommunications.

**Les informations classifiées de l'État**, à savoir les informations les plus sensibles, dont la divulgation pourrait porter préjudice à la sécurité nationale.

3

## Un environnement numérique de plus en plus complexe

Deux tendances contribuent aujourd'hui à rendre l'espace numérique plus complexe à comprendre, à gérer et à protéger :

- **Le monde numérique est de plus en plus dans les nuages !**
  Autrefois, protéger un réseau informatique et les ordinateurs qui y étaient connectés consistait avant tout à sécuriser les portes d'entrée et de sortie vers internet d'une organisation, dont le système d'information était le plus souvent installé dans ses locaux. Avec le développement du travail à distance, l'interconnexion croissante des entreprises (etc.), le numérique est devenu un immense **écosystème** interdépendant d'acteurs, de services, d'équipements. Cela est notamment rendu possible par le développement de l'informatique en nuage (*Cloud*) rendant accessibles à distance de nombreux services et permettant l'accès à des données localisées à plusieurs endroits en même temps sur la planète.

- **La multiplication des acteurs impliqués dans la fourniture de matériel et de services numériques** (la chaîne d'approvisionnement), incluant de nombreux sous-traitants, fournisseurs ou intégrateurs, ayant tous un rôle à jouer dans la sécurisation des systèmes et des données. Faire en sorte que chacun assume sa part de responsabilité dans la sécurisation des systèmes d'information n'est pas toujours évident ! Or, chaque maillon de la chaîne non sécurisé la rend plus vulnérable.



FICHE 3

# La cybersécurité

# 1 Définition

La cybersécurité désigne l'ensemble des **activités** visant à protéger les **données** et **l'ensemble des « systèmes d'information »** contre les menaces issues du cyberespace, susceptibles de compromettre leur **disponibilité**, leur **intégrité** ou leur **confidentialité**.

### Disponibilité

La disponibilité est la capacité à accéder à des données ou à un service au moment souhaité. Elle peut être, par exemple, compromise par la destruction (effacement de données), le chiffrement (les informations deviennent illisibles à moins de posséder la clé de déchiffrement) ou encore par l'interruption d'un service. Un ordinateur peut devenir inaccessible si un logiciel malveillant chiffre l'ensemble des données qu'il contient.

### Intégrité

L'intégrité est la propriété garantissant que des données sont exactes, complètes et n'ont pas été modifiées. L'intégrité peut être compromise par la modification du contenu d'un fichier. Par exemple, l'intégrité des notes d'élèves sur un espace numérique de travail est compromise si ses notes sont modifiées par une personne n'ayant pas le droit de le faire.

### Confidentialité

La confidentialité est la garantie que des données, des services ou tout autre bien ne sont accessibles qu'aux personnes autorisées. La confidentialité est compromise dès lors qu'une personne non autorisée accède à des données ou tout autre bien sans en avoir le droit. Par exemple, si une personne parvient à ouvrir un téléphone mobile et à accéder aux informations contenues dedans.



# 2 Prévenir et répondre

La cybersécurité recouvre schématiquement **deux dimensions principales**.

### La prévention

La prévention correspond à l'ensemble des mesures permettant de renforcer la sécurité d'un système d'information pour lui permettre de résister aux attaques susceptibles de menacer les données et les services auxquels il permet d'accéder.

**La prévention passe principalement par :**

- La mise en place de mesures de sécurité adaptées notamment au niveau technique, comme le fait de sauvegarder régulièrement les données dans un environnement distinct et sécurisé ou encore de chiffrer de bout-en-bout des conversations via une messagerie.
- La sensibilisation des personnes aux risques et aux bonnes pratiques de sécurité informatique pour éviter que des erreurs ou des négligences facilitent le travail des attaquants, par exemple, en affichant son code PIN au dos de son téléphone.
- Pour aller plus loin, l'analyse approfondie des risques pour un système d'information ou pour une organisation permettant d'identifier des mesures de sécurité complémentaires renforçant leur sécurité.

### La réaction

La réaction correspond à l'ensemble des moyens et des activités permettant de détecter et de répondre aux cyberattaques en vue de les stopper et de revenir à un mode de fonctionnement normal.

**La réaction aux cyberattaques passe notamment par :**

- La détection des cyberattaques.
- La réponse à incident, par la mobilisation d'équipes techniques (les CSIRT).
- La gestion d'une crise d'origine cyber au sein d'une organisation.
- La reconstruction des systèmes d'information infectés.
- La lutte contre les cybercriminels.

3

# Les acteurs de la cybersécurité en France

Assurer la cybersécurité des administrations, des citoyens et des entreprises est une tâche immense. Des acteurs publics et privés y travaillent d'arrache-pied 7j/7, 24h/24. Parmi ces acteurs, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) joue un rôle central en matière d'expertise, de réponses aux attaques et de coordination.

Relevant des services du Premier ministre, l'ANSSI est l'autorité nationale en matière de cybersécurité et de cyberdéfense.

Elle œuvre à la prévention des cyberattaques contre l'État, les opérateurs les plus critiques de la nation et au-delà de l'ensemble de l'économie et de la société. Elle participe également à détecter et à répondre aux cyberattaques. Chaque année, l'ANSSI gère plusieurs crises majeures d'origine cyber. L'ANSSI joue également un rôle central dans l'animation de l'action publique en matière de cybersécurité.

Elle peut compter pour cela sur plusieurs centaines d'agents disposant d'une expertise technique, opérationnelle et stratégique de haut niveau.



FICHE

4

# Les sources de menaces

## 1
# Les quatre dimensions de la menace cyber

Une menace cyber est toujours composée de 4 éléments principaux :

- **Un attaquant ou un groupe d'attaquants** aux profils divers.
- **Un ou plusieurs objectifs** correspondant aux motivations de l'attaquant.
- **Une cible** (personne, organisation, etc.) qui peut être le système d'information et/ou les données visées d'une victime.
- **Une cyberattaque** ou un mode opératoire qui désigne les étapes et les opérations que mène l'attaquant pour atteindre son objectif.

