­­­

DICTIONNAIRE DE LA

CYBERSÉCURITÉ

ET DES RÉSEAUX

*Du même auteur*

*aux éditions Nuvis*

Cyberstratégie,

l’art de la guerre numérique, 2012

Cybertactique,

conduire la guerre numérique, 2014

*Prix du livre Cyber 2014*

**Bertrand BOYER**

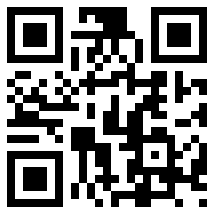
**DICTIONNAIRE DE LA**

**CYBERSÉCURITÉ**

**ET DES RÉSEAUX**

**nuvis**

17, rue Dupin, 75006 Paris



Flasher ce *QR Code* pour accéder au site www.nuvis.fr

Les livres publiés par Nuvis sont téléchargeables

sur tablette numérique au format électronique ePub

Tous droits de reproduction, d’adaptation et d’exécution réservés pour tous pays, notamment la traduction, la réimpression, l’exposition, la photocopie du texte, des illustrations et des tableaux, la transmission par voie d’enregistrement sonore ou visuel, la reproduction par scanner, par microfilm ou tout autre moyen ainsi que la conservation dans une base de données. La loi française sur le copyright du 9 septembre 1965 n’autorise une reproduction intégrale ou partielle que moyennant le paiement de droits spéciﬁques. Elle sanctionne toute représentation, reproduction, contrefaçon, photocopie, et toute conservation dans une base de données par quelque procédé que ce soit.

© 2015 — Nuvis*,* 17 rue Dupin, 75006 Paris



# Avertissement

1. Ce dictionnaire a été réalisé pour répondre au besoin d’un large public cherchant à disposer des bases nécessaires à la compréhension des réseaux et de la sécurité informatique.
2. Il regroupe dans un même ensemble des définitions issues de sources multiples mais également fruit de la libre interprétation de l’auteur.
3. Ainsi, certains termes reprennent les définitions officielles, retenues par la commission de terminologie et de néologisme, ainsi que celles couramment utilisées par l’Agence Nationale de la Sécurité des Systèmes d’Information[[1]](#footnote-2). D’autres termes sont détaillés et développés sous forme de concept pour permettre au lecteur de se constituer un avis construit.

# Introduction

1. *La logique du révolté est... de s'efforcer*
2. *au langage clair pour ne pas épaissir*
3. *le mensonge universel.*
4. Albert Camus, L’Homme révolté.
5. Pourquoi un dictionnaire de la cybersécurité et des réseaux ? Cet ouvrage s’est imposé comme une évidence tant les études sur le cyberespace, les mondes numériques et les réseaux reposent essentiellement sur des questions de sémantique. La difficulté d’élaborer des réponses aux enjeux de la numérisation croissante de nos sociétés prend en partie naissance dans notre difficulté à visualiser les phénomènes immatériels. L’information, son flux, sa gestion, sa manipulation souffre d’un déficit de représentation. Ainsi, nommer, c’est déjà commencer à comprendre.
6. Ce dictionnaire a donc une vocation pédagogique, il propose des clés de compréhension accessibles à tous pour sortir les questions numériques d’un entre-soi confortable où les acronymes anglo-saxons le disputent au jargon technique, excluant de fait le plus grand nombre.
7. Le livre s’ouvre sur le mot *Accès* et se ferme sur *Zombie* ce hasard résume à lui seul la dualité du cyberespace. D’abord prolongement des réseaux, le cyberespace est le lieu de l’accessibilité, l’ouverture aux savoirs, à l’échange il permet cette élévation, il incarne la marche en avant du progrès et fait grandir l’Homme. Mais chaque médaille a son revers et le dernier mot du dictionnaire sonne comme un avertissement, un douloureux réveil pour nous rappeler que le cyberespace c’est aussi des zombies, des morts-vivants, des ordinateurs infectés, le vôtre peut-être, si proches mais si différents, le mal incarné.
8. Au long de ces pages nous chercherons à faire saisir les concepts qui nous semblent essentiels pour approcher les mondes numériques.
9. Cet ouvrage s’adresse donc à un vaste public désireux de se forger une culture solide, de comprendre, de progresser. Les étudiants en télécommunications y trouveront les bases nécessaires à leurs apprentissages, mais ce dictionnaire se veut ouvert et doit pouvoir toucher également les lecteurs qui cherchent à dépasser les lieux communs.

# Mode d’emploi

1. Par nature, un dictionnaire résiste mal à une lecture linéaire, son intérêt réside dans les entrées multiples et un accès thématique. Notre ouvrage peut être lu de façon linéaire ou totalement aléatoire, allant d’un concept à l’autre au gré de votre besoin immédiat.
2. Certains termes sont présentés pour illustrer des problématiques liées au numérique et n’ont pas vocation à « apprendre » un mot de vocabulaire au lecteur (ex : archive) ; d’autres présentent des notions de terminologie militaire et stratégique afin de mieux comprendre les enjeux de l’affrontement dans le cyberespace et les concepts utilisés pour les présenter ; enfin des termes anglo-saxons jalonnent ce dictionnaire.
3. Sans vouloir faire offense à la langue française, force est de constater que les usages du numérique et des télécommunications donnent naissance à une multitude de termes et d’acronymes en anglais. Ceux-ci seront présentés dans ce dictionnaire, traduits lorsque cela est possible mais systématiquement explicités. Nous utilisons pour ce faire la terminologie officielle française ayant fait l’objet d’une publication au Journal Officiel.
4. Le lecteur trouvera donc en entrée le terme le plus courant (qu’il soit en français ou en anglais). Ainsi à la lettre C vous trouverez l’expression « *Crowdfunding*» en entrée, l’expression y sera traduite et analysée.
5. En fin d’ouvrage l’index présente l’ensemble des entrées du dictionnaire : en **gras** figurent **les entrées principales** (celles qui font l’objet de la définition), en *italique*, les termes de langue anglaise.
6. Plus que la langue, c’est la pratique qui nous a conduit à sélectionner les entrées de ce dictionnaire. Ainsi, certains acronymes sont directement accessibles (donc en gras) et certains termes en anglais également.

# A

**Accès**

*(Access- hit)*

Qualité qui permet de bénéficier d’un service particulier sous certaines conditions. Ainsi pour bénéficier d’une connexion Internet l’usager doit solliciter un fournisseur d’accès Internet (FAI\*). En matière de télécommunication, il existe plusieurs types d’accès, de mécanisme d’accès ainsi que des techniques de contrôle d’accès\*. L’accès désigne également le fait d’engager une consultation d’un document sur un serveur[[2]](#footnote-3). Ainsi, le nombre d’accès est une mesure courante de l’audience d’un site Internet ou de la fréquence de consultation d’un document. Dans cette approche, le terme en anglais le plus juste est *hit*.

**Accès de base et accès primaire**

*(Basic Rate Interface – Primary Rate Interface)*

Dans les Réseaux Numérique à Intégration de Services (RNIS\*), l’accès de base est le raccordement élémentaire qui fournit deux canaux B à 64 Kbps et un canal de signalisation\* à 16 Kbps. Il se distingue de l’accès primaire (Interface S2) qui lui, procure trente canaux B, un canal de signalisation.

**Accès direct**

*(Direct access – Random access)*

Mode d’écriture ou de lecture de données se faisant au moyen d’adresses qui repèrent l’emplacement des données[[3]](#footnote-4).

**Accès multiple**

(*Multiple Access)*

Technique permettant à un certain nombre de terminaux ou de stations d’utiliser simultanément les ressources d’un moyen de transmission, d’une façon prédéterminée ou en fonction du volume des échanges[[4]](#footnote-5). Ainsi, dans un réseau local, l’accès des terminaux à une même ligne de transmission est un exemple d’accès multiple. Pour réaliser un accès multiple il est nécessaire de mettre en œuvre des techniques particulières. On peut choisir de répartir dans le temps (chaque équipement dispose d’une fenêtre temporelle spécifique – ex *Time Division Multiple Access* -TDMA\*), d’effectuer une répartition en fréquence (*Frequency Division Multiple Access -* FDMA\*) par détection de porteuse ou étalement de spectre (voir AMRC\* ou CDMA *Code Division Multiple Access* CDMA\*).

Voir également AMRC – Accès Multiple par Répartition en Code, AMRF – Accès Multiple par Répartition en Fréquence, AMRT – Accès Multiple par Répartition Temporelle.

**Accès séquentiel**

*(Serial access)*

L’accès séquentiel désigne un mode d’écriture ou de lecture de données, effectuées en suivant un ordre préétabli de rangement[[5]](#footnote-6). L’accès séquentiel s’oppose à un accès direct.

**Acheminement**

*(Routing)*

Processus qui consiste à envoyer un bloc d’information vers sa destination finale via une ou plusieurs stations du réseau [SERVIN 2003]. Dans un environnement IP\*, l’acheminement des paquets est ainsi la fonction principale d’un réseau, ce mécanisme fait l’objet de protocoles, et d’optimisations permanentes.

**ACL - *Acces Control List***

(Liste de contrôle d’accès)

Une liste de contrôle d’accès établit les personnes, machines, fonctions ou protocoles qui peuvent accéder à une ressource (fichier, machine, service réseau, etc.). En matière de réseau, une ACL définit par exemple les ports\*, adresses MAC\*, adresses IP\* et protocoles\* autorisés à franchir un équipement actif (pare-feu\*, routeur, etc.).

**Acquittement**

*(Acknoledgement) (ACK)*

Message d’accusé de réception positif dans une procédure de transmission.

**Action de lutte informatique défensive - LID**

*(Computer Network Defense)*

Dans le cadre des opérations dans le cyberespace\*, action consistant à surveiller, analyser, détecter et réagir face à des attaques, intrusions ou perturbations qui pourraient compromettre, paralyser ou détruire nos systèmes, réseaux et données[[6]](#footnote-7).

**Action de lutte informatique offensive – LIO**

*(Computer Network Attacks - CNA)*

Dans le cadre des opérations dans le cyberespace\*, action non physique entreprise dans le cyberespace contre des systèmes d’information ou des données pour les perturber, les modifier, les dégrader ou les détruire[[7]](#footnote-8).

**Action d’exploitation informatique - EI**

*(Computer Network Exploitation – CNE)*

Dans le cadre des opérations dans le cyberespace\*, action conduite dans le cyberespace en vue d’obtenir l’accès aux logiciels, configurations matérielles et données des réseaux informatiques. Elle vise à exploiter les données issues de systèmes d’information ou de réseaux cibles et à recueillir du renseignement sur ces systèmes et réseaux pour alimenter le renseignement d’intérêt cyberdéfense\* (RIC)[[8]](#footnote-9).

**Action d’influence**

*(Influence Activity)*

Dans la terminologie militaire française, ensemble des activités intentionnelles pour obtenir un effet sur les perceptions en vue de modifier les attitudes et/ou les comportements[[9]](#footnote-10).

**Action d’information**

*(Information Activity)*

Les actions d'information désignent les activités offensives et défensives portant sur les données, les contenus informationnels (messages et connaissances) ou les systèmes d’information[[10]](#footnote-11).

***Add-on***

(Additif – Module complémentaire - *Plug-in*)

En informatique, un *add-on* est un module complémentaire d’un logiciel (ou d’un matériel) qui lui confère des améliorations ou des fonctionnalités supplémentaires. L’*add-on* ne peut fonctionner qu’avec son logiciel maître et peut être ajouté indépendamment de l’installation de ce dernier. A titre d’illustration, le navigateur libre *Mozilla Firefox* dispose de multiples modules complémentaires qui permettent par exemple de bloquer la publicité, d’afficher la localisation du serveur\* sur lequel vous êtes connecté, son certificat\* de sécurité ou encore forcer l’utilisation du protocole sécurisé HTTPS\* lorsque cela est possible.

**Administration de réseau**

*(Network management)*

Action qui consiste à assurer le fonctionnement d’un réseau (de ses équipements, interconnexions et des ressources qui le constituent en général), ainsi que sa gestion fonctionnelle (ajout, modification ou suppression d’équipements, d’interconnexions, de fonctionnalités, configuration, etc.).

**Adressage**

*(Addressing)*

Ensemble des moyens permettant d’accéder à une entité déterminée. On distingue plusieurs types d’adressage :

• Adressage absolu : adressage pour lequel on accède à l’entité via une chaine de caractères absolu, il n’y a alors aucune relations entre les adresses.

• Adressage hiérarchique : ensemble de moyens permettant d’accéder à une ressource via une succession de champs qui déterminent une localisation au sein de sous-ensembles hiérarchisés. Les adresses IP\* en sont une forme, un numéro de téléphone également.

• Adressage logique : type d’adressage qui permet d’identifier et de joindre une entité sur un réseau sans nécessairement connaître sa localisation physique. L’adressage logique intervient sur la couche 3 (réseau) du modèle OSI et identifie l’interface réseau d’une machine. Une adresse logique n’est donc pas déterminée par son emplacement géographique. L’adresse IP\* est un exemple d’adresse logique.

• Adressage physique : ensemble de moyens permettant d’accéder à une entité physique. L’adresse MAC\* est, par exemple, utilisée dans ce type d’adressage pour identifier un équipement physique au sein d’un réseau (ordinateur, routeur, etc.)

Voir Adresse IP, Adresse MAC, Adresse.

**Adresse**

*(Address)*

Ensemble de données structurées qui permet de désigner tout ou partie d’une ressource (équipement informatique, réseau, bloc de stockage mémoire, portion de programme informatique, etc.) et le plus souvent, de l’identifier de façon unique parmi d’autres ressources dans un périmètre défini et à un instant donné.

**Adresse IP**

*(IP address)*

L’adresse IP permet d’identifier une ressource informatique (ordinateur, imprimante, téléphone) au sein d’un réseau qui repose sur le protocole de communication IP – *Internet Protocol*\*. Cette identification peut être permanente ou provisoire et demeure un élément essentiel pour permettre l’acheminement des paquets\* de données\*. Dans tout les cas elle est unique. L’adresse IP est codée sur 32 bits\* (4 octets) pour la version 4 et sur 128 bits (16 octets) pour la version 6 (voir IP V6\*).

C’est *l’Internet Corporation for Assigned Names and Numbers* (ICANN\*) qui a la responsabilité de la gestion des adresses IP et de leur distribution. Ce rôle est évidemment extrêmement important dans la gestion de l’Internet et de sa gouvernance.