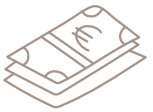
## 2
# Les principaux profils d'attaquants

**Les amateurs, sans compétence particulière** (connus sous l'appellation *« script-kiddies »*) sont des attaquants disposant d'une faible expertise. Ils ont le plus souvent recours à des outils disponibles sur internet et facilement téléchargeables. **Leur motivation est ludique, récréative** (« pour s'amuser »).

**Les attaquants « vengeurs » ou « malveillants », souvent isolés dont la motivation est personnelle voire affective.** Par exemple, une revanche contre un ex-employeur.

**Les cyberhacktivistes** (fusion de *hacker* et activiste), soit tout type d'attaquant agissant selon des **motivations d'ordre idéologique, politique, etc**.

**Les attaquants expérimentés** dont la **motivation est essentiellement technique**.

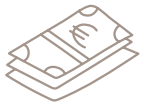


**Les cybercriminels organisés et les mercenaires** travaillant à leur compte ou pour celui d'une autre organisation criminelle. Leur **motivation est principalement lucrative** (financière).

**Les acteurs étatiques**, dotés de moyens souvent importants et aux **motivations multiples. Elles peuvent être de nature stratégique**, en fonction des intérêts d'un État et peuvent parfois poursuivre un dessein offensif.

## 3
# Les objectifs des attaquants

**Le défi, l'amusement**, visant à réaliser un exploit à des fins de reconnaissance sociale, de défi ou de simple amusement. Même si l'objectif est essentiellement ludique ce type d'opération peut avoir de lourdes conséquences pour la victime.



**La cybercriminalité à des fins lucratives** désigne les attaques visant à retirer un avantage pécuniaire d'activités cyber malveillantes. Ex. : le recueil illicite de coordonnées bancaires, etc.

**L'influence, l'agitation** consistant à agir sur le champ de l'information, souvent à l'initiative de cyberhacktivistes : détournement de comptes sur les réseaux sociaux, défiguration de sites internet, etc.

**L'espionnage** a pour objectif l'exfiltration d'informations stratégiques, de secrets industriels ou étatiques.

**Le pré-positionnement stratégique** consiste à se positionner discrètement dans un réseau informatique sans volonté d'agir immédiatement, par exemple pour préparer une attaque future, sans que la finalité poursuivie soit toujours évidente.

**L'entrave au fonctionnement, par des opérations de sabotage, de neutralisation** désigne les attaques dont l'objectif est de rendre indisponible un système d'information et des données, par la saturation (par exemple, des attaques par « déni de service » pouvant rendre inaccessible un site internet ou encore les « rançongiciels ») voire par la destruction physique de matériel (par exemple : tromper des instruments de mesure dans les installations d'un opérateur d'infrastructure critique afin d'empêcher les mécanismes d'alarme de se déclencher et aller jusqu'à la destruction du système).

## 4 Le jeune à capuche : le profil pas si courant

L'attaquant cyber est souvent décrit dans les films et les médias comme un « hacker » se résumant à un « jeune » isolé, portant un sweat à capuche et agissant tard dans la nuit pour « pirater la CIA » depuis l'ordinateur de sa chambre.

- Si l'attaquant isolé agissant depuis sa chambre constitue bien une catégorie réelle, celle-ci est caricaturale, négligeable en termes d'impact. La réalité de la menace est aujourd'hui davantage celle de groupes d'attaquants professionnels, agissant sur leurs heures de travail.

- Le terme « hacker » est, par ailleurs, à tort, associé aux seuls acteurs malveillants. Pourtant, celui-ci renvoie historiquement à une culture positive de la « débrouille », du « partage » et de « l'amélioration » dans des domaines comme l'informatique mais également l'électronique, la menuiserie, la mécanique, etc. Par souci de distinction avec les acteurs malveillants, on parle désormais de « hackers éthiques ».



FICHE 5

# Les cyberattaques

Une cyberattaque désigne l'ensemble des étapes, des ressources et des actions utilisées par un attaquant pour atteindre son objectif. Afin de mener son attaque, un attaquant tire partie de vecteurs d'attaque en vue d'exploiter des vulnérabilités.

## 1 Les vecteurs d'attaque

Trois vecteurs (chemins, points d'entrée) peuvent être utilisés voire associés afin de conduire une attaque.

### Humain

Les personnes sont les premiers vecteurs d'attaque. En ayant recours à des techniques dites « d'ingénierie sociale », les attaquants peuvent, par exemple, avoir recours au hameçonnage (ou *phishing*) pour tromper la vigilance de leur cible (voir ci-dessous les « grands types d'attaques »). Une autre manière de procéder est de laisser traîner des clés USB infectées par un code malveillant, en pariant sur le fait que des salariés négligents les ramassent et les connectent au réseau de l'organisation.

### Informatique

Il existe d'autres vecteurs d'attaque comme des techniques informatiques et des codes malveillants pouvant nuire à un système informatique.

### Physique

S'introduire dans une pièce (salle serveur ou bureau par exemple), sectionner des câbles, voler un serveur (etc.) sont d'autres moyens physiques permettant d'accéder à un système d'information ou de l'endommager.



## 2 Les vulnérabilités

Les cyberattaques exploitent des vulnérabilités, soit **une ou plusieurs failles repérées dans un système**.

En matière de cybersécurité, l'enjeu est de les identifier et de les corriger. Ces vulnérabilités peuvent être de différentes natures :

- Une vulnérabilité au sein d'un équipement ou du code d'un logiciel, présente par négligence ou introduite dès la conception de manière involontaire. Ces vulnérabilités peuvent être corrigées par la mise en œuvre d'un correctif de sécurité.
- Les vulnérabilités liées à l'absence de sensibilisation des utilisateurs, l'absence de prise en compte du risque cyber.

## 3 Trois exemples de cyberattaques

### Rançongiciel

Les cyberattaques reposant sur l'utilisation de logiciels malveillants (*malware* en anglais, contraction des mots « *malicious* » et « *software* ») qui regroupent tous les codes et les programmes informatiques malicieux, qui peuvent être dangereux pour les systèmes d'information. La plus courante est le rançongiciel (*ransomware* en anglais), contraction des mots « rançon » et « logiciel ». C'est une cyberattaque consistant à installer un programme malveillant, si possible sur le maximum d'équipements du système d'information de la victime, dans le but d'obtenir de celle-ci le paiement d'une rançon. Pour y parvenir, le rançongiciel va empêcher les utilisateurs d'accéder à leurs données (photos, fichier client, etc.).

## DDOS

**Les attaques par déni de service distribué** (*denial of service* en anglais) visent à rendre indisponible un ou plusieurs services. Pour ce faire, un nombre trop important de requêtes peut être adressé au dit service (site web, service de résolution de noms, etc.), le rendant inaccessible à d'autres utilisateurs. On parle de déni de service distribué (*destributed denial of service* ou DDoS) lorsque l'attaque prend appui sur un réseau de machines « zombies » préalablement manipulées à l'insu de leur propriétaire. Ces réseaux peuvent être composés de serveurs, d'ordinateurs ou encore d'objets connectés à internet comme des caméras de vidéosurveillance. Lorsqu'ils sont composés de machines compromises, on parle de « *botnets* ».

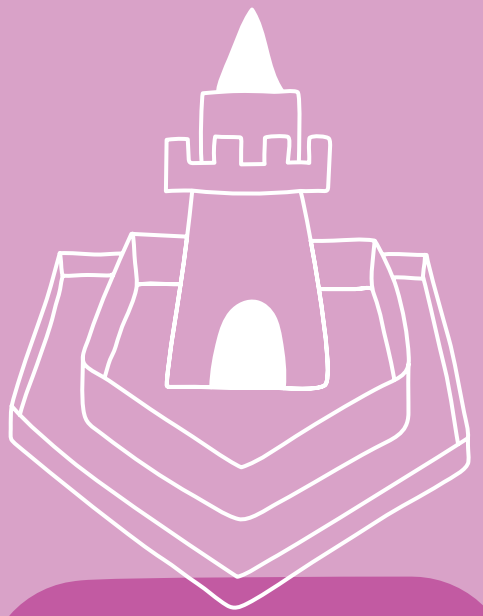
## APT

**Les cyberattaques persistantes** (*Advance Persistent Threat* en anglais, ou APT) sont des attaques plus sophistiquées, à la portée d'acteurs malveillants disposant de compétences et/ou de ressources leur permettant de pénétrer en profondeur dans un réseau. Ces attaques sont principalement menées à des fins d'espionnage économique, industriel ou scientifique.



FICHE

6



# Les bonnes pratiques de sécurité informatique

Des mesures de protection sont nécessaires afin de prévenir les cyberattaques et de se préparer à y répondre. Parmi les nombreuses mesures susceptibles d'être mises en œuvre, certaines sont communes à tous les individus et à toutes les organisations.

## 1 Exemples de mesures essentielles pour les individus

1. **Utiliser des mots de passe robustes :** pour l'accès à un téléphone ou à un ordinateur en choisissant des mots de passe longs et complexes (au moins 12 caractères), tout en évitant les mots du dictionnaire, les dates de naissance et autres informations faciles à deviner. Autant que possible, utiliser un gestionnaire de mots de passe de confiance et dès que possible mettre en place des sécurités additionnelles pour accéder aux comptes (mails, réseaux sociaux) comme la « double authentification » (impliquant deux vérifications consécutives avant de permettre l'accès à un service), afin d'éviter qu'une personne non autorisée y accède.

2. **N'utiliser que des logiciels officiels et à jour** (par exemple, issus des bibliothèques d'application mobiles officielles) et mettre à jour ces logiciels (système d'exploitation d'un ordinateur, logiciels de bureautique, applications mobiles), afin notamment d'éviter que les vulnérabilités de logiciels obsolètes soient utilisées pour mener une attaque et pénétrer dans un système d'information.

3. **Effectuer des sauvegardes régulières** des systèmes et des données, si possible sur d'autres appareils (par exemple un disque dur, un serveur) déconnectés, pour pouvoir les récupérer, dans le cas où ces dernières seraient détruites ou rendues inaccessibles, en cas d'attaque par rançongiciel, par exemple.

4. **Utiliser des réseaux sécurisés**, notamment wifi, en évitant les réseaux sans mot de passe et sécuriser l'accès wifi d'un foyer ou d'une entreprise.

5. **Être autant prudent avec un smartphone et une tablette qu'avec un ordinateur et bien séparer les usages personnels et professionnels.**

6. **Prendre soin de ses informations personnelles, professionnelles, de son identité numérique.** Penser notamment à chiffrer les données – la plupart des ordinateurs permettent de chiffrer le disque dur – à savoir les rendre illisibles aux personnes qui y auraient accès mais ne pourraient pas les « déchiffrer ».

## 2 Ressources

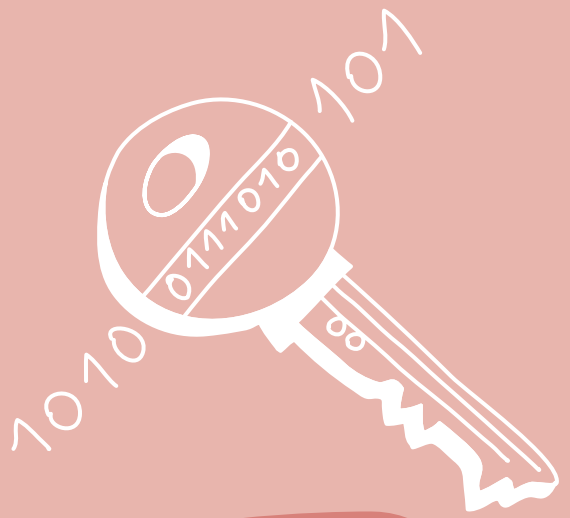
Pour les particuliers, voir les bonnes pratiques recommandées sur la plateforme cybermalveillance.gouv.fr.

Pour les petites et moyennes entreprises (TPE/PME) voir le guide des bonnes pratiques de l'informatique : *La cybersécurité pour les TPE/PME en 13 questions*.

Pour aller plus loin, consulter *Le guide d'hygiène informatique* édité par l'ANSSI.