Voir également IP V4 et IP V6.

***Pour aller plus loin***

**Les classes d’adresse IP**: face à l’augmentation rapide du nombre de réseau et d’adresse à distribuer, il a été nécessaire d’organiser la façon dont on attribuait ces adresses. En 1981, la RFC\* 790, *Assigned numbers*, est publiée, elle organise le mécanisme d’adressage. Ainsi, une adresse IP est divisée en deux parties, l’une servant à identifier le réseau (*net id*) l’autre servant à identifier la machine (*host id*). Partant, cinq classes d’adresses sont définies :

• Classe A : un octet pour définir l’adresse réseau : XXX.000.000.000.

• Classe B : deux octets pour l’adresse réseau : XXX.XXX.000.000.

• Classe C : trois octets pour l’adresse réseau : XXX.XXX.XXX.000.

• Classe D et E : adresses particulières.

Ainsi, en fonction de la taille du réseau l’ICANN assigne une « plage d’adresse » de la classe associée. Par exemple avec la classe C, il est possible d’identifier 2 097 152 réseaux distincts de 254 machines chacun. L’ICANN réserve également des adresses « privées » pour chaque classe. Ces adresses peuvent être attribuées librement (sans contrôle de l’ICANN) à une ressource informatique, sous réserve qu’elle ne soit pas directement connectée à Internet. Toutefois, l’accès de ces équipements à Internet peut s’effectuer par l’intermédiaire d’un équipement qui dispose lui, d’une adresse (publique) attribuée par l’ICANN. C’est le cas des ordinateurs de votre réseau domestique (qui disposent d’adresses IP privées de classe C le plus souvent, de type 192.168.X.Y.) qui accèdent à Internet par l’intermédiaire de votre « box », disposant elle-même d’une adresse attribuée par l’ICANN.

**Les sous-réseaux :**

Pour assurer un niveau supplémentaire de répartition des adresses IP, la notion de sous-réseau est introduite, en 1984, dans la RFC 917, *Internet* *subnets*. Ce fractionnement, qui ne remet pas en cause la notion de classe mais permet une utilisation plus flexible de l’espace d’adressage de chaque classe, en permettant la construction de sous-réseaux de taille arbitraire, grâce à l’utilisation d’un « masque ». Le masque de sous-réseau permet, lorsqu’il est appliqué à une adresse IP (par le biais d’une opération booléenne de type « ET ») de déterminer le sous-réseau associé à une adresse. Le masque de sous-réseau a donc la même longueur qu’une adresse IP et se présente, en notation binaire, comme une suite de 1 puis de 0. En notation décimale à point, un masque de classe C se présente ainsi : 255.255.255.0

**Adresse MAC**

*(Medium Access Control address)*

L’adresse MAC est l’adresse unique qui identifie un matériel électronique de communication réseau compatible avec le standard\* Ethernet\* (typiquement, une carte réseau d’ordinateur). Elle est codée sur 6 octets. Cette adresse est attribuée dès la construction, et constitue l’adresse « matérielle » d’un objet connecté.L’adresse est divisée en deux champs : le premier identifie le constructeur de l’interface matérielle, et le second est un numéro séquentiel attribué par le constructeur. L’adresse MAC est aussi appelée adresse « physique », par opposition à l’adresse « logique » (par exemple l’adresse IP\*) de l’équipement informatique associé.

**Adresse URL**

(*Uniform Ressource Locator)*

L’adresse URL, plus simplement appelée URL\*, désigne l’emplacement d’une ressource sur Internet. Le terme français retenu par la Commission générale de terminologie et de néologisme est : adresse universelle. Le Journal Officiel en donne alors la définition suivante : dénomination unique à caractère universel qui permet de localiser une ressource ou un document sur l’Internet, et qui indique la méthode pour y accéder, le nom du serveur et le chemin à l’intérieur du serveur[[11]](#footnote-12).

Ex : http ://monsiteinternet.com est l’URL de « mon site internet », cette adresse est interprétée par le navigateur pour retrouver la ressource sur Internet (voir DNS). Le mécanisme du DNS\* fait correspondre une adresse IP\* à une URL. Cette dernière étant plus simple à retenir qu’une suite de chiffres.

Voir également : URL, URI, DNS

**ADSL - *Asymmetrical Digital Subscriber Line***

**Littéralement « liaison numérique asymétrique », l’ADSL est une technologie d’accès\* numérique à Internet\* par l’intermédiaire d’une ligne téléphonique analogique, qui s’appuie sur des méthodes de transmission plus performantes que le classique RNIS\*. Les liaisons ADSL sont dites « asymétrique\* » dans la mesure où le débit en réception (*download\**- descendant) est supérieur au débit d’émission (*upload\** montant).**

**AES - *Advanced Encryption Standard***

AES est un algorithme de chiffrement symétrique, il remplace le DES\* comme standard de chiffrement à partir de 1997. Ses créateurs, Joan Daemen et Vincent Rijmen ont proposé un algorithme de chiffrement par bloc utilisant des clés de 128, 192 ou 256 bits. AES utilise peu de ressources mémoire et s’avère un standard très rependu.

**AET – *Advanced Evasion Techniques***

(Technique d’évasion avancées)

Les techniques d’évasion avancées regroupent l’ensemble des pratiques qui permettent le contournement des systèmes de détection d’intrusion. Ces techniques sont en général pratiquées par des attaquants déterminés et disposant de moyens conséquents pour atteindre leurs objectifs. Le terme est à rapprocher des attaques de type APT (*Advanced Persistant Threat*).

Voir également APT.

**AFF – *Advanced Forensic Format***

**Affaiblissement du signal**

Rapport entre la puissance en entrée d’un système et celle en sortie. Ce rapport s’exprime en décibel (db). L’af­faiblissement traduit donc une diminution d’une puissance électrique, acoustique ou électromagnétique entre deux points[[12]](#footnote-13). Lorsque l’affaiblissement du signal est trop important, le récepteur interprète moins correctement le signal et génère des erreurs.

**AFNIC – Association Française pour le Nommage Internet en Coopération**

L’association française pour le nommage internet en coopération est une association à but non lucratif en charge de la gestion de la gestion des domaines de premier niveau (TLD) suivants : .fr ; .re (la Réunion), .tf (Terres australes et antartiques françaises) ; .yt (Mayotte) ; .pm (Saint-Pierre et Miquelon) ; .wf (Wallis et Futuna). Créée en 1997, l’association se fixe comme objectif de contribuer au développement d’un internet plus sûr et stable ; ouvert aux innovations ; où la communauté Internet française joue un rôle de premier plan. Les missions de l’AFNIC sont ainsi de : « d’exceller dans la fourniture de services essentiels résilients au cœur de l’infrastructure Internet en France ; de développer et de partager son expertise pour faciliter les transitions vers l'Internet du futur. »[[13]](#footnote-14)

**AFNOR - Association Française de NORmalisation**

Association loi 1901 fondée en 1926 responsable, en France, de la normalisation. Elle est membre de l'ISO (International Standard Organisation) et du comité Européen de normalisation CEN. L’AFNOR est par ailleurs membre du comité de normalisation en électronique et en électrotechnique (CENELEC). L’association a le monopole de la normalisation en France et édite les normes NF.

**Agent**

*(Agent)*

Programme qui effectue une tâche de façon autonome sans intervention de l’utilisateur (les agents peuvent dialoguer entre eux). Il peut ainsi effectuer la liaison entre deux entités du réseau, filtrer des informations ou effectuer des recherches. On parle d’agent logiciel, ou d’agent intelligent.

***Air gap – air wall***

(Isolation physique)

Mesure de sûreté utilisée pour sécuriser un système en l’isolant physiquement de tout autre réseau informatique. Dans ce cadre, aucune connexion physique n’est autorisée (branchement de périphériques, câbles, connexions sans fil, etc.). On peut par ailleurs inclure dans ces mesures une isolation électromagnétique qui assure qu’aucune fuite de données, ou attaque, ne peut avoir lieu à l’aide d’émissions de signaux parasites. Il faut toutefois noter qu’un *air gap*, s’il confère un niveau de sécurité élevé à un système, s’avère pénible à utiliser et rend donc son déploiement peu performant. Son usage est, en général, limité à des systèmes critiques à sécuriser en priorité. Enfin, plusieurs attaques informatiques ont déjà réussi à franchir des *air gap* avec l’aide active ou passive d’utilisateurs. Le facteur humain s’avère ainsi un élément clé de la sécurité du système d’information.

**Alice**

Voir Bob…

**Algorithme**

Suite d’instructions exprimées dans un langage simplifié permettant d’effectuer une opération spécifique. La science associée, l’algorithmique, est donc l’étude de la résolution de problèmes par la mise en œuvre de suites d’opérations élémentaires selon un processus défini aboutissant à une solution[[14]](#footnote-15). Elle est ainsi à la base de la programmation : elle permet, soit sous forme graphique, soit sous forme de pseudo code, de présenter les séquences d’instructions, définir les variables, les entrées et sorties afin de réaliser une opération spécifique.

**Algorithme de Dijkstra**

Algorithme de choix du plus court chemin entre deux points d’un réseau, utilisé pour le routage\* de paquets de données. Issu de la théorie des graphes, il est couramment utilisé dans les algorithmes de routages à états de liaisons\* et notamment par le protocole OSPF\* (*Open Shortest Path First*).

**Algorithme de Karn**

Algorithme développé par Philippe Karn en 1987 qui permet d’améliorer la mesure du temps de transmission aller-retour de données sur un réseau. Il permet donc d’obtenir une mesure fiable du *Round Trip delay Time* (RTT)\* lors d’une transmission via le protocole de transport TCP\*.

**Algorithme de routage**

Méthode de résolution permettant d’établir les routes à suivre pour l’acheminement de paquets dans un réseau en fonction de critères de choix.

Voir Routage, Table de routage.

**Algorithme de routage à état de liaisons (de liens)**

Dans les algorithmes de routage dynamique, comme ceux à état de liaisons, les routeurs sont censés fournir des informations sur le coût de la connexion à chacun de leurs voisins. Le routeur tient à jour une base de données décrivant la topologie réseau, il est donc en mesure de calculer la distance qui le sépare d’une destination, il construit donc un « arbre » dont il est la racine. Le routeur calcule la route complète vers la destination mais ne conserve que l’information sur le saut suivant. Le principal inconvénient de ce type d’algorithme est son coût en termes de capacité de calcul et d’utilisation de la mémoire. À chaque changement d’état sur le réseau, le routeur doit mettre à jour sa base et recalculer les routes possibles avant de déterminer la plus courte.

**Algorithme de routage par vecteur de distance**

Deuxième type d’algorithme de routage dynamique, le vecteur distance est également appelé algorithme de Bellman-Ford. Dans ce cas, chaque routeur dispose d’une table de routage\* qui indique pour chaque réseau, l’interface locale permettant d’atteindre la destination et la meilleure distance qui lui est associée. Cette distance est estimée par le routeur en fonction des messages envoyés par ses voisins. Cet algorithme nécessite de déterminer une métrique commune pour évaluer le coût d’une destination. Il peut s’agir du nombre de saut\* (un saut = distance entre routeurs voisins), du nombre de paquets dans la file d’attente de l’interface (système qui permet d’évaluer le niveau de congestion du réseau) ou encore le temps mis pour atteindre le prochain routeur. En échangeant leurs tables de routage de proche en proche, les routeurs finissent par connaître les réseaux auxquels ils ne sont pas connectés directement mais que leurs voisins sont capables d’atteindre. Le protocole RIP\* *Routing Information Protocol* est fondé sur un algorithme à vecteur de distance. La métrique choisie est le nombre de réseau qu’un paquet doit traverser pour atteindre sa destination finale.

**Allocation de ressources**

L’allocation de ressources est une méthode qui consiste à répartir les ressources d’un système entre plusieurs utilisateurs. L’allocation dynamique permet de choisir les bénéficiaires en fonction de critères déterminés en temps réel. Cette méthode s’oppose à l’allocation statique qui se fonde sur des critères définis en amont.

**Amorce**

*(Boot)*

En informatique, l’amorce (ou programme d’amorçage) est un programme nécessaire à la mise en fonction d’un système d’exploitation. Ce programme s’exécute à chaque mise sous tension (allumage). Au sein du support de stockage de masse le plus courant d’un ordinateur (le disque dur), il est stocké dans une zone particulière appelée MBR (*Master Boot Record)*.

Voir MBR.

**AMRC - Accès Multiple par Répartition en Code**

*(CDMA – Code Division Multiple Access)*

Plus connu sous le vocable anglo-saxon CDMA, *Code Division Multiple Access*, il s’agit d’une technique de mutualisation des accès\* à un lien de communication (il s’agit de permettre à plusieurs machines d’utiliser un seul et même canal de communication commun). Une seule fréquence de transmission est utilisée sur le lien, et chaque station qui y accède se voit attribuer un code propre. Ainsi, plusieurs stations peuvent transmettre de l’information sur le même lien : l’information d’une station donnée est identifiée par son code. Ce type d’accès s’appuie souvent sur une modulation à spectre étalé.

**AMRF - Accès Multiple par Répartition en Fréquence**

*(FDMA – Frequency Division Multiple Access)*

Le FDMA, *Frequency Division Multiple Access*, est une technique de mutualisation des accès\* à un lien de communication. Elle repose sur le multiplexage fréquentiel : plusieurs fréquences de transmission sont utilisées sur le même lien, et chaque station utilise sa propre fréquence parmi celles-ci pour transmettre des informations.

**AMRT - Accès Multiple par Répartition Temporelle**

*(TDMA – Time Division Multiple Access)*

Le TDMA, *Time division multiple access* est une technique de mutualisation des accès\* à un lien de communication. Elle repose sur le multiplexage temporel : chaque station dispose d’un intervalle de temps dédié (*slot\*)* pendant lequel elle peut transmettre sur le lien. Cette technique nécessite que toutes les stations utilisant le lien soient parfaitement synchronisées en temps.

Voir TDM, TDMA.

**Analogique (signal)**

*(Analogic)*

Un signal analogique est un signal\* qui varie sur une échelle de valeurs continue au cours du temps. Il se distingue d’un signal numérique\* qui varie de façon discrète dans le temps. Le signal numérique est « binaire\* », présent ou absent, c’est une succession de 0 et de 1. Il permet de mettre en œuvre des techniques avancées de compression de message et également l’utilisation de codes correcteurs d’erreur.