FICHE 7




# La cryptographie

## 1
## Chiffrer pour protéger

**La cryptographie est l'ensemble des procédés permettant de transformer une donnée lisible par tous (dite « en clair ») comme une photo, en une donnée « chiffrée » compréhensible seulement de celles et ceux disposant d'une « clé » pour la déchiffrer** (une clé de déchiffrement). Les données sont chiffrées grâce à des algorithmes de chiffrement, qui sont des suites mathématiques.

Grâce à ce procédé, deux personnes peuvent échanger de manière confidentielle et sécurisée, pourvu qu'elles possèdent la clé leur permettant de chiffrer et de déchiffrer leurs messages.

**La cryptographie est l'un des piliers historiques de la cybersécurité. Elle permet notamment de protéger les informations les plus sensibles** de l'État, des entreprises, des centres de recherche. Le chiffrement joue également un rôle central dans de nombreux autres usages numériques en permettant, par exemple, de protéger les données d'utilisateurs navigant sur internet et accédant à des services en ligne.

## 2
## Aux origines : une histoire des codes secrets

En 50 avant J.-C. : le chiffre de **César** est l'un des chiffres de substitution que Jules César (100-44 av. J.-C.) avait coutume d'employer dans ses récits et ses correspondances. Il consiste à substituer une lettre par une autre en décalant l'alphabet de trois places vers la droite.

| Message d'origine | B | O | N | J | O | U | R |
|---|---|---|---|---|---|---|---|
| Numéro de la lettre dans l'alphabet | 2 | 15 | 17 | 10 | 15 | 21 | 18 |
| Numéro augmenté de 3 | 5 | 18 | 17 | 13 | 18 | 24 | 21 |
| Lettre correspondante | E | R | Q | M | R | X | U |



Au XVI[e] siècle, le diplomate français **Blaise Vigenère** invente une nouvelle méthode de chiffrement, le chiffre de Vigenère. Beaucoup plus solide que le chiffre de César, cette méthode a seulement été élucidée en 1863 ! Elle est restée efficace pendant trois siècles !

1975-2000 : le *Data Encryption Standard* (**DES**) est un algorithme de chiffrement symétrique standardisé en 1976. Il utilisait alors une clé de chiffrement de 56 bits, jugée à l'époque suffisante pour prémunir les entreprises du risque d'espionnage industriel, ce qui n'est plus le cas aujourd'hui. En 2000, DES cède la place à l'algorithme *Advanced Encryption Standard* (**AES**), encore en usage aujourd'hui et dont les propriétés, parmi lesquelles des clés d'au moins 128 bits, offrent un niveau de sécurité bien plus grand.

## 3
## Chiffrer soi-même un message : un exemple

Bob et Alice sont en classe. Ils n'ont plus leur téléphone portable et veulent s'envoyer un message sans que personne ne puisse le lire. Bob « chiffre » son message grâce au code CESAR (ci-dessous) et le transmet en le faisant passer de main en main jusqu'à Alice. Alice est au courant de la façon dont Bob a chiffré son message et parvient à le déchiffrer !

| Message d'origine à chiffrer | Méthode de chiffrement | Message chiffré |
|---|---|---|
| On mange ensemble ce midi ? | CESAR avec un décalage de 3 lettres dans l'alphabet.<br>ABCDEFGHIJKLMNO PQRSTUVWXYZ<br>=<br>DEFGHIJKLMNOPQRS TUVWXYZABC | Rq pdqjh hqvhpeoh fh plgl ? |

De nombreux sites internet en ligne permettent de s'exercer simplement au chiffrement et au déchiffrement de messages.

## 4

## Cryptologie, cryptanalyse, cryptographie : quelles différences ?

La **cryptologie** est la *science du secret*. Elle comporte 2 branches :

- La **cryptographie**, décrite dans cette fiche.
- La **cryptanalyse**, qui est l'étude de systèmes cryptographiques permettant de chiffrer des données afin d'en évaluer la robustesse, par la recherche de failles, par exemple ou pour parvenir à lire des données chiffrées, lorsque l'on ne dispose pas de la clé de déchiffrement.

## 5

## On dit, on ne dit pas !

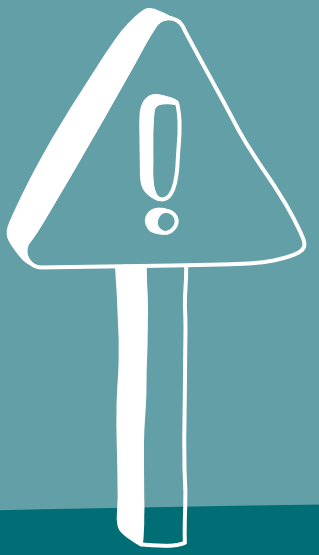
**On peut dire :** chiffrement, chiffrer, puis déchiffrer (lorsque l'on a la clé de chiffrement). On parle aussi de décrypter, lorsque l'on cherche à accéder, par des moyens de cryptanalyse, à une information chiffrée sans avoir la clé de déchiffrement, comme quelqu'un qui tenterait de rentrer de force dans une maison sans en avoir la clé.

**On ne dit pas :** cryptage, encodage, crypter, coder, encoder…



FICHE

8



# La gestion des risques cyber

## 1
## Qu'est-ce qu'un risque cyber ?

Les individus comme les organisations – entreprises privées, administrations, associations – sont exposés à des risques de cyberattaques : on parle couramment de risques cyber.

La nature de ces risques diffère d'une organisation à une autre, d'un secteur d'activité à un autre, en fonction de leurs spécificités, des motivations des attaquants. Ces risques varient également en termes de gravité dans l'hypothèse où ceux-ci viendraient à se réaliser. Par exemple :

- une attaque informatique contre le système de gestion des feux de signalisation d'une ville pourrait gravement perturber la circulation routière ;
- la défiguration visible du site interne d'une commune aurait, par comparaison, des conséquences moins graves.

## 2
## Comment faire face aux risques cyber ?

Faire face aux risques cyber consiste, pour une organisation, à anticiper les risques susceptibles de peser sur elle en vue de choisir :

- les risques contre lesquels elle souhaite se protéger en identifiant les mesures de sécurité à mettre en œuvre pour diminuer ses vulnérabilités et réduire ainsi la probabilité que ces risques se réalisent ;
- les risques que l'organisation est prête à accepter de prendre : ce sont les risques « résiduels ».