**Ancre**

*(Anchor)*

Appelée également, ancre de lien ou point d’ancrage, c’est une zone déterminée d’un document qui sert de départ ou d’arrivée à un lien hypertexte\*. Ainsi, une ancre permet dans un document de cliquer sur un mot ou une phrase qui est associé à un lien. C’est une façon plus intelligible de faire des références dans un document web par exemple, en évitant d’utiliser l’URL\* du lien.

**Android**

Système d’exploitation pour des terminaux mobiles (téléphones, tablettes) ou embarqués (télévisions, ordinateurs de bord automobiles, etc.), basé sur un noyau Linux. Racheté par Google en 2005, il représente, en 2012, 75% du marché des systèmes d’exploitation\* OS pour *smartphone* (ou ordiphone). Les concurrents d’Android sont l’IOS d’Apple et Windows Mobile de Microsoft.

**ANFR - Agence Nationale des Fréquences**

Etablissement public dont la mission est de gérer le spectre\* hertzien, de répartir les fréquences entre les différents organismes et administrations. L’ANFR conduit les négociations internationales sur les fréquences. Elle contrôle également, sur le territoire national, les stations radioélectriques (dont les stations de bases des opérateurs de téléphonie mobile).

**Anonymat**

*(Anonymity)*

Une des caractéristiques souvent évoquée de l’Internet, est l'anonymat (réel ou supposé) qu’il procurerait à ceux qui s’en donneraient les moyens. L’anonymat est ainsi une qualité qui rend impossible le lien entre une activité réseau (surf, requête) et une personne physique. Nouvelle esquive numérique à une censure d’État, l’anonymat incarne également le principal obstacle à la mise en place de réponses juridiques réellement efficaces dans le cadre de la lutte contre la cybercriminalité. Cette qualité est pourtant remise en question par les révélations successives d’Edward Snowden depuis le mois de juin 2013. La mise à jour des capacités de surveillance globale de certaines agences de renseignement étatiques nous amène aujourd’hui à penser que l’anonymat ne peut être totalement garanti.

**Anonymisation**

*(Anonymysation)*

Approche qui vise à rendre impossible, à une catégorie d’observateurs, l’identification réelle d’un usager du réseau en fonction de son activité. L’anonymisation est rendue possible par l’utilisation d’outils et de techniques spécifiques qui masquent ou modifient les paramètres d’identification d’une connexion (notamment adresse IP\* de la machines utilisée, empreintes).

**Techniques et outils d’anonymisation**

Il n’existe bien évidemment pas de « solution » complète et totalement sûre. L’internaute curieux pourra ainsi avoir accès à de nombreux outils dont l’usage est plus ou moins aisé mais c’est la combinaison de plusieurs outils et le strict respect d’une discipline d’usage qui peuvent permettre l’anonymat. Il existe différents outils correspondants à différents usages.

Naviguer sur le web :

Utiliser un « serveur proxy\* » qui permet de masquer votre véritable adresse IP\* ainsi que des données sur votre système d’exploitation et votre navigateur internet. Certains sont gratuits et d’autres services sont payants. De nombreux sites proposent des listes de proxy (il convient toutefois de vérifier la localisation physique de ces serveurs ainsi que leur stabilité). L’usage de proxy peut entrainer des expériences de navigation différentes et certains sites interdisent l’accès des connexions issues de proxys.

TOR, *the onion router* (Voir TOR)

L’installation du navigateur spécifique (TOR Browser) permet de rejoindre le réseau TOR sur lequel, les connexions sont chiffrées entre routeurs (il est donc théoriquement impossible d’intercepter une connexion). Attention toutefois, TOR ne protège que les paquets TCP il n’est donc pas infaillible, par ailleurs, chacun peut devenir un « nœud TOR » et faire transiter du flux par sa machine. La NSA par exemple disposerait de plusieurs relais contrôlés mais les capacités réelles d’interception sont sujettes à caution[[15]](#footnote-16).

**Anonymous**

Anonymous, désigne un mouvement informel d’activistes actifs notamment sur Internet. Ce mouvement, regroupe généralement des collectifs d’internautes agissant de manière anonyme, le plus souvent pour défendre la liberté d’expression et s’opposer à la censure. Le collectif peut agir également dans le monde « réel » en organisant des rassemblements où les participants arborent le masque de Guy Fawkes[[16]](#footnote-17) rendu populaire par la bande dessinée et le cinéma. Dans les années 80, le personnage de *V pour Vendetta* porte en effet un masque inspiré du visage de Guy Fawkes, puis en 2006 l’adaptation au cinéma réalisé par James Mc Teigue finit de populariser ce symbole et de l’associer définitivement avec le mouvement. Le collectif a connu une forte médiatisation à partir de 2008 avec notamment l’attaque contre l’église de scientologie (projet Chanology) puis contre les pays pratiquants une censure de l’Internet. Utilisant massivement les outils numériques, la mouvance est très présente sur les réseaux sociaux et sur l’ensemble des media 2.0. Le site *Anonops[[17]](#footnote-18)* par exemple offre de nombreux tutoriels\* pour rejoindre les canaux IRC\* du groupe en utilisant TOR\*.

Par ces relais ils informent la communauté des projets d’action et chaque internaute peut se joindre au mouvement. Les actions sont baptisées OP (pour opération) suivi du nom de la cible et généralement précédé du symbole dièse (hastag\*, #) rendu commun par le réseau social Twitter pour marquer un sujet.

Ainsi, au mois de février 2011, au début des Printemps arabes, le collectif vise la Tunisie et lance #optunisia, la répression est féroce et le gouvernement arrête plusieurs blogeurs et activistes liés au mouvement. La même année, #oplybia est lancée sous la forme d’un forum visant à regrouper et échanger des informations sur la situation dans le pays et permettre aux activistes d’échanger de façon sécurisée. Enfin, plus récemment, c’est la lutte contre la propagande de l’Etat Islamique qui a mobilisé la communauté (#opisis).

**ANSSI - Agence Nationale de la Sécurité des Systèmes d’Information**

L’ANSSI est l’autorité nationale française en matière de sécurité et de défense des systèmes d’information. Créée par décret en 2009, l’agence succède à la DCSSI (direction centrale de la sécurité des systèmes d’information). L’agence est ainsi chargée de proposer des règles pour la protection des systèmes de l’Etat et de vérifier l’application de ces mesures. Dans le domaine de la cyberdéfense, l’ANSSI assure via un centre opérationnel, la veille, la détection et l’alerte en cas d’attaques informatique sur les réseaux étatiques entre autres. Dirigée depuis février 2014 par Guillaume Poupard, succédant à Patrick Pailloux, l’agence compte environ 360 agents pour un budget de 75 M€ en 2013.

**Antivirus**

*(Antivirus)*

Logiciel destiné à détecter et prévenir l’infection d’une machine par un logiciel malveillant. L’antivirus inspecte ainsi les fichiers, courriers électroniques et les secteurs de démarrage d’un ordinateur.

Voir IDS, HIDS, IPS, HIPS, Heuristique.

**API - *Application Programming Interface***

(Interface de programmation)

Interface de programmation qui met à disposition des programmeurs des fonctionnalités et des accès aux programmes systèmes de façon simple et sans en exposer tous les détails. Une API comporte ainsi classiquement des classes, des méthodes, des fonctions et des constantes mises en œuvre par une bibliothèque logicielle. L’API regroupe, pour un langage de programmation donné, les fonctions « de base » déjà accessibles. Il suffit alors « d’appeler » la fonction existante plutôt que de la programmer entièrement. Cette pratique s’est particulièrement développée avec les langages de programmation par objets\*. Pour Java\* par exemple il existe de nombreuses API : Java RMI, Java IDL, Java Media Framework API…

**Appairage**

*(peering)*

Action qui consiste à échanger du trafic Internet avec des pairs. Les opérateurs\* suffisamment grands n’achètent pas de transit mais disposent d’accords d’appairage pour acheminer les paquets de leurs clients vers d’autres opérateurs. Ils sont appelés opérateurs de niveau 1 (tier-1). Le *peering* est donc un type d’accord entre deux réseaux qui s’échangent du trafic IP. Les accords de *peering* entre opérateurs permettent d’optimiser la connectivité géographique. Lorsqu’un accord de *peering* est impossible entre deux FAI\*, il est nécessaire de procéder à un accord de transit (qui lui est un accord commercial).

**Application**

*(Application)*

En informatique, une application est un ensemble de fonctionnalités regroupées dans une même famille d’activité. Le traitement de texte, par exemple, est une application courante de bureautique, comme la messagerie électronique. Le terme regroupe également l’outil qui supporte l’activité. Ainsi, Microsoft Word est une application de traitement de texte et Libre Office Calc une application de tableur.

**APT - *Advanced Persistant Threat***

Terme utilisé dans le milieu de la sécurité informatique et de l’analyse des menaces cyber pour désigner autant un type d’attaque qu’un groupe d’attaquants méthodiques, à des fins d’espionnage informatique. Plusieurs définitions du terme coexistent mais paraissent souvent ne traiter qu’un aspect du problème. Ainsi, le groupe de sécurité américain *Mandiant* (à qui l’on doit le rapport sur l’unité chinoise en charge de la lutte informatique offensive – APT1[[18]](#footnote-19)) parle d’« un groupe d'attaquants sophistiqués, déterminés et coordonnés, qui ont systématiquement compromis le gouvernement des États-Unis et les réseaux informatiques commerciaux depuis des années. ». Pour *Dell SecureWorks*: « APT, terme le plus couramment utilisé pour se référer à des activités de cyberespionnage menées contre les gouvernements, activistes et industries. ». Enfin, pour le NIST\* : « un adversaire qui possède un niveau d'expertise sophistiqué et des ressources importantes, qui lui permettent de créer des opportunités pour atteindre ses objectifs et utilisant de multiples vecteurs d'attaques. Ces objectifs sont typiquement l'établissement et l'extension d’une compromission dans l’infrastructure informatique dans le but d'exfiltrer de l'information, décourager ou entraver des aspects critiques d'une mission, d’un programme ou organisation ; ou se placer en position de remplir ces objectifs dans le futur ».

Finalement l'analyse « mot à mot » est également très intéressante car elle soulève de multiples questions. Le terme « *advanced*» en premier lieu ramène souvent au niveau technique des attaquants (« les plus évolués »). Cet aspect peut largement être critiqué, car d'une part il contribue à l'aspect « *marketing*» de l'analyse des menaces et d'autre part il est généralement faux. En effet, la plus part des APT n'exploitent pas de « vulnérabilités inconnues » (*0-day*) et utilisent bien souvent un vecteur d'infection classique (le mail ciblé – *spear* *phising*\*).

*SecureWorks* semble du même avis et écrit dans un document intitulé « Cycle de vie d'une APT » que « la nature organisée des attaques APT est ce qui les rend avancées et c'est cet attribut combiné avec le ciblage d'une entreprise spécifique qui les rend différents des autres scénarios de menaces. Les opérations démarrent avec un plan. Les objectifs sont définis et une série de procédures coordonnées très rodées est mise en mouvement ». En revanche, le terme « *Persistent*», semble plutôt faire l'unanimité. L'idée sous jacente étant qu'une APT, par nature, cherche à se maintenir sur le système cible. Le dernier terme de l’expression APT, « *Threat*» est encore plus complexe à cerner, et s'il peut paraître lié au « code » mis en œuvre, il fait plutôt référence à « l'intelligence » qu'il y a derrière. La menace ce n'est pas le code malveillant, c'est le groupe qui cherche à l'utiliser dans un but précis. Cedric Pernet dans son ouvrage sur les APT, fait converger les approches pour ne retenir que la formulation suivante : « Une attaque informatique persistante ayant pour but une collecte d'information sensibles d'une entreprise publique ou privée ciblée, par la compromission et le maintien de portes dérobées sur le système d'information. »[[19]](#footnote-20)

D’autres analyses enfin laissent entendre que le terme APT ne désignerait pas un type d’attaque mais serait un terme utilisé pour évoquer des attaquants chinois, sans les nommer expressément, lors des échanges d’informations entre le gouvernement américain et le secteur privé[[20]](#footnote-21).

**Archive – archivage**

*(Record, archive)*

L’archivage est l’action qui consiste à réunir, organiser et conserver des données. Il se distingue de la sauvegarde qui elle duplique les données pour un stockage sur un support distinct dans une démarche de sécurité, afin de pouvoir les restaurer en cas d’incident. La sauvegarde impose un éloignement (géographique, support, etc.) des données afin que ces dernières ne soient pas susceptibles de subir les mêmes sinistres que les données originales.

**ARP – *Address Resolution Protocol***

(Protocole de résolution d’adresse)

Protocole\* qui intervient entre la couche réseau (couche 3) et la couche liaison (couche 2) du modèle OSI\*. Son rôle est central car il permet d’assurer une correspondance entre des adresses réseau (typiquement une adresse IP\*) et une adresse physique (adresse MAC\*). ARP établit une table de correspondance entre les deux types d’adresse et interroge régulièrement le réseau pour mettre à jour cette table. Cette dernière, appelée *cache ARP,* est stockée dans une mémoire temporaire de chaque équipement qui souhaite communiquer. Ainsi pour pouvoir échanger un message avec une autre machine sur un même réseau local, la machine source doit interroger les autres machines pour savoir à adresse physique est associée l’adresse IP du destinataire. Un message *broadcast\** est alors envoyé et seul la machine dont l’IP correspond répond en indiquant une adresse MAC de destination. Ce mécanisme peut faire l’objet de détournement, on parle alors d’attaque de type *ARP cache poisoning*\*. Le protocole est décrit par la RFC\* 826 en 1982 et devient le standard internet STD 37.

Enfin, *arp* est également une commande qui peut être exécutée dans un terminal elle permet de consulter (et parfois modifier) les tables ARP. Ainsi, la commande *arp – a* retourne toutes les entrées du cache ARP.

**ARP *poisoning –* ARP *spoofing***

(Empoisonnement de cache ARP – Usurpation de cache ARP)

Technique d’attaque informatique qui permet de détourner le flux légitime vers un autre équipement d’un même réseau local. Pour ce faire, l’attaquant doit « forger » un message ARP dans lequel il fait correspondre à l’adresse IP de la passerelle (*Gateway\*)* l’adresse physique (adresse MAC\*) de sa propre machine. Ainsi, tout le flux du réseau local à destination de la passerelle transitera par sa machine, lui permettant d’écouter le trafic.

**ARPANET - *Advanced Research Projects Agency Network***

Le réseau ARPANET est généralement considéré comme « l’ancêtre » du réseau Internet. Il s’agit dans les faits d’un projet du département de la défense américain lancé en 1969 qui utilise pour la première fois le principe de la commutation de paquets.

L’ARPA (*Advanced Research Project Agency*) est créée en 1957, sous l’impulsion du président Dwight D. Eisenhower. Cette agence est chargée de piloter les projets scientifiques d’importance stratégique afin de garantir aux États-Unis la position de leader scientifique mondial. Dix ans plus tard, Lawrence G. Roberts, à la tête du projet « réseau informatique » au sein de l’ARPA publie ses « plans pour le réseau ARPANET ». Donald Davies et Robert Scantlebury du NPL proposent quant à eux un système qui s’appuie sur le concept de réseau à commutation de paquets[[21]](#footnote-22). La même année, Paul Baran de la RAND publie un article sur l’utilisation d’un réseau à commutation de paquets afin de sécuriser les communications en cas d’attaques nucléaire. De façon très schématique, l’idée de Paul Baran consiste à créer un réseau distribué\*, c’est-à-dire sous forme de toile d’araignée où chaque nœud est relié à plusieurs autres. Pour communiquer sur ce réseau, chaque message est découpé en trame\* contenant les informations nécessaires à son bon acheminement (routage\*), chaque paquet ainsi constitué part du point A et rejoint B en empruntant différents nœuds. Au point B, le message est reconstitué et exploité. Ainsi, si la liaison entre deux nœuds était détruite ou compromise, la transmission pourrait continuer en utilisant un autre canal. La guerre froide et la crainte d’une attaque nucléaire soviétique avaient fait naître le besoin de réseaux résilients, insensibles à la destruction d’un ou plusieurs de ces pions.

Les quatre premiers ordinateurs du réseau ARPANET sont connectés à la fin de l’année 1969, ils permettent de relier le *Stanford Research Institute*, l’université de Santa Barbara et l’université de l’Utah à Salt Lake city (UCLA). Le premier échange entre deux machines n’a permis l’envoi que de trois lettres. Internet n’était pas encore né !

La deuxième étape fondamentale du développement d’ARPANET sous l’égide du département de la défense réside dans la création par Bob Kahn d’un protocole\* capable de transmettre des informations par paquets radio, en s'affranchissant des perturbations. Avec la collaboration de Vinton Cerf, Bob Kahn élabore le célèbre protocole TCP/IP (toujours en vigueur à ce jour, même s’il a été largement amendé). En 1976, le DoD adopte TCP/IP pour son réseau ARPANET composé alors de 111 machines.

**Arobase**

*(at-sign)*

L’arobase ou l’arobe est le symbole @. Il est utilisé dans les adresses de messagerie électronique pour séparer l’identifiant du nom de domaine auquel il est rattaché. Il est couramment utilisé pour désigner un pseudonyme sur Twitter en début d’identifiant (@monsieurX).

**Article Contrôlés de la Sécurité des Systèmes d’Information – ACSSI**

Les ACSSI sont des dispositifs de sécurité mettant en œuvre des logiques cryptographiques qui sont utilisés afin de protéger des informations[[22]](#footnote-23).

En France, l’Instruction générale interministérielle 1300 sur la protection du secret de la défense nationale, précise ainsi que « *certains moyens, tels que les dispositifs de sécurité ou leurs composants, et certaines informations relatives à ces moyens (spécifications algorithmiques, documents de conception, clés de chiffrement, rapports d’évaluation, etc.) peuvent nécessiter la mise en œuvre d’une gestion spécifique visant à assurer leur traçabilité tout au long de leur cycle de vie ainsi que la connaissance de la version logicielle et matérielle. Il s’agit des moyens et des informations, qu’ils soient eux-mêmes classifiés ou non, qu’il est essentiel de pouvoir localiser à tout moment et en particulier en cas de compromission suspectée ou avérée. Ces moyens et informations sont appelés “articles contrôlés de la sécurité des systèmes d’information” (ACSSI)* ».

**ASCII – *American Standard Code for Information Interchange***

ASCII est un standard qui permet de coder des caractères sur huit bits (soit 256 caractères distincts possibles) permettant ainsi leur traitement numérique. Pour autant, ASCII ne définit que 128 caractères (numérotés de 0 à 127) et n’utilise donc que sept bits (le dernier étant placé à 0).Typiquement, lorsque nous saisissons une lettre sur un clavier, l’ordinateur utilise un code pour stocker et manipuler ce caractère. Ainsi, la lettre « a » devient le numéro « 97 » en code ASCII standard, « 61 » en hexadécimal. Les numéros de 0 à 31 ne sont pas affichables, ils sont appelés caractères de contrôle et permettent d’effectuer des actions particulières tel que « espace » (caractère numéro 32), « échappe - ESC » (numéro 27) ou « annulation » (numéro 24). Initialement développé pour la langue anglaise, ASCII ne prévoit pas de caractères accentués, ceux-ci sont codés par le système Unicode, plus complet.

Voir Unicode, UTF, UCS.

**Assembleur**

*(Assembler)*

Le langage assembleur est un langage de programmation de bas niveau (c’est-à-dire très proche du langage interne de la machine), qui permet de transmettre des instructions à un processeur. Il existe plusieurs types de syntaxe en fonction du processeur. Un ordinateur n’interprète que des instructions spécifiques en binaire\* (soit une suite de 0 et de 1), les compilateurs\* sont des programmes conçus pour convertir des programmes de langage évolué (ex. langage C) en langage machine correspondant à une architecture précise (exemple x86). Les instructions en langage machine sont codées et stockées dans la mémoire.

Les commandes comprises par un processeur sont relativement simples : ce sont des opérations avec éventuellement des « arguments » supplémentaires (comme la source ou la destination de la donnée à manipuler). Toute action peut se résumer à des déplacements de données stockées en mémoire, et à des opérations mathématiques sur celles-ci. Le langage assembleur n’est qu’une représentation pour programmeur des instructions machines qui vont être exécutées pas le processeur. Il existe deux syntaxes majoritaires : AT&T et Intel. En pratique, le langage assembleur n’est utilisé que pour des portions de code critiques, pour exploiter des fonctions atypiques du processeur, ou pour effectuer une rétro ingénieurie d’un code compilé.

Voir Compiler.

**Asymétrie**

*(Asymetric)*

Dans le domaine militaire, l’asymétrie qualifie des relations entre acteurs dont les attributs de puissance sont de nature différents. Ainsi, les combats asymétriques décrivent des affrontements mettant face à face des forces ne conduisant pas le même type de combat (forces régulières contre partisans par exemple). La terminologie militaire française en donne ainsi la définition suivante, disparité totale ou très prononcée des buts de guerre, de la nature des moyens et des modes d’action utilisés, au point que les formes de pensée et d’action de l’une des parties restent impuissants à apporter des réponses appropriées aux problèmes posées par le système de pensée de l’autre partie, l’inverse n’étant pas nécessairement vrai[[23]](#footnote-24).

Dans le domaine de la cryptographie*\**, le terme désigne un mode de chiffrement*\** qui utilise des clés*\** distinctes pour chiffrer*\** et déchiffrer\*. Les clés sont dites asymétriques, bien que différentes elles sont mathématiquement liées de sorte qu’il est aisé de déduire la seconde à partir de la première mais très difficile de conduire l’opération inverse. Le couple de clés est généré en même temps, l’une est rendue publique (clé publique\*) l’autre est conservée et permet les opérations de déchiffrement.

Voir Chiffrement.

**ATM – *Asynchronous Transfer Mode***

(Mode de transfert asynchrone)

Technique de transfert de petits paquets de taille fixe (53 octets), appelés, cellule\*, utilisant une commutation et un mode avec connexion[[24]](#footnote-25).

Voir Mode de transfert asynchrone.

**Attaque**

*(Attack)*

Dans la doctrine militaire française, l’attaque se définit comme « l’acte essentiel de la manœuvre offensive visant par la combinaison du feu et du mouvement, soit à détruire un ennemi déterminé, soit à le chasser des zones qu’il occupe en lui infligeant le plus de pertes possibles ». En sécurité informatique, une attaque désigne plutôt une série d’actions techniques qui vise à accéder sans autorisation à un système d’information ou à perturber son fonctionnement normal. L’attaque informatique se caractérise par l’exploitation d’une faille*\** (ou d’un ensemble de failles) sur la cible afin de produire un effet.

**Attaque par canal auxiliaire**

*(Side channel attack)*

Le principe d’une attaque par canal auxiliaire repose non pas sur l’attaque directe du mécanisme de sécurité, mais sur son implémentation matérielle. Ainsi, si le mécanisme de chiffrement RSA\* est mathématiquement très robuste, il n’en demeure pas moins que des mécanismes de sécurité utilisant cette méthode peuvent être attaquées avec succès. C’est, par exemple, l’analyse précise du fonctionnement du processeur qui peut révéler une clé de chiffrement. On peut alors dresser la typologie suivante :

Attaque par mesure de la consommation électrique (ou du rayonnement électromagnétique) ;

Attaque par temps de calcul (ou temporelle) ;

Attaque par faute (il s’agit d’introduire des erreurs pour provoquer de nouveaux calculs et ainsi dériver des clés) ;

Analyse acoustique.

Les parades sont déployées par les producteurs de puces utilisées dans les systèmes cryptographiques. Ainsi, pour lutter contre les attaques temporelles, des nombres aléatoires pour effectuer des calculs inutiles sont générés.

Les parades sont de deux ordres : technologiques (conception de mécanismes qui brouillent les signaux écoutés), et algorithmiques. Dans ce dernier cas, il s’agit de concevoir des algorithmes dont le déroulement est indépendant de la composition de la clé.

**Attaque par déni de service (DOS) et déni de service distribué (DDOS)**

*(Denial of service – Distributed denial of service)*

Le déni de service est un type d’attaque informatique qui vise à rendre indisponible un ou plusieurs services. Le déni de service peut utiliser une vulnérabilité logicielle ou matérielle mais on peut également saturer les ressources critiques (bande passante, ports disponibles, mémoire) et ainsi limiter ou interdire l’accès à une ressource[[25]](#footnote-26).

Lorsqu’il est conduit par plusieurs machine qui font converger leurs requêtes vers une seule on le qualifie de distribué (déni de service distribué – DDOS). Il est impossible de se prémunir totalement d’une attaque par saturation car elle n’exploite pas nécessairement une faille mais « pousse les limites » du fonctionnement normal de certains protocoles\* de communication entre machines. Il est toutefois possible d’en diminuer les effets en organisant la redondance, en effectuant des bascules de charge ou en filtrant les requêtes, etc.

**Attaque par point d’eau**

*(Watering hole – water holing)*

Technique d’attaque qui consiste à piéger un site Internet légitime afin d’infecter les machines des visiteurs[[26]](#footnote-27). Cette technique est généralement utilisée dans les attaques ciblées. Dans ce cas, des sites associatifs ou dédiés à des centres d’intérêts particuliers sont piratés (exploitation de vulnérabilités présentes sur ces sites) et les visiteurs sont alors contaminés. Première étape de l’attaque, le « point d’eau » permet alors de se procurer des identifiants et des données personnelles de cibles et généralement des paramètres de connexions vers des réseaux professionnels plus sensibles. Le terme utilise l’analogie avec une technique de chasse (ou de braconnage) en Afrique : les animaux ayant besoin de se regrouper autours de rares points d’eau, la technique consiste, pour les chasseurs à patienter autour jusqu’à l’arrivée de leurs cible. Ce faisant, ils évitent la longue et fastidieuse phase de pistage et de traque.

**Attribution**

*(Attribution)*

Action technique qui consiste à déterminer l’origine d’une attaque informatique. L’attribution est à distinguer de l’imputation qui elle est un acte juridique qui attribue la responsabilité d’une action malveillante.

**Audience**

*(Audience)*

L’audience regroupe l’ensemble des personnes touchées par un vecteur de communication. Dans les opérations d’information\* (OI) on parlera ainsi d’audience cible pour définir les populations vers qui le message est diffusé ou sur lesquelles il est censé avoir un effet.

**Audit**

Il existe de nombreuses définitions de l’audit en fonction du contexte. Dans le cas des systèmes d’information, l’ANSSI le définit, au sein de son référentiels d’exigences, comme un processus systématique, indépendant et documenté en vue d’obtenir des preuves d’audit\* et de les évaluer de manière objective pour déterminer dans quelles mesure les critères d’audit\* sont satisfaits[[27]](#footnote-28). Le référentiel d’exigences présente par ailleurs plusieurs types d’audit :

• L’audit d’architecture, consiste en la vérification de la conformité des pratiques de sécurité relatives au choix, au positionnement et à la mise en œuvre des dispositifs matériels et logiciels déployés dans un système d’information à l’état de l’art ainsi qu’aux exigences et règlements internes de l’audité. L’audit peut être étendu aux interconnexions avec des réseaux tiers, et notamment Internet.

• L’audit de configuration a pour vocation de vérifier la mise en œuvre de pratiques de sécurité conformes à l’état de l’art et aux exigences et règles internes de l’audité en matière de configuration des dispositifs matériels et logiciels déployés dans un système d’information. Ces dispositifs peuvent notamment être constitués des équipements réseau, des systèmes d'exploitation (de serveurs ou postes de travail), des applications ou des produits de sécurité.

• L’audit de code source, consiste en l’analyse de tout ou partie du code source ou des conditions de compilation d’une application dans le but d’y découvrir des vulnérabilités, liées à de mauvaises pratiques de programmation ou des erreurs de logique, qui pourraient avoir un impact en matière de sécurité.

• Audit organisationnel et physique : L’audit de l’organisa­tion de la sécurité logique et physique vise à s’assurer que les politiques et procédures de sécurité définies par l’audité pour assurer le maintien en conditions opérationnelles et de sécurité d’une application ou de tout ou partie du système d’information sont conformes au besoin de sécurité de l’organisme audité, à l’état de l’art ou aux normes en vigueur ; elles complètent correctement les mesures techniques mises en place ; elles sont efficacement mises en pratique ; les aspects physiques de la sécurité de l’application ou du système d’information sont correctement couverts[[28]](#footnote-29).