Pour « manager les risques », la méthode EBIOS Risk Manager – développée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) – permet aux organisations d'identifier l'ensemble des risques. Dans le cadre de cette méthode, elles peuvent être amenées à suivre plusieurs étapes importantes :

- Identifier les données et les processus à protéger et les évènements redoutés susceptibles de leur porter atteinte, leurs impacts et leur gravité.
- Identifier les sources de risques (par exemple des attaquants, des concurrents), qui pourraient conduire à vouloir porter atteinte à ces données ou ces processus.
- Imaginer, à un niveau stratégique, par quel chemin ces risques pourraient se concrétiser, nécessitant de bien connaître le système d'information de l'organisation et de l'ensemble de ses parties prenantes, comme ses sous-traitants.
- Imaginer ensuite comment un attaquant peut conduire son attaque au niveau tactique.
- Définir les mesures de sécurité à mettre en place pour corriger les vulnérabilités identifiées et réduire la vraisemblance que ces risques se produisent.

## 3
## Exemple fictif d'analyse de risque dans le cadre d'un établissement scolaire

**ÉTAPE 1** – LES DONNÉES/PROCESSUS À PROTÉGER

| Données/processus | Évènement redouté, impact, gravité. |
|---|---|
| Les notes et les données personnelles des élèves. | L'intégralité des notes est supprimée ou quelques notes sont modifiées (à la hausse ou à la baisse). Impact significatif pour la délivrance des bulletins de note. |
| La gestion des emplois du temps. | Les emplois du temps et les numéros de salle de classe sont modifiés plusieurs fois, ce qui empêche ou perturbe la tenue des cours. Impact grave bouleversant le déroulé des cours. |
| Les accès internet de l'établissement, y compris pour les élèves. | L'ensemble des ordinateurs sont bloqués, rendant impossible la réalisation de certains cours nécessitant du matériel informatique, les agents sont incapables de travailler. Impact significatif empêchant certains cours de se dérouler. |

## ÉTAPE 2 – LES SOURCES DE RISQUES

| Sources de risques | Objectifs visés |
|---|---|
| Des cybercriminels diffusant aléatoirement sur internet un logiciel malveillant de type rançongiciel infectent, par hasard, l'établissement scolaire. | Obtenir un versement d'argent. |
| Des élèves perturbent l'informatique de l'établissement. | Loisir, découverte. |
| Des élèves insatisfaits de leurs notes. | Modifier leurs notes à la hausse ou celles des autres à la baisse. |

## ÉTAPE 3 – LES SCÉNARIOS STRATÉGIQUES

- Les élèves ou le personnel de l'établissement accédant à internet infectent, par mégarde, un ou plusieurs ordinateurs de l'établissement.
- L'un des services numériques en ligne (par exemple, une plateforme pédagogique) utilisé par l'établissement comporte une vulnérabilité utilisée par des attaquants qui obtiennent accès aux données d'organisations utilisant ces services, dont celles de l'établissement.
- Un prestataire de maintenance informatique est attaqué pour parvenir à atteindre, dans un second temps, l'établissement.

## ÉTAPE 4 – LES SCÉNARIOS OPÉRATIONNELS

- Une pièce jointe piégée est ouverte en accédant à son interface mail depuis un ordinateur de l'établissement.
- Une clé USB infectée est introduite par l'un des prestataires de l'établissement à son insu. Un attaquant infecte un site internet de l'établissement (par exemple le site des emplois du temps) afin d'infecter les machines des élèves et des enseignants qui le visitent (attaque dite par « point d'eau »).

## ÉTAPE 5 – LE TRAITEMENT DU RISQUE

Mise en place de mesures de sécurité pour corriger les vulnérabilités qui pourraient être exploitées par un attaquant pour mener à bien son attaque.



FICHE 9

# Détecter les cyberattaques

## 1 La détection

**Réagir face à une cyberattaque suppose de savoir qu'une attaque est bien en train de se dérouler.** Et rien n'est moins simple, tant les attaquants peuvent se faire discrets et les attaques ne pas causer de dommages visibles.

**Pour cela, la « détection des cyberattaques » est une activité clé de la cybersécurité.** Elle repose sur des dispositifs techniques, en particulier les « sondes de détection » permettant de détecter des « signatures d'attaques » à savoir des traces de cyberattaques déjà rencontrées par le passé ou des comportements anormaux, par exemple, un ordinateur utilisé un dimanche alors que les locaux d'une entreprise sont fermés...

L'existence d'un dispositif de détection ne garantit pas de tout voir et peut même parfois se tromper. On distingue :

- Les **faux positifs** qui correspondent à des activités légitimes détectées comme malveillantes.
- Les **faux négatifs** qui correspondent à des activités malveillantes détectées comme légitimes.

## 2 L'avantage aux attaquants

La difficulté à détecter les attaques et les attaquants est d'autant plus complexe qu'il existe une asymétrie entre les attaquants et les personnes en charge de la cybersécurité, au bénéfice des premiers. Plusieurs raisons concourent à cela :

- **Une attaque informatique n'est pas en soi « visible »** à moins que les conséquences de l'attaque le soient (par exemple la destruction de données, le sabotage) ou que les attaquants ne soient pas discrets par incompétence. Cette « discrétion » des attaques joue en faveur des attaquants.

- **Les outils et les techniques mobilisables par les attaquants sont très nombreuses et parfois inconnues des défenseurs.** Les attaquants peuvent, par exemple, exploiter des vulnérabilités de systèmes d'information qui ne sont pas encore connues (vulnérabilités dites « 0-day »).

- **Le cyberespace mondialisé permet aux acteurs malveillants d'attaquer des systèmes depuis l'autre bout de la planète.** On parle d'ubiquité. Trouver et poursuivre les attaquants en est d'autant plus complexe.

- **Le coût d'une cyberattaque peut être très faible et les capacités techniques nécessaires très accessibles** en comparaison des dommages susceptibles d'être causés. Ces propriétés facilitent l'activité de « cyberattaquant ».

Tenter de tout protéger, tout le temps, contre des attaquants discrets et des attaques souvent invisibles, agissant avec une boîte à outils potentiellement infinie, tel est le défi des acteurs de la cybersécurité !

FICHE

10

# Réagir aux cyberattaques

# 1 Répondre à un incident informatique

Lorsqu'une attaque informatique est détectée, l'objectif pour une organisation victime est de la faire cesser, limiter ses impacts et revenir à la normale.

Pour cela, plusieurs étapes doivent être franchies :

- Comprendre et caractériser l'attaque et les impacts causés ou susceptibles d'être causés.
- Contenir et protéger les systèmes concernés.
- Faire cesser l'attaque, en désinfectant/réparant, puis en restaurant et en reconstruisant les systèmes concernés.

**Acteurs essentiels de la réponse à incident, les équipes de réponse à incident de sécurité** – les CSIRT (*computer security incident response team*) ou CERT – sont les « médecins » chargés d'intervenir et de diagnostiquer les mesures à prendre pour faire cesser l'infection. Ils sont aussi souvent les « pompiers » qui interviennent eux-mêmes pour éteindre l'incendie. Le CSIRT d'une organisation peut également coopérer avec d'autres équipes en-dehors d'une organisation, en France et à l'international.

# 2 La gestion d'une crise d'origine cyber

**On parle de crise « d'origine cyber » face à un incident informatique malveillant brutal, soudain, menaçant gravement la stabilité d'une organisation, d'un ou plusieurs États :**

- Pour une ou plusieurs organisations, comme l'interruption de la fourniture d'un service à des clients ou la divulgation de leurs données à caractère personnel, source d'un mécontentement légitime.
- Pour la France voire l'Europe, lorsque les conséquences d'une cyberattaque s'avèrent massives, par le nombre de victimes ou les impacts causés par l'attaque (par exemple, l'interruption de la fourniture de services essentiels comme l'électricité ou l'accès à internet).

Face à une telle crise, la réaction d'une organisation ou d'un État ne pourra pas être seulement technique mais également opérationnelle et stratégique (coordination interne, avec les partenaires, communication, etc.) afin de permettre une sortie de crise rapide.

Il existe, à l'échelle de l'État français, des dispositifs de gestion des crises de toutes origines, notamment cyber :

- Le Premier ministre prépare et coordonne au niveau politique l'action des pouvoirs publics en cas de crise majeure (art. L. 1131-1 du code de la défense).
- La cellule interministérielle de crise (CIC), activée par le Premier ministre, met en œuvre la réponse globale de l'État. Elle réunit des représentants de haut niveau des différents ministères concernés et d'autres entités comme l'Agence nationale de la sécurité de système d'information (ANSSI), dans le cas d'une crise d'origine cyber.

- Des plans préexistent à certains types de crise afin de préparer la prise de décision des autorités. Le plan spécifique au cyber s'appelle Piranet mais la cybersécurité fait désormais partie d'autres plans de gestion de crise.

- La gestion de crise de l'État français nécessite, par ailleurs, la conduite régulière d'exercices de gestion de crise.



FICHE

11

# La réglementation

# 1 Les règles en matière de cybersécurité et de lutte contre la cybercriminalité

Des catégories de règles existent en matière de cybersécurité et de lutte contre la cybercriminalité :

**Les règles visant à renforcer la protection des systèmes d'information de l'administration et d'opérateurs particulièrement critiques,** en les obligeant à mettre en œuvre certaines mesures techniques et non techniques pour protéger leurs systèmes d'information.

**Les règles visant à interdire et, le cas échéant, punir des actions ou des comportements illicites en ligne.**

# 2 Les règles pour renforcer la cybersécurité

**2 familles de réglementation participent particulièrement au renforcement de la cybersécurité en France :**

- **Les règles s'appliquant aux entités publiques**, afin de garantir un niveau de sécurité adapté de leurs systèmes d'information et des services publics numériques notamment accessibles au public. Ces règles incluent la politique de sécurité des systèmes d'information de l'État (PSSIE) ou encore le référentiel général de sécurité (RGS).

- **Les règles applicables aux opérateurs publics et privés les plus critiques.** Cela inclut les « opérateurs d'importance vitale » (loi de programmation militaire de 2013) gérant des installations indispensables à la survie de la nation et les règles européennes applicables aux « entités essentielles » et aux « entités importantes » pour l'économie et la société (directive européenne sur la sécurité des réseaux et des systèmes d'information adoptée en 2022). Ces opérateurs doivent mettre en œuvre des mesures de sécurité numérique et notifier à l'autorité nationale de cybersécurité (ANSSI), les incidents survenus sur leurs systèmes d'information.

- **Les règles applicables à l'ensemble des entreprises et des autres entités, en vue de protéger les données à caractère personnel.** La loi informatique et libertés en France et le règlement européen sur la protection des données à caractère personnel dit « RGPD » imposent à toutes ces entités de prendre des mesures afin d'assurer la sécurité de ces données, comme le chiffrement.

3

## Les amendes et les peines de prison pour des actions ou des comportements illicites en ligne

**Le droit français, en particulier le code pénal, prévoit plusieurs infractions pouvant entraîner des amendes et des peines de prison, lorsqu'elles ont été commises en ligne :**

- **L'escroquerie** (article 313-1 du code pénal), passible d'une peine d'emprisonnement de cinq ans et de 375 000 euros d'amende.
- **La collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite** (article 226-18 du code pénal) : une telle collecte constitue un délit passible d'une peine d'emprisonnement de cinq ans et de 300 000 euros d'amende.
- **Les accès, les entraves, l'extraction de données, et les autres comportements frauduleux envers un système de traitement automatisé de données** (article 323-1 et suivants du code pénal) comme un ordinateur, un serveur, un téléphone, ou tout autre système d'information. Les peines peuvent atteindre sept ans d'emprisonnement et 300 000 euros d'amende. La tentative est réprimée de la même manière. Le fait de posséder des outils permettant de réaliser ces infractions, même sans en faire usage, est également illégal (article 323-3-1).
- **La contrefaçon et l'usage frauduleux de moyen de paiement** (articles L. 163-3 et suivants du code monétaire et financier) : délit passible d'une peine d'emprisonnement de sept ans et de 750 000 euros d'amende.
- **L'usurpation d'identité** d'une personne tierce (article 226-4-1 du code pénal), passible d'une peine d'un an d'emprisonnement et de 15 000 euros d'amende.
- **La contrefaçon des éléments visuels (logos, signes, identité graphique, emblèmes…) utilisés lors de l'hameçonnage** (articles L. 335-2 et suivants, L. 716-10 et suivants du code de la propriété intellectuelle) : délit passible d'une peine d'emprisonnement de trois ans et de 300 000 euros d'amende.