Voir Preuve d’audit, Critère d’audit.

**Auditabilité**

Propriété d’un système d’information\* (SI) apte à être audité. Typiquement pour un système d’information, l’auditabilité se caractérise par la capacité à détecter et enregistrer des évènements définis (à l’avance).

Voir Audit, Critère d’audit.

**Authenticité**

*(Authenticity)*

Si la définition classique parle de l’authenticité comme du caractère de ce qui est exact, le terme recouvre en sécurité réseau et cryptographie\* d’autres aspects. L’authenticité d’un message indique ainsi qu’il émane bel et bien de la source indiquée. L’authenticité est donc intimement liée à l’identité et sa vérification fait l’objet de mécanismes techniques particuliers. Avec l’intégrité, et la confidentialité, l’authenticité est une caractéristique essentielle de la sécurité des échanges. Voir Authentification.

**Authentification**

(*Authentication*)

Les mécanismes d’authentification permettent à un système de s’assurer de l’identité de celui (individu ou équipement informatique) qui cherche à accéder à une ressource, afin de contrôler que l’accès lui est autorisé. L’authen­tification se distingue de l’identification, qui permet uniquement de déclarer une identité. Ainsi, l’identification déclare une identité (je dis qui je suis) et l’authentification s’assure du contrôle de l’identité déclarée (je suis bien celui que je prétends être). Il faut donc disposer et présenter des preuves permettant d’assurer ce contrôle d’identité. Les preuves d’une identité peuvent être assurées de différentes façons, en démontrant par exemple :

• Un élément que je suis le seul à connaître (un secret personnel comme un mot de passe) ;

• Un élément que je suis le seul à posséder (un élément physique comme une carte à puce, ou un fichier tel qu’un certificat électronique\*) ;

• Ce que je suis (un identifiant biométrique comme une empreinte digitale ou rétinienne).

Il existe en outre plusieurs types d’authentification qui se déclinent comme suit :

• L’authentification simple : une seule preuve est nécessaire (le plus souvent un élément que je suis le seul à connaître comme le mot de passe) ;

• L’authentification forte : deux preuves, au moins, de natures différentes, doivent être apportées  (par exemple disposer d’une carte à puce et d’un mot de passe);

• L’authentification unique : dans ce cas une seule authentification de l’usager lui permet d’accéder à plusieurs ressources.

**Autoclave**

En cryptographie\*, une méthode de chiffrement est dite autoclave si elle utilise tout ou partie du message clair comme clé de chiffrement\*. Le terme est issu du latin *auto* (de lui-même) et *clavis* (la clé).

Voir Chiffrement.

***Autonomous System* - AS**

(Système autonome)

Un AS est un ensemble de réseaux au sein duquel la politique de routage est cohérente. Ainsi, dans un AS, la politique de routage est définie par une même autorité administrative. (il s’agit en général d’un opérateur de communications électroniques et typiquement un fournisseur d’accès à Internet - FAI\*). La politique de routage interne à l’AS utilise des protocoles particuliers de la famille IGP\* - *interior Gateway* *Protocol*, alors que la gestion du dialogue entre AS utilise pour sa part un protocole de type EGP – *Exterior Gateway Protocol,* le plus souvent *BGP*\* - *Border Gateway Protocol*. Selon la RFC\**\** 4893, chaque AS est désigné par un numéro (ASN) délivré par les Registres Internet Régionaux*\** - RIR. Internet comptait 5000 AS en 1999 et plus de 45000 en 2014.

Voir BGP, Routage.

**Autorité de certification**

*(Certification Authority –CA)*

Les échanges numériques sont basés sur la confiance entre les acteurs (clients-serveurs\*) et nécessitent donc de disposer de moyens de vérification d’identité. La cryptographie\* nous permet de réaliser des échanges sécurisés mais la confiance à accorder à un site ou une personne peut encore être sujette à caution. L’autorité de certification est donc un organe de confiance qui s’engage auprès des acteurs en établissant des certificats\* numériques. Ces certificats assurent, entre autre, que l’identité a bien été vérifiée. Ils lient une identité avec une clé cryptographique publique (cette dernière permet au minimun d’authentifier une signature numérique\* émise par ladite entité). Les certificats peuvent avoir un champ d’action et de validité limité (dans les usages comme dans le temps). L’autorité de certification, créé, délivre et gère les certificats électroniques. Par ailleurs elle signe les dits certificats avec sa clé privée\* afin de garantir leur intégrité assurant ainsi que les données du certificat n’ont pas été modifiées.

En France l’usage de la signature électronique\* et donc de certificats\* dans le cadre des marchés publics, est encadré par l’arrêté du 15 juin 2012 relatif à la signature électronique dans les marchés public – NOR EFIM1222915A.

Voir Certificat électronique\*.

**Autorité d’homologation**

Personne physique ou morale qui, après instruction du dossier d’homologation, prononce l’homologation de sécurité du système d’information, c’est à dire prend la décision d’accepter les risques résiduels identifiés sur le système.

**Avatar**

*(Avatar)*

L’avatar est une représentation d’une personne physique dans la sphère numérique. Il peut s’agir d’un personnage en trois dimensions dans un jeu vidéo ou d’une toute autre représentation symbolique associée au pseudonyme ou à l’identité réelle de l’usager. L’avatar procède de l’identité numérique d’une personne physique, il en est une forme sans prétendre l’incarner.

**AXFR – Transfert de zone DNS complet**

AXFR est un mécanisme de transfert de zone DNS\* défini par les RFC\* 1034-1935 et RFC 5936.

Voir Transfert de zone DNS.

**Ayant droit**

Personne morale détenant un droit dérivé du droit d’auteur (*copyright*). Sauf exception, il est interdit d’exploiter, copier ou diffuser une œuvre sans l’accord des ayants droits. L’arrivée du numérique et des possibilités de copie et d’échange à grande échelle a replacé sur le devant de la scène la question du droit d’auteur. Les sites d’échanges (vidéo, musique, logiciel, livre numérisé) et les plateformes *peer to peer* (pair à pair\*) sont ainsi devenus les cibles prioritaires des ayants droits soucieux de préserver leurs revenus d’exploitation des œuvres. L’action de télécharger gratuitement des œuvres numériques protégées par le droit d’auteur (films, musiques, livres) est, en France, un délit depuis la loi Création et Internet (loi n°2009-669 du 12 juin 2009).

Voir HADOPI.

# B

1. ***Backbone* *Internet***
2. (Dorsale Internet)
3. Le terme désigne les liaisons très haut débit qui constituent le cœur du réseau Internet. Il s’agit principalement des câbles terrestres et sous-marins qui relient les continents entre eux et permettent donc l’interconnexion des réseaux de plus petite taille.
4. ***Backdoor***
5. (Porte dérobée)
6. Les *backdoors* désignent des accès cachés sur un système ou sur une application présents dès la conception ou à la suite d’une implantation malveillante a posteriori. L’objec­tif est de générer un comportement particulier après l’activation par une commande spécifique. L’utili­sa­tion d’une *backdoor* permet donc à un acteur tiers (par exemple un attaquant informatique) de disposer d’un accès sur un système à l’insu de son propriétaire.
7. **Balayage de ports**
8. *(Ports scanning)*
9. Le balayage de ports\* est une technique utilisée en sécurité informatique qui consiste à envoyer des paquets\* vers les différents ports\* d’une machine. La réponse de la machine permet de déterminer l’état des différents ports (ouverts, fermés, filtrés) ainsi que les services fonctionnant.
10. Voir Port, Scan, Ping.
11. **Balise**
12. *(Tag)*
13. Dans un langage de description de documents, marque destinée à l’identification, la description ou la mise en forme d’un élément de document[[29]](#footnote-30). Le format de notation XML\* utilise, par exemple, des balises pour structurer et faciliter le traitement des informations.
14. Voir XML, HTML.
15. **Balise (voie)**
16. *(Beacon Channel)*
17. En téléphonie mobile, il est nécessaire de gérer et partager entre utilisateurs la bande radio (qui est une ressource rare et donc…chère). Pour ce faire, il faux disposer de canaux logiques entre le mobile et la station de base afin de garantir le service. Dans ce cadre, la voie balise permet au mobile de se raccrocher en permanence à la station la plus favorable. Le mobile mesure en permanence la puissance en réception de la voie balise et scrute les autres voies pour connaître les autres stations susceptibles de l’accueillir si nécessaire.
18. **Balisage**
19. *(Beaconing)*
20. Signal\* envoyé (à intervalle régulier en général) par un système vers un autre au sein d’un réseau. La norme 802.11 (Wifi\*) définit, dans son mode infrastructure, une hiérarchie entre le point d’accès\* et les stations. Ainsi, dans un réseau sans fil en mode infrastructure, le point d’accès (box) diffuse régulièrement une trame\* balise (*beacon*) donnant les informations nécessaires au rattachement des stations. Toute les 0,1 secondes, une trame indiquant les caractéristiques du point d’accès est diffusée, on y retrouve généralement le BSSID et l’ESSID (si l’option n’est pas désactivée).
21. Dans le contexte d’une attaque informatique, le *beaconing* caractérise le signal envoyé par un système infecté vers une infrastructure de contrôle afin de signaler à l’attaquant que la contamination est active. L’attaquant peut alors transmettre des commandes vers la victime. Le même phénomène est également appelé *heartbeat* dans la terminologie anglaise.
22. **Bande de fréquence banalisée**
23. *(Citizen’s band – CB)*
24. Bande de fréquence publique, elle est mise à disposition du public dans des conditions déterminées pour assurer, à titre privé et avec des émetteurs de faible puissance, des communications personnelles[[30]](#footnote-31).
25. **Bande passante**
26. *(bandwidth)*
27. En informatique et réseaux, la bande passante désigne un débit d’informations, il s’agit d’un débit binaire\* maximal sur le canal de communication. C’est une donnée qui est généralement utilisée par les fournisseurs d’accès\* pour désigner le débit maximal d’un abonnement (en bits par seconde, ou en octets par seconde, en bauds).
28. En téléphonie analogique\*, elle caractérise la largeur d’une voie de transmission et se mesure en Hertz (Hz).
29. Pour une fibre optique\*, la bande passante représente la fréquence maximale de transmission pour laquelle le signal subit un affaiblissement\* de 3dB. Cette bande passante dépend donc des paramètres physiques de la fibre et des paramètres de transmission (longueur d’onde). La Commission Electrotechnique Internationale\* la définit comme la bande de fréquence dans laquelle l’affaiblissement reste inférieur à une valeur spécifique[[31]](#footnote-32).
30. **Banque de données**
31. *(Data bank)*
32. Ensemble de données relatif à un domaine défini de connaissances et organisé pour être offert aux consultations des utilisateurs[[32]](#footnote-33). A ne pas confondre avec une base de données\*.
33. Voir Base de données.
34. **Barrière**
35. Dans le cadre de la défense en profondeur\* d’un système d’information, une barrière est un moyen de sécurité capable de protéger une partie du système d'information contre au moins une menace. Une barrière peut être humaine, procédurale ou technique, statique ou dynamique, manuelle ou automatique. Elle doit bénéficier d'un moyen de contrôle de son état[[33]](#footnote-34).
36. Voir Défense en profondeur.
37. **Base de données**
38. *(Data base)*
39. Ensemble de stockage de données structurées. La structuration en base permet de parcourir rapidement des données ou d’effectuer des requêtes exhaustives. L’organi­sation, la gestion et la sécurité des bases de données doivent faire l’objet d’une attention particulière au sein d’un système d’information. Enfin, les bases de données sont au cœur du développement du marché de la donnée\* et de son exploitation dans le cadre notamment du *big data\**.
40. Voir SQL, *Big data*, *Data minig.*
41. ***Bash - Bourne Again Shell***
42. *Bash* est un interpréteur de commandes (*shell\*)* qui permet à un utilisateur d’interagir avec un système d’exploitation\* par l’intermédiaire de lignes de commandes. Il permet par exemple, de passer des instructions au système d’exploitation (opérations de fichiers), mais il possède également les attributs d’un langage de programmation. *Bash* est un outil intégré dans la majorité des distributions\* Linux et de nombreux autres systèmes (Mac OS X, systèmes embarqués).
43. **BECN *Backward explicit congestion notification***
44. Dans un réseau *Frame Relay*\*, le BECN est un bit\* d’en-tête de trame\* transmis par le destinataire pour avertir la source de problèmes de congestion. La source doit donc limiter ou réduire les envois vers la destination afin d’éviter l’engorgement du réseau et des pertes de paquets. Le FECN\*, *Forward Explicit Congestion Notification*, est le mécanisme inverse.
45. **BGP - *Border Gateway Protocol***
46. BGP est un protocole de routage\* entre Systèmes Autonomes\* (AS), il est défini par le standard RFC\* 4271. BGP est donc responsable du routage sur Internet entre opérateurs, il échange des informations entre routeurs sur l’accessibilité entre AS (les préfixes\*). Ces informations permettent aux routeurs de connaître les « parcelles » d’Internet accessibles à chaque AS. Les routeurs voisins BGP utilisent TCP\* comme protocole de transport via une session\* sur le port\* 179.
47. Les routeurs BGP sont appelés annonceurs (ils annoncent des routes à leurs voisins).
48. BGP n’est pas directement accessible aux particuliers, il constitue l’ossature du transit Internet mondial. La sécurité de ce protocole est essentielle à la bonne connectivité mondiale et la moindre défaillance de BGP a des conséquences importantes.
49. ***Pour aller plus loin***
50. BGP se divise en réalité en deux familles, eBGP et iBGP pour *exterior* BGP et *interior* BGP. La première gérant les liaisons entre AS et iBGP les annonces de routes entre routeurs au sein d’un même AS. Ainsi, les routeurs de bord d’AS échangent leurs informations de routage en iBGP, alors que eBGP relie point à point des routeurs d’AS différents (mais également sur la périphérie).
51. Un processus BGP échange 5 types de messages distincts :
52. • OPEN : message initial pour échanger les numéros d’AS ;
53. • KEEPALIVE : demande de maintien de session ouverte (l’absence de message KEEPALIVE ou UPDATE pendant 90 secondes entraine la fermeture de la session) ;
54. • UPDATE : mise à jour - annonce ou retrait de routes ;
55. • NOTIFICATION : fin de session BGP ;
56. • ROUTE REFRESH : demande de ré-annonce de route. [RFC 2918].
57. Les informations de routes sont associées à des attributs de types différents qui serviront ensuite à déterminer les meilleures routes.
58. Les 4 types d’attributs sont :
59. • WM : *well known mandatory*: ces attributs doivent être pris en charge et diffusés ;
60. • WD : *Well known discretionary*: attributs qui doivent être pris en charge mais dont la propagation est optionnelle ;
61. • OT *Optional Transitive*: attribut qui n’est pas nécessairement pris en charge mais à propager ;
62. • ON *Optional Nontransitive*: pas nécessairement pris en charge ni propagés, ces attributs peuvent être ignorés.
63. **Exemple d’attributs :**
64. L’AS PATH est un attribut WM, donc à prendre en charge et à diffuser, il liste et ordonne les différents AS traversés. Il permet ainsi de rejeter des routes qui seraient reçues d’un voisin mais qui contiendrait déjà le numéro d’AS. Ce rejet évite la création de boucles dans le routage.
65. Next Hop, est de type WM également, il précise l’adresse IP du « voisin » eBGP (donc sur l’AS suivant).
66. *Weight* est un attribut spécifique de type ON (extension CISCO) qui pondère les routes afin de créer de préférences locales.
67. *Local pref* est un attribut WD pour les routeurs internes afin de préférer certaines routes externes.
68. Pour effectuer des choix, lorsque plusieurs routes vers une destination sont possibles, BGP utilise les attributs spécifiques pour effectuer le choix de la meilleure route.
69. **Bibande**
70. *(Dual band)*
71. Dans la téléphonie mobile, un terminal bibande est un téléphone capable de fonctionner sur l’une ou l’autre des bandes de fréquences accordées au système GSM\*. En Europe il s’agit des bandes autour de 900 et 1800 MHz.
72. Voir GSM.
73. **Bien informationnel (patrimoine informationnel)**
74. Expression issue du monde de l’intelligence économique et progressivement adoptée par le milieu de la sécurité. Le patrimoine informationnel de l’entreprise regroupe l’ensemble des informations qui peuvent présenter un intérêt pour un concurrent. Ces données recouvrent ainsi ce qui relève de la recherche et développement, les négociations contractuelles, les données administratives des employés, les données comptables… Le spectre est donc souvent assez large. Dans tous les cas, le patrimoine informationnel de l’entreprise doit faire l’objet de mesures de protection adaptées.
75. Ces données sont donc un « actif » de l’entreprise qui, bien souvent, n’en a pas forcément conscience. Au-delà de la protection de ce patrimoine, l’entreprise doit également s’attacher à valoriser ce patrimoine, c’est à dire, mettre en place des actions pour créer de la valeur à partir de ces informations.
76. ***Big Brother***
77. Dans le roman de George Orwell, *1984* paru en 1949, *Big Brother* désigne le personnage à la tête du Parti et dirigeant l’Oceania. Le Parti et *Big Brother* assurent une surveillance permanente sur la population. Par extension, l’expression *Big Brother* désigne tout système qui limiterait les libertés individuelles. Ce terme a ainsi été utilisé pour qualifier les programmes de surveillance de masse de l’Internet de la NSA\*, dévoilés par Edward Snowden.
78. ***Big data***
79. (Données de masse - mégadonnées)
80. Terme qui désigne des volumes de données très importants générés ou agrégés par les systèmes d’information et qui dépassent les capacités de traitement des systèmes courants. Une étude d’IBM estime ainsi qu’en 2014, 2,5 trillions d’octets de données sont générées dans le monde, 90% des données existantes aujourd’hui ont été créées durant les deux dernières années… Le problème des « *big data*» est donc à la fois lié au volume, mais également à la vitesse de création de nouvelles données et donc à terme, à la mémoire et aux besoins associés au stockage. Il est alors courant de caractériser les mégadonnées par l’ex­pres­sion « 6V », qui regroupe : Volume, Variété, Vitesse, Visibilité, Valeur et Véracité[[34]](#footnote-35). L’expression « *big data*» s’applique également aux solutions de traitement de volumes importants d’informations. Il s’agit alors de développer des algorithmes et technologies qui permettent de parcourir le volume de données, leur variété et de supporter la rapidité de création et de modification. Cette capacité d’exploration et d’extraction est également appelée *data minig\*.* Les grands groupes du web ont rapidement investi ce champ de recherche. Les technologies développées visent à réduire le temps de traitement sur les bases de données très importantes. On peut ainsi distribuer le traitement sur une infrastructure de serveurs, ce sont alors les traitements dits « massivement parallèles » et combiner avec des systèmes d’organisation de bases de données (NoSQL).
81. Voir SQL, *data minig,* base de données*.*
82. **Bimode**
83. *(Dual mode)*
84. En téléphonie, un terminal bimode est un téléphone capable de fonctionner suivant plusieurs technologies distinctes et donc plusieurs protocoles\* (ex GSM\* et UMTS\*).
85. **Binaire**
86. *(Binary)*
87. En mathématique le binaire est un système de numération en base 2. Dans ce système, les nombres sont donc codés à l’aide de deux signes, 0 et 1. Les nombres sont décomposés en puissance de 2. Ainsi, en binaire, 2 (décimal) devient 10, car 2 se décompose en 1 x 21 + 0 x 20.
88. 11 (décimal) se décompose lui en 1 x 23+ 0 x 22 + 1 x 21 + 1 x 20, soit 1011 en binaire.
89. En informatique et télécommunication, le binaire est central car le bit\* ne prend que deux valeurs 0 ou 1. Le langage machine doit donc s’appuyer sur le binaire car les processeurs des ordinateurs ne gèrent, pour l’heure, que deux états.
90. Voir également Code, Ordinateur quantique.
91. **BIOS – *Basic Input Output System***
92. En informatique le BIOS est un programme stocké sur la carte mère\* d’un ordinateur. C’est le premier programme chargé en mémoire lors du démarrage de l’ordinateur, il permet d’effectuer un certain nombre de tests sur la carte mère avant de lancer le système d’exploitation\* (OS).
93. **Bitcoin**
94. Le bitcoin est une « monnaie virtuelle » ou « crypto monnaie » lancée le 1er novembre 2008. Le terme désigne à la fois une unité de compte pour les échanges entre pairs mais également le système de paiement dans cette devise lorsqu’il est écrit avec une majuscule (Bitcoin). Le système est qualifié de pair à pair\*, il n’existe en effet aucune autorité centrale (banque centrale ou Etat) qui en régule le cours. Les règles qui organisent l’émission de monnaie (la création de bitcoins) reposent sur un code informatique publié sous licence libre. Sans cotation officielle, le cours du bitcoin est assez volatile, il a connu une véritable explosion passant de 0,06€ au mois d’août 2010 à 28€ un an plus tard. Au début du mois de novembre 2013 un bitcoin s’échangeait 234€ le cours s’enflamme et atteint 919€ début décembre. Les banques centrales et les Etats s’intéressent alors au phénomène des monnaies virtuelles, soulignant bien souvent les risques associés à leur usage. Ainsi en France, un rapport d’information du Sénat présente, en 2014, le bitcoin comme un phénomène illustratif de l’impact de la « révolution numérique » sur certains secteurs économiques :
95. Avec les monnaies virtuelles, c’est un élément plus fondamental encore qui est remis en cause : le monopole d’émission des banques centrales, manifestation par excellence du pouvoir régalien et clé de voûte de la politique monétaire. Exemple le plus connu et le plus « réussi », le bitcoin, créé en en 2009 par Satoshi akamoto, se veut une alternative libre, anonyme et décentralisée, permettant aux utilisateurs d’échanger entre eux des biens et des services sans avoir recours à la monnaie classique. Stricto sensu, toutefois, il ne s’agit ni d’une monnaie ayant cours légal, ni d’un moyen de paiement au sens du code monétaire et financier (CMF) : contrairement à la « monnaie électronique », le bitcoin n’est pas émis contre la remise de fonds. Il est un support de transactions. Pour l’instant, le bitcoin relève avant tout d’une forme de troc en version numérique. Toutefois, vos rapporteurs estiment que l’on ne peut écarter d’un revers de main cette innovation, sous prétexte qu’il ne s’agirait que d’un épiphénomène. Le bitcoin connaît un succès croissant auprès des e-commerçants tels que le voyagiste Expedia ou encore l’éditeur de blogs WordPress, et il est désormais accepté par service de paiement en ligne PayPal.
96. Si le bitcoin connaît un tel développement, c’est qu’il présente des avantages tangibles, en dépit de risques clairement identifiés[[35]](#footnote-36).
98. **Blogue**
99. (*blog*)
100. Journal personnel publié sur Internet dans lequel sont partagés des textes, des photos et des vidéos. L’accès est public.
101. **Blogueur**
102. *(blogger)*
103. Individu qui anime un blogue.
104. **Blogosphère**
105. *(blogosphere)*
106. Sous-ensemble du *World Wide Web* qui regroupe les blogues, le terme désigne également la communauté des blogueurs. La blogosphère peut être qualifiée et spécialisée : francophone, politique, économique, mode, universitaire… Pour chaque domaine il existe des classements de notoriété permettant d’identifier les personnages influents et les blogues à suivre.
107. **Bluetooth**
108. *(Bluetooth)*
109. Technologie établie pour les réseaux sans fil\* à faible portée (quelques dizaines de mètres au plus). Elle permet de relier les téléphones mobiles, les casques d'écoute, les ordinateurs et les périphériques. Cette technologie a été normalisée en 2005 pour sa version 1.2 par l’IEEE 802.15.1 – 2005. La communication radio Bluetooth utilise la modulation de fréquence (GFSK – *Gaussian Frequency Shift Keying*) et divers algorithmes de correction d’erreurs. Sur le plan physique, on retrouve des technologies de saut de fréquence (FHSS\*) qui minimisent les interférences sur 79 canaux dans la bande 2,402 – 2,480 GHz. Les appareils connectés forment un picoréseau\* de type maître-esclave. Le maître décide des sauts de fréquences de façon pseudo-aléatoire.
110. Les débits ne cessent d’augmenter depuis 1999 (date de la spécification 1.0) et la deuxième génération (2006) passe ainsi de 1 Mb/s à 3 Mb/s.
111. Voir Picoréseau, Réseau sans fil.
112. **Bob**
113. Personnage mythique des origines de la cryptographie. On sait encore peu de choses sur lui hormis le fait qu’il cherche désespérément à communiquer avec Alice. Leurs tentatives illustrent depuis le début des années 70 les cours de cryptographie. Pour en savoir plus voir *Max\*, Eve\**et également Charlie qui depuis le début tentent d’écouter et d’enregistrer ce que Alice et Bob échangent.
114. ***Body Area Network* – BAN**
115. (Réseau corporel)
116. Dans le domaine médical, un BAN est un réseau sans fil composé de télé transmetteurs utilisé sur les patients (ou à proximité) afin d’effectuer des mesures ou des actions particulières. Un réseau BAN répond à la norme IEEE 802.15.6, consacrée à la communication des appareils dans, sur ou autour du corps humain. Utilisé en médicine mais également dans le sport, pour mesurer les performances individuelles, les BAN sont en plein développement.
117. **Bogue**
118. *(Bug)*
119. Un *bug* logiciel est une erreur dans un programme informatique ou un système qui entraine un comportement ou des résultats non attendus. Le résultat d’un *bug* peut-être important et déboucher sur une fermeture inopinée d’un programme, ou du système, des pertes de données…
120. Historiquement, le terme vient d’un dysfonctionnement qui a tenu en haleine les informaticiens concernés… jusqu’à ce qu’ils découvrent qu’un insecte (*bug*, en anglais) mort en était l’origine (matériel et non logiciel, dans ce cas d’espèce). En outre, lorsqu’un *bug* peut être exploité pour contrôler le flot d’exécution du programme concerné, on parle de vulnérabilité\*.
121. **Bombardement de courriels**
122. *(Mail bombing)*
123. Action malveillante qui consiste à envoyer une grande quantité de courriels à un destinataire unique. Il s’agit d’une forme particulière de déni de service\* contre un système de messagerie électronique.
124. Voir Attaque par déni de service.
125. **Bombe logique**
126. *(logic bomb)*
127. Par analogie avec le monde réel et les actions terroristes, une bombe logique est un code malveillant implanté dans un système d’information dont l’objectif est de détruire ou modifier des données lorsque des conditions particulières sont atteintes. La « bombe » peut ainsi être « déclenchée » à une date prédéfinie, lorsque l’utilisateur tape un mot clé ou accède à certaines applications. La terminologie française retient également le terme de bombe programmée[[36]](#footnote-37).
128. **Botnet**
129. *(botnet)*
130. Un *botnet*, ou réseau de machines zombies\*, est un ensemble d’ordinateurs contrôlé à distance par un utilisateur tiers en vue de conduire des attaques distribuées. La taille d’un *botnet* est variable, mais ceux-ci peuvent compter jusqu’à plusieurs milliers de machines réparties dans des dizaines de pays. Un marché du *botnet* s’est constitué et il est possible de louer à l’heure ou à la journée de tels réseaux.
131. **Boucle locale**
132. *(Local loop)*
133. En télécommunication, la boucle locale, également appelé réseau téléphonique local, désigne l’installation qui relie le point de terminaison du réseau chez l’abonné au répartiteur principal ou à toute autre installation équivalente d’un réseau de commutation électronique fixe ouvert au public[[37]](#footnote-38). La réglementation européenne en donne la définition suivante :
134. L'expression boucle locale désigne le circuit physique à paire torsadée métallique du réseau téléphonique public fixe qui relie le point de terminaison du réseau dans les locaux de l'abonné au répartiteur principal ou à toute autre installation équivalente.
135. Le cinquième rapport de la Commission sur la mise en œuvre de la réglementation en matière de télécommunications souligne que le réseau d'accès local demeure l'un des segments les moins concurrentiels du marché libéralisé des télécommunications. Les nouveaux arrivants ne possèdent pas d'infrastructures de réseaux de substitution étendues et ne peuvent pas, en utilisant des technologies classiques, égaler les économies d'échelle et la couverture des opérateurs désignés comme étant puissants sur le marché du réseau téléphonique public fixe. Cette situation est due au fait que ces opérateurs ont, pendant des périodes relativement longues, déployé leurs infrastructures d'accès local métalliques en bénéficiant de la protection de droits exclusifs et qu'ils ont pu financer les dépenses d'investissements grâce à des rentes de monopole[[38]](#footnote-39).
136. **Bribe**
137. *(chip)*
138. En télécommunication, une bribe est, dans un signal\* numérique formé suivant une loi déterminée à partir d’un élément de donnée, une des parties émises successivement, qui possède des caractéristiques distinctes des autres[[39]](#footnote-40).
139. ***Broadcast***
140. (Diffusion générale)
141. En télécommunication, le *broadcast* est une technique qui consiste à envoyer les mêmes informations à tous les utilisateurs qui disposent d’un terminal permettant la réception. Ainsi, un message diffuser en *broadcast* permettra dans certains réseaux de déterminer si un usager particulier est atteignable. La technique permet également de communiquer à l’ensemble des stations réceptrices des éléments techniques particuliers issus de la station émettrice.
142. **Brouillage**
143. *(Jamming)*
144. Le brouillage est une action qui consiste à troubler la réception d’un signal utile par l’émission d’autres signaux venant se superposer au signal utile. Le brouillage est donc la conséquence d’une perturbation électromagnétique ou d’un signal brouilleur (émis intentionnellement). Le brouillage ne doit pas être confondu avec le phénomène d’interférence\*. L’action de brouiller est un des modes d’action de la guerre électronique.
145. **Brute force (attaque par force brute)**
146. *(brute-force – brute-force attack)*
147. Les attaques par force brute recouvrent les méthodes *cryptanalytiques*\* utilisées pour retrouver une *clé de chiffrement*\* ou un mot de passe. C’est une méthode exhaustive (donc très consommatrice en ressources de calcul et qui génère de nombreux *log\** sur le système cible) qui consiste à tester une à une toutes les combinaisons possibles. Ce type d’attaque se justifie si la taille du mot de passe ou de la clé est relativement petite Par ailleurs certains systèmes interdisent un traitement dans l’ordre des différentes possibilités, ce qui oblige à développer des outils pour tester de façon aléatoire les combinaisons. La durée de l’opération dépend donc de la taille de la clé et des capacités de calcul. La puissance de calcul d’un ordinateur personnel permettant aujourd’hui de tester plusieurs millions de combinaisons par seconde. Ainsi un mot de passe de 6 caractères alphanumériques ne résiste guère à ce type d’attaque. Néanmoins, l’ajout d’un bit d’information à la clé multiplie par 2 le temps de calcul, ce qui explique que la cryptanalyse par force brute nécessite des architectures distribuées et des capacités de calcul considérables.
148. Voir *Rainbow table,* Cryptanalyse.
149. **BSS – *Base Station Subsystem***
150. (Sous-système des stations de base)
151. Dans un réseau de téléphonie mobile, le BSS est la partie radio de l’architecture en charge de la connexion entre les stations et la partie réseau en charge de la commutation (typiquement le MSC\* – *Mobile service Switching Center*).
152. **BSSID – *Basic Service Set Identification***
153. Dans une architecture Wifi\*, en mode infrastructure, le BSSID est l’adresse MAC\* du point d’accès codée sur 24 bits.
154. Voir Wifi.
155. **BTS*- Base Transceiver Station***
156. (Station de base)
157. La BTS, ou station de base\*, est un des éléments du système de téléphonie mobile (GSM\*). La BTS est une antenne relai du réseau associée à une cellule\*, elle se compose d’un ou plusieurs émetteurs récepteurs radio d’une part et d’une liaison avec la station de contrôle (BSC\*). Voir Station de base\*, GSM.
158. **Bus**
159. *(Bus)*
160. Un bus est un dispositif qui permet de relier entre eux plusieurs composants (ou matériels) afin de garantir la circulation d’informations. Un bus est un dispositif qui est dit non bouclé, c’est à dire sans retour vers une station principale.
161. Voir Topologie réseau\*.
162. ***Business Intelligence*** **– BI**
163. (Informatique décisionnelle)
164. Ensemble d’outils et de techniques qui assure généralement la collecte, le traitement, la modélisation et la présentation des données relatives à l’activité d’une entité. Le BI, en fournissant une vue globale de la situation et de l’activité concernée, fait partie des outils d’aide à la décision.
165. ***Buzz***
166. Terme anglais qui désigne littéralement le bourdonnement. Utilisé pour désigner une information ou un message qui se diffuse rapidement en ligne et qui alimente les conversations entre usagers. Généralement « faire le *buzz*» consiste à monopoliser l’attention médiatique. Un *buzz* est par nature intense (il dépasse le seuil de bruit ambiant) et de courte durée, quelques heures à quelques jours.