FICHE

12

# Les enjeux de paix et de sécurité internationale du cyberespace

## 1 Le cyberespace, source croissante de conflictualité

Désormais considéré comme un espace de confrontation à part entière par les armées de plusieurs États dans le monde, le cyberespace est devenu le lieu de rapports de force entre États mais également entre États et acteurs non-étatiques (cybercriminels, terroristes, etc.).

L'utilisation de moyens cyber-offensifs en dehors du cadre des conflits armés, régis par le droit international public, suscite un nouveau risque : celui qu'une crise d'origine cyber conduise à un conflit entre États, notamment dans le monde physique.

## 2 Des facteurs aggravants

**Les difficultés à attribuer l'origine des attaques**

La discrétion et la furtivité associées aux attaques informatiques, notamment les plus sophistiquées, peuvent rendre complexe l'attribution de l'origine d'une cyberattaque dont est victime un État.

Le risque de ripostes fondées sur une attribution erronée contre les installations d'un État n'étant en fait pas à l'origine de l'attaque – par exemple conduite par un groupe cybercriminel sur son territoire – peut entraîner une escalade entre deux États, voire de contagion à d'autres États.

**La prolifération des armes cyber**

Les outils et les techniques cyber-offensifs ou « armes cyber » étant de nature informatique, celles-ci sont par nature réplicables, modifiables, plus difficiles à contrôler et moins chères à développer ou à acquérir.

Le risque de prolifération des armes cyber augmente la probabilité que des cybercriminels ou des États ne disposant pas de moyens de développement de ces derniers, se dotent eux-mêmes de ces capacités. Cette situation menace de « polluer » le cyberespace avec une quantité toujours plus importante d'actions malveillantes. La divulgation d'outils et de techniques utilisées par les services de renseignement de certains États contribue à ce risque de prolifération.



## 3 Renforcer la confiance entre États

Plusieurs mécanismes concourent à renforcer la sécurité et la stabilité internationale du cyberespace au travers d'échange entre États. On parle de « mesures de renforcement de la confiance ».

### Les mesures de transparence

Elles consistent à partager publiquement toute information apte à rassurer les autres États face à la perspective d'un différend : partage de points de contacts techniques et diplomatiques afin de faciliter les échanges ; partage de la stratégie nationale de cybersécurité mais aussi de la doctrine cyber offensive et des conditions d'emploi de ces capacités, etc.

### Les mesures de coopération

Elles consistent en l'ensemble des mécanismes de coopération, notamment les techniques entre équipes de réponse à incidents (CSIRTs) permettant au quotidien d'œuvrer collectivement à identifier les vulnérabilités et à rendre les systèmes d'information plus sûrs, mais aussi au niveau diplomatique ou politique, permettant de résoudre de manière pacifique d'éventuels différends.

### Les mesures de stabilité

Ces dernières consistent en l'établissement de mécanismes de signalement et de dialogue en vue de permettre une désescalade entre États en cas de différend et de perspective de conflit, le plus souvent au niveau politique. C'est, par exemple, le cas entre les États-Unis et la Russie qui ont mis en place une ligne de signalement d'urgence en cas d'attaque.

4

## Fixer les règles pour un cyberespace stable et sécurisé

Au-delà du renforcement de la confiance, le cyberespace doit être protégé par le droit international afin d'encadrer les actions des États, éviter la survenue de conflits entre eux ou encadrer ces derniers. À cette fin, deux axes de travail guident depuis plusieurs années des travaux entre diplomates principalement à l'ONU.

### Les normes de comportement responsables des États dans le cyberespace

Non contraignantes, ces normes de comportement, décrites dans plusieurs rapports de l'ONU décrivent les comportements que les États devraient adopter pour prévenir les incidents cyber et y répondre, en priorité par la coopération.

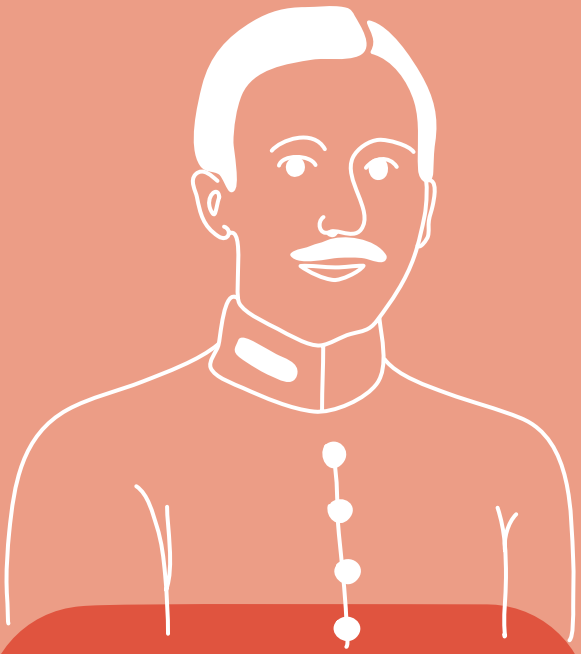
### L'application du droit international au cyberespace

Les discussions à l'ONU portent également sur les modalités d'application du droit international au cyberespace. Par exemple, quelles sont les conditions d'exercice du droit à la légitime défense des États face à des cyberattaques comme prévu par l'article 51 de la Charte des Nations Unies ?