# C

**Câblage**

*(Wiring)*

Action qui consiste à connecter les divers éléments d’un système de communication.

**Cache**

*(Cache)*

Le cache ou mémoire cache est une composante de la mémoire, habituellement plus rapide mais plus limité en taille, qui stocke des données de façon transparente et transitoire afin qu’elles soient retrouvées plus rapidement. Un processeur contient habituellement plusieurs niveaux de cache, de rapidité décroissante et de capacité croissante. La mémoire cache, d’accès plus rapide que la mémoire centrale, est utilisée pour stocker temporairement les données d’une opération arithmétique ou logique.

Dans le cas de la navigation Internet, les données sont stockées localement au sein d'un cache, elles peuvent avoir été consultées préalablement et sont ainsi immédiatement disponible en cas de nouvelles requêtes (ce qui évite d’effectuer une nouvelle résolution DNS\*).

**CALID – Centre d’Analyse et de Lutte Informatique Défensive**

Unité militaire française en charge de la cyberdéfense des réseaux du ministère de la défense. La mission englobe également les forces projetées. Les équipes analysent en temps réels les événements collectés par des sondes réseaux déployées.

**Canal caché**

*(Covert channel)*

Un canal caché est un canal de communication qui permet à un processus malveillant de transférer des informations en exploitant un mécanisme qui n’est pas censé servir à la communication[[40]](#footnote-41). Par exemple : protocoles de signalisation, bits de bourrage, gigue de temps, etc.

**Canal de fréquence**

*(Frequency channel – channel)*

Un canal de fréquence est une partie du spectre des fréquences comprise entre deux fréquences spécifiées et destinée à être utilisée pour une transmission. Il peut être caractérisé par sa fréquence centrale et la largeur de bande associée[[41]](#footnote-42).

**Canal de transmission**

*(Channel)*

En télécommunication, un canal de transmission désigne un ensemble de moyens nécessaires pour assurer une transmission de signaux dans un seul sens entre deux points. On parle également de voie de transmission[[42]](#footnote-43). Ainsi plusieurs voies de transmission peuvent partager un même support physique (câble).

**CAPEC – *Common Attack Pattern Enumeration and Classification***

Développé par le MITRE\*, le CAPEC est une typologie très large des différents modèles d’attaques connues. CAPEC se veut un outil au profit, entre autre, des analystes en charge de la cybersécurité permettant de mieux comprendre les modes d’action des attaquants. On peut effectuer des recherche par domaine d’attaque (exemple : *social engineering\**, *supply chain*, *Software*…) ou par mécanisme d’at­taque (exemple : *flooding*, *sniffing*…). Chaque mécanisme fait l’objet d’une fiche descriptive où l’on retrouve la description de l’attaque, les prérequis nécessaires, les mécanismes de protection éventuels… La base est accessible en ligne à l’adresse : http://capec.mitre.org/ — Voir STIX\*.

***Capture The Flag -* CTF**

(Capture du drapeau)

En sécurité informatique, un CTF est un challenge qui consiste, seul ou en équipe, à s’introduire dans un système d’information désigné et accomplir une action qui prouve l’intrusion.

**Caractérisation**

*(Characterization)*

Pour un composant électronique, la caractérisation est l’action de vérifier la conformité d’un produit à ses spécifications par un ensemble de tests physiques ou électriques.

**Carte électronique**

*(Electronic board)*

En électronique, il s’agit d’un circuit imprimé équipé de composants.

**Carte fille**

*(Daughter board – Daughtercard)*

Carte électronique enfichée sur une autre carte, en général la carte mère[[43]](#footnote-44).

**Carte mère**

*(Mother board – mothercard)*

Carte électronique qui sert de support aux composants principaux d’un ensemble électronique et éventuellement aux cartes filles[[44]](#footnote-45).

**Carte réseau**

*(NIC – Network Interface Card)*

Eléments physiques (composants électroniques) reliés sur circuit imprimé dont la fonction est d’assurer l’interface\* entre la machine à laquelle elle appartient et l’ensemble des autres équipements connectés sur le même réseau.

**Carte SIM**

*(Subscriber Identity Mobile card)*

Carte à puce présente dans les téléphones mobiles (existe également sous format « micro » ou « nano »). Elle con­tient des informations qui permettent l’identification de l’usager sur son réseau ainsi que des paramètres d’accès. Elle contient un processeur et trois types de mémoire (ROM\* – EPROM – RAM\*). La carte SIM contient ainsi les données obligatoires (information administratives, IMSI\*, information de localisation, liste des fréquences radio à utiliser, les derniers réseaux utilisés, la clé de chiffrement Kc), les données de sécurité (clé d’authentification Ki, code CHV1 ou PIN\*) et les données facultatives (raccourcis numéros, opérateur, types de messages acceptés…).

**CASE - *Common Application Services Elements***

Au niveau application du modèle OSI\* (soit la dernière des sept couches du modèle), les CASE regroupent des ensembles normalisés de protocoles utilisables par des applica-  
tions. Connu aujourd’hui sous l’acronyme ACSE – *Application Common Service Elements*.

**CBAC - *Context-Based Access Control***

Le CBAC est une application intégrée aux matériels Cisco (routeurs\*) qui permet le filtrage avancé de sessions de paquets. La CBAC s’obtient par la configuration des listes de contrôle d’accès (ACL\*), il est alors possible de refuser le transfert du trafic et son traitement par l’équipement.

**CBC - *Cipher Block Chaining***

(Chiffrement parenchaînement des blocs)

Mode de chiffrement par blocs utilisé par l’algorithme DES\*. Avec CBC, chaque bloc de données chiffrées est l’opérande d’une opération sur le bloc de données suivant avant le chiffrement de ce dernier, rajoutant ainsi de la complexité aux données chiffrées finales.

Voir Chiffrement.

**CBR - *Constant Bit Rate***

(Taux d’échantillonnage fixe)

Trafic à débit constant. Utilisée pour transmettre des flux numérisés comme la voix ou la vidéo. Un CBR signifie donc qu’une piste audio ou vidéo est encodée avec un taux d’échantillonnage constant. Ce mode est à opposer au VBR\* *variable bit rate*.

Voir VBR.

**CDN - *Content Delivery Network***

(Réseau de distribution de contenus)

Le CDN ou réseau de livraison de contenus est une architecture permettant d’accélérer la diffusion du trafic vers un client en « rapprochant » les contenus de l’usager. Le CDN s’appuie sur un réseau de serveurs sur lesquels l’information initiale est stockée en cache\*. Ce système assure aux sites très fréquentés une meilleure gestion des pics d’affluence, une meilleure répartition du trafic de consultation, et une utilisation optimale de la bande passante\*.

**CEI – Commission Electrotechnique Internationale**

*(IEC - International Electrotechnical Commission)*

La CEI est l’organisme international de normalisation pour les domaines de l’électricité, électronique et des nanotechnologies. Créée en 1906, elle rassemble 60 états membres et 23 associés qui édictent des normes reconnues dans une centaine de pays. On lui doit ainsi la normalisation d’unités de mesure comme le Gauss et l’Hertz.

**Cellule**

*(Cell)*

La cellule en télécommunication fait référence à une zone élémentaire d’un réseau de radio communication à laquelle est affectée un ensemble de fréquences non réutilisables. La cellule désigne ainsi la zone de couverture radio d’une station de base\* (BTS). De cette définition découle l’expression « téléphone cellulaire » employée lors des premiers déploiements de la téléphonie mobile dans les années 90.

Le terme cellule désigne également un paquet\* comprenant un nombre fixe d’éléments binaires dans un mode le transfert asynchrone\*. La cellule est donc l’unité de transport du protocole ATM\*.

**Centre de commutation radio mobile**

Voir MSC.

**CERT - *Computer Emergency Response Team***

Les CERT ou centre de réponse d’urgence aux incidents informatiques, sont des organismes chargés d’assurer, entre autre, la réponse aux incidents de sécurité informatiques détectés. Leurs fonctions dépassent ce cadre car ils établissent et diffusent des bases de données qui répertorient les vulnérabilités. Ils assurent également une fonction de prévention en diffusant des « guides de bonnes pratiques ». Enfin, ils contribuent à une meilleure connaissance de la menace en échangeant leurs informations avec d’autres CERT. Certains CERT ont une vocation privée (industriels, grands groupes), sectorielle, locale ou nationales.

Le premier a été créé aux Etats-Unis par la DARPA\* en 1988 à la suite de l’incident du ver Morris. En France, plusieurs organismes font fonction de CERT. Ainsi, le CERT-FR (successeur du CERTA) dépend de l’ANSSI et a pour principal périmètre les administrations françaises, le CERT-RENATER est le CERT de la communauté des membres du GIP RENATER (Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche), le CERT Société Générale est celui du groupe bancaire du même nom, sans oublier les industriels qui offrent des prestations de réponse à incident.

Le terme CERT est une marque déposée par l’université Carnegie Mellon aux Etats-Unis, son utilisation est en principe soumise à une autorisation et à un enregistrement. Le terme générique associé est CSIRT (*Computer Security Incident Response Team*)*.*

**Certificat**  
*(Certificate)*

Un certificat est un message indiquant qu’une clé publique\* appartient bel et bien à une personne (ou un système). Ce message est signé numériquement à l’aide de la clé privée\* d’une, ou de plusieurs parties de confiance (autorité de certification\* - AC).

Dans le cadre d’un échange électronique (entre un particulier et un serveur de vente en ligne par exemple), un certificat numérique peut être utilisé. Ce certificat est alors un document certifiant l’identité de l’émetteur ou du récepteur (il spécifie également, la date d’expiration du certificat, l’algorithme utilisé et l’autorité de certification). Le vol ou l’usurpation de certificat est donc un mode d’action très efficace pour conduire une attaque car il permet à l’attaquant d’obtenir des droits légitimes.

Les certificats sont essentiels pour l’établissement d’une session\* chiffrée entre un client et un serveur (déclaration d’imposition en ligne par exemple). D’autres sont en revanche utilisés pour l’identification de certains équipement réseau comme des *firewall*\* ou des routeurs\* (dans le cas de certificats IPSEC\*).

Voir Autorité de certification, Chiffrement, signature électronique.

**Certification de sécurité**

Délivrée pour la France par l’ANSSI, une certification de sécurité porte sur des produits de sécurité (matériels ou logiciels). Elle atteste de la conformité d’un produit de sécurité à un niveau de sécurité donné. Il s’agit d’une évaluation à l’état de l’art réalisée en fonction d’une cible de sécurité et d’un niveau de sécurité visé. Elle est matérialisée par un rapport de certification et un certificat tous deux signés par le Directeur Général de l’Agence. Le catalogue des produits de sécurité certifiés, accompagnés de leur cible de sécurité et de leur rapport de certification est publié sur le site Web de l’Agence. On parle de certification « premier niveau » (CSPN) ou de certification « Critères Communs\* ». Cette certification est délivrée par l’ANSSI sur la base des travaux dévaluation menés par un CESTI (Centre d’Evaluation de la Sécurité des Technologies de l’Information). Les CESTI sont des laboratoires accrédités par le COFRAC (Comité Français d’Accréditation) et agréés par l’ANSSI. Le catalogue des CESTI est publié sur le site Web de l’Agence. Au sein de l’ANSSI, c’est le Centre National de Certification de la Sous-direction Expertise qui remplit ces missions[[45]](#footnote-46).

**Certification de sécurité de premier niveau – CSPN**

La Certification de Sécurité de Premier Niveau (CSPN) mise en place par l’ANSSI en 2008 consiste en des tests en « boîte noire » effectués en temps (2 mois) et charge (25 ou 35 hommes x jours) contraints. La CSPN est une alternative aux évaluations Critères Communs, dont le coût et la durée peuvent être un obstacle, lorsque le niveau de confiance visé est moins élevé[[46]](#footnote-47).

**Chapeau blanc – chapeau noir**

(*whitehat - blackhat*)

Terminologie utilisée pour désigner différents groupes de hackers\* en fonction de leurs intentions. Ainsi, *whitehat* désigne un hacker cherchant à améliorer la sécurité d’un système, les éditeurs concernés sont prévenus puis les failles découvertes publiées. A l’inverse, le *blackhat* cherche à nuire, et à générer des profits des découvertes qu’il peut faire. Cette distinction est évidemment très réductrice et fait l’objet de nombreuses polémiques sur la toile.

Le terme *blackhat* désigne également une société organisatrice de conférences de sécurité informatique. Ces conférences très originales et attendues par la communauté de la sécurité regroupent de nombreux experts dont plusieurs hackers de renom. Chaque conférence est le lieu privilégié pour de nouvelles révélations sur ce qu’il est possible de faire (hacker un système de navigation, une voiture…) et présenter des « preuves de concepts » qui seront ensuite discutées. Cet événement se tient annuellement à Las Vegas en marge d’une autre conférence de sécurité plus académique la Defcon\*. Amsterdam et Tokyo accueillent également une *blackhat*.

**Chaos Computer Club (CCC)**

Le Chaos Computer Club est une association de hackers\* née dans les années 80 à Berlin, qui milite pour la liberté de l’information et de la communication. Le CCC est ainsi une plateforme de dialogue et d’échange pour hackers principalement active en Europe. L’histoire du groupe est entourée de zones d’ombre en raison des liens (réels ou supposés) de ses membres avec certains services de renseignement (des membres du CCC auraient revendu au KGB des données dérobées sur un site de l’OTAN en 1989). Un congrès annuel également baptisé CCC (*Chaos Computer Congres*) a lieu à Berlin ou Hambourg et réunit de nombreux experts en sécurité.

**Cheval de Troie**  
*(Trojan)*

En informatique, un cheval de Troie est un programme malveillant\* caché dans un autre réputé sûr aux yeux de l’utilisateur. Un cheval de Troie peut voler des mots de passe, copier des données sensibles, ouvrir une brèche dans un réseau en autorisant des accès à des parties protégées. Le cheval de Troie n’est pas nécessairement un virus\* car il n’a pas forcément vocation à se reproduire pour infecter d’autres machines. Le mode de propagation le plus classique demeure la messagerie électronique en utilisant une pièce jointe infectée. Il existe deux types de chevaux de Troie qui diffèrent essentiellement sur le mode de prise de contrôle par le hacker. En connexion directe (peu fréquent) il est nécessaire de disposer de l’adresse IP\* de la cible afin d’établir la liaison, en mode *remote connexion* c’est l’ordinateur de la victime qui va se connecter de façon autonome à l’ordinateur du pirate.

**Chien de garde**

(*watchdog*)

Association informelle, individus ou ONG, qui pratiquent une veille thématique ayant pour objectif de dénoncer les abus ou les détournements. Leurs activités touchent ainsi le comportement des entreprises (dénonçant l’usage d’enfants ou les conditions de travail précaires), les gouvernements et les médias. Le groupe « *copwatch*» par exemple, surveille en permanence le comportement des forces de police aux Etats-Unis, filmant les interpellations et dénonçant les comportements inappropriés.

En informatique industrielle, un chien de garde désigne un dispositif électronique ou logiciel qui s’assure qu’un processus de traitement ne demeure pas bloqué à une étape particulière. Il vérifie ainsi que certaines conditions de fonctionnement sont remplies et peut donc contribuer à la défense d’un système d’information ou de production.

**Chiffrement**  
*(Encryption)*

Le chiffrement est un processus cryptographique qui vise à modifier une information afin de la rendre inintelligible, tout en permettant un retour à sa forme initiale. Il s’agit donc de dissimuler le sens d’un message afin d’augmenter sa confidentialité. Dans ce cadre le chiffrement est l’action qui consiste à transformer un message clair en un autre qui sera dit chiffré. L’action inverse est appelée déchiffrement.

La sécurité du chiffrement réside dans la détention d’un élément secret, la clé. Les méthodes de chiffrement différent de la stéganographie\* où le message est simplement « caché » sur un autre support mais demeure intelligible.

***Pour aller plus loin…***

**Une petite histoire de chiffre, du monoalphabétique au carré de Vigenère**

La dissimulation de l’information est un phénomène ancien, les premières techniques de chiffrement connues remontent ainsi à l’antiquité. David Khan dans son ouvrage, « la guerre des codes secrets » considère qu’une inscription d’un scribe égyptien datant de 1900 av JC et utilisant des hiéroglyphes non conformes à l’usage classique est la première trace de chiffrement de l’histoire qui nous soit parvenue. Pus tard vers 1500 av.JC, des tablettes mésopotamiennes chiffrées contenant des formules pour la réalisation de vernis de poteries ont été réalisées par des artisans babyloniens [Khan,1980]. Le premier exemple de chiffre de substitution est développé par des scribes hébreux pour la transcription du livre de Jérémie entre 600 et 500 av JC. Ce code simple, dit d’Atbash (ville où il aurait été imaginé) est une substitution simple monoalphabétique de l’alphabet hébreux. Ainsi, la première lettre est remplacée par la dernière, la seconde par l’avant dernière et ainsi de suite. Suivant un principe similaire de substitution, le code Cesar apparaît entre 60 et 40 av JC et fut largement utilisé par son créateur Jules César. Son principe réside dans un simple décalage fixe. Ainsi pour un décalage de deux, la lettre A du message clair devient C dans le message chiffré.

Le premier chiffre polyalphabétique est mis au point par Leon Battista Alberti en 1466 qui développa également un cadran permettant de réaliser le chiffrement plus rapidement. Il rédige en outre ce qui semble être le premier traité de cryptanalyse\* occidental dans lequel il analyse la fréquence d’utilisation des lettres et en déduit des méthodes pour décrypter les messages. D’autres sources attribuent l’invention du chiffre polyalphabétique à Giovan Battista Bellasodans son traité publié en 1553. Giovani Battista della Porta (1535 - 1615) est pour sa part l’inventeur de la substitution bigrammatique (deux lettres sont représentées par un seul symbole) mais réalise surtout la première classification des principes majeurs cryptographiques : substitution et transposition. L’Italie de la renaissance est bien le creuset de la cryptographie moderne.

Blaise de Vigenère, diplomate français du XVIème siècle développe une méthode de chiffrement polyalphabétique originale qui résiste à l’analyse des fréquences. Vigenère en s’inspirant visiblement des travaux de Bellaso et della Porta, publie le *traité des chiffres* en 1586 dans lequel il présente sa méthode. La véritable originalité de la technique est qu’elle introduit pour la première fois une notion de clé de chiffrement raffinée avec un procédé dit autoclave\*, c’est à dire où la clé de chiffrement utilise le texte clair. Ainsi, le concept de Vigenère consiste à utiliser le chiffre de César mais avec un décalage qui dépend de la lettre utilisée (qui est donnée par la clé). Pour réaliser ces différentes substitutions on réalise une table composée de 26 alphabets dans l’ordre mais décalés d’une lettre à chaque ligne.

Le code de Vigenère n’a été cassé qu’en 1863 par un officier prussien.

***Chroot Jail***

Dans un système Unix, un *chroot* (contraction de *change* et *root*, changement de racine) est une opération qui réduit l’arborescence du système de fichiers à un de ses sous-ensemble, pour un processus donné. Au sein d’un environnement « *chroot*» on ne peut remonter à la racine du système de fichiers initial. Il s’agit donc d’une arborescence de fichiers modifiée qui masque la visibilité du système de fichiers complet à un processus. Le mécanisme *jail* (prison), introduit par le système FreeBSD, contraint quant à lui un processus à s’exécuter au sein d’un environnement (fichier, bibliothèques logicielles, droits d’accès, etc.) minimaliste reproduisant celui du système d’exploitation\* initial.

**Cible**

*(target)*

Le mot cible désigne le système ou l’équipement qui est visé par une attaque informatique. En *marketing* il désigne le public visé par une campagne de publicité ou un message particulier. Dans ce cadre il est synonyme d’audience.

La notion de cible est essentielle dans les opérations numériques car elle se distingue de l’adversaire au sens classique du terme. La cible est une représentation matérielle de cet adversaire, un objet physique sur lequel va porter l’action mais dont on attend des effets ailleurs et typiquement sur l’adversaire.

**Circuit**

*(Circuit)*

En télécommunication, un circuit est un ensemble de deux voies de transmission associées pour assurer une transmission dans les deux sens[[47]](#footnote-48)entre deux points. Il s’agit plus généralement d’un ensemble de ressources qui met en relation un émetteur et un récepteur, ces ressources n’appartiennent qu’au couple émetteur – récepteur.

**Circuit virtuel**

*(Virtual circuit)*

Dans un réseau de données exploité en commutation de paquets\*, un circuit virtuel est un ensemble de moyens fournis par le réseau, qui assurent un transfert de données entre stations équivalant à celui qui serait assuré par commutation de circuits\*[[48]](#footnote-49).

**Circuit virtuel commuté**

*(Switched virtual circuit)*

Circuit virtuel établi et libéré à l’initiative d’un des correspondants[[49]](#footnote-50).

**Clavardage**   
*(Chat)*

Terme utilisé en français du Québec pour désigner une conversation en ligne. Le terme utilisé en France est l’anglicisme : *chater*. Pour pratiquer le « clavardage », le français du Québec nous offre un autre terme dédié : le clavardoir (*chat room*) le français utilise lui le bien moins poétique : *chat*.

**Clé de chiffrement**

*(Encryption key)*

En cryptographie, chiffrer consiste essentiellement en une modification d’une suite d’octet représentant l’informa­tion. Ces modifications sont des opérations mathématiques effectuées suivant un algorithme déterminé. Les algorithmes cryptographiques sont connus, il est donc nécessaire d’utiliser un paramètre d’entrée supplémentaire pour garantir le secret de l’opération. Ce paramètre essentiel est la clé de chiffrement. Il existe deux types de clé, fonction du type de système cryptographique utilisé. Le chiffrement reposant essentiellement sur des problèmes mathématiques (notamment arithmétiques pour les problèmes de factorisation), la longueur de la clé, exprimée en bits, permet d’évaluer la robustesse d’un système. Aucun système cryptographique n’est totalement « incassable », à l’ex­cep­tion de OTP\* – *One Time Pad*, qui n’utilise pas de clé de chiffrement. Les clés symétriques ont une longueur minimale de 128 bits aujourd’hui et les clés asymétriques 1024. La longueur des clés doit augmenter en fonction de l’augmentation des capacités de calcul à disposition des attaquants. Cet aspect soulève deux problématiques liées aux clés de chiffrement en cryptographie :

• La longueur des clés, qui est liée à la capacité à la casser ;

• La périodicité de renouvellement qui est liée à la probabilité de compromission ou au volume de données échangé.

*Clé symétrique :*

Les clés symétriques sont associées au mode de chiffrement symétrique. Dans ce cas lorsqu’Alice veut échanger un message avec Bob, il est nécessaire que les deux personnages disposent de la même clé. Alice chiffre avec sa clé et Bob déchiffre avec la même clé. Le secret est partagé entre Alice et Bob. Ainsi une clé symétrique sert aussi bien lors de l’étape de chiffrement que lors du déchiffrement. Ce mode cryptographique très utilisé pendant des siècles (et encore aujourd’hui) est très robuste et rapide en termes de calcul mais soulève un problème de taille : la distribution des clés. En effet si Alice veut communiquer avec Bob, il est nécessaire de partager la même clé, donc celle-ci doit être générée puis distribuée. Or cette étape est très risquée puisqu’il suffit alors à Max (acteur malveillant) d’inter­cepter une clé pour pouvoir lui aussi déchiffrer l’ensemble du trafic. Enfin cette technique ne garantit que la confidentialité des données, il n’y a pas d’authenti­fi­cation (preuve cryptographique que le message provient bien de l’émetteur prétendu).

*Clés asymétriques :* clé privée – clé publique

Mis en œuvre dans le processus de chiffrement asymétrique, le principe réside dans la génération d’une paire de clés liées mathématiquement (la clé publique se dérive de la clé privée mais l’opération inverse