FICHE

13



# Une brève histoire de la cybersécurité

## 1

# La cybersécurité : un domaine aux racines très anciennes…

Si l'on pourrait croire que la cybersécurité est un domaine très lié aux « nouvelles technologies » et donc relativement récent, elle trouve en fait ses racines dans un sujet vieux de plusieurs siècles : la cryptographie (voir les fiches consacrées à la cryptographie). Au fur et à mesure de la création des États, les dirigeants ont, en effet, ressenti le besoin de protéger leurs secrets – politiques, stratégiques et diplomatiques – des puissances étrangères. Jules César est à cet égard un exemple célèbre et très ancien de chef d'État qui a recouru à la cryptographie pour protéger ses correspondances.

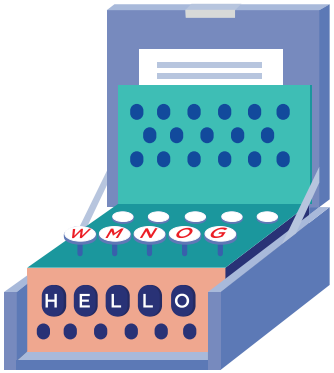
Entre les années 1200 et 1650, la construction de l'État français tel que nous le connaissons est passée par des étapes importantes, qui ont contribué à structurer son organisation et ses missions les plus essentielles : création des Archives nationales, du Trésor, d'une monnaie unique dans tout le royaume, d'un impôt (la taille) permettant de lever une armée permanente ou encore des postes. À partir de 1600 environ et jusqu'à la Révolution française, une fonction de « cryptographe du Roy » sera ainsi tenue à plein temps. L'un d'entre eux, Antoine Rossignol sera, par exemple, remarqué par le cardinal de Richelieu. Il servira pendant plus de 50 ans les rois Louis XIII puis Louis XIV et ira jusqu'à transmettre sa fonction à son fils et son petit-fils, avec pour mission de chiffrer et de déchiffrer les correspondances du Roi et lui transmettre directement les résultats des messages interceptés.



## 2

# La sécurité des communications, au cœur des grands conflits mondiaux

La protection des communications des autorités politiques et militaires a pris une importance critique lors des grands conflits mondiaux. Pendant la première guerre mondiale, la France dispose ainsi d'une équipe chargée de travailler sur les messages allemands interceptés pour en « casser » le chiffrement. En juin 1918, dans une séquence épique et héroïque, Georges Painvain, jeune et brillant officier affecté à cette unité, réussira à percer les codes allemands pour décrypter le « Radiogramme de la Victoire ». Transmise aux hautes autorités politiques et militaires, cette information permettra aux Français d'anticiper les mouvements adverses et de mener une contre-offensive décisive pour barrer la route aux troupes ennemies, jouant un rôle capital dans la tournure du conflit.




Durant la seconde guerre mondiale, le « Chiffre » joue de nouveau un rôle central. Le film *Imitation Game* a contribué à faire connaître l'action de personnages illustres tels qu'Alan Turing – considéré comme l'un des fondateurs de l'informatique moderne – dans la cryptanalyse de la machine de chiffrement Enigma, utilisée par les Allemands pour protéger le secret de leurs échanges. Au-delà du rôle des britanniques, un travail fondamental a été mené par les français, derrière le général Gustave Bertrand, en collaboration avec de brillants mathématiciens polonais tels que Marian Rejewski[1].

1. L'excellent ouvrage *Enigma, ou comment les Alliés ont réussi à casser le code nazi*, de Dermot Turing, neveu d'Alan Turing, est une référence complémentaire précieuse sur cet épisode.

3

## Avec l'essor de l'électronique, de l'informatique et d'internet, l'avènement de la sécurité des systèmes d'information (SSI)

Les années 1950 et 1960 sont le théâtre de plusieurs inventions majeures dans le domaine de l'électronique : le transistor, le circuit intégré et le microprocesseur. Ces éléments seront fondateurs d'une nouvelle discipline : l'informatique. La fin des années 1960 et la décennie 1970 donneront une autre ampleur à ce domaine en mettant les ordinateurs – ou plus largement, les systèmes d'information (SI) – en réseau, jetant ainsi les bases de l'internet que nous connaissons aujourd'hui. C'est l'époque de l'essor de technologies basées sur l'informatique et les télécommunications, comme internet, le Minitel ou la carte à puce.

Allant au-delà de la seule protection de la confidentialité des messages, assurée par la cryptographie, l'avènement des systèmes d'information et de leurs réseaux permet également l'essor d'une discipline plus large : la sécurité des systèmes d'information (SSI) ou « sécurité informatique ». Initialement cantonnée aux mondes gouvernemental et universitaire, la matière profitera de la démocratisation d'internet et de l'accroissement de la connectivité pour se répandre largement. Elle englobera progressivement de nombreux domaines, faisant appel à des expertises techniques variées : sécurité des réseaux, des logiciels, des composants matériels, des communications, etc.



4

## Le début du web : une (hyper-)connexion qui offre de fabuleuses opportunités et génère des menaces redoutables

Le début des années 1990 voit internet s'ouvrir à une utilisation commerciale qui ne cessera de s'accroître, portée dans les années 2000 par le développement des services en ligne, des réseaux haut débit filaires ou sans fil, de l'internet mobile et du « web 2.0 » – participatif, interactif et social. Le numérique progresse largement dans la société et l'économie, créant de formidables opportunités.

Outre cette dynamique vertueuse, il fait également émerger de nouvelles sources de menace. Les cyberattaques sont désormais courantes, visibles et peuvent avoir des impacts de plus en plus significatifs. Pour répondre à cette tendance, dans la logique « du chat et de la souris », c'est le domaine de la cyberdéfense qui prend tout son essor, créant au passage de nombreux métiers importants et fascinants.

Comme l'était le Chiffre au temps de Louis XIV, la cybersécurité devient un enjeu stratégique pour les États qui, pour contrer les menaces d'espionnage, de sabotage et de déstabilisation auxquelles ils font face, ils mettent en place des dispositifs structurés basés sur des capacités techniques, mais également politiques, réglementaires et industrielles. Au-delà des seuls échelons nationaux, la cybersécurité devient par ailleurs un enjeu de dimension européenne et internationale.

Ce livret a été élaboré conjointement
par l'Agence nationale de la sécurité des
systèmes d'information et le ministère
de l'Éducation nationale et de la Jeunesse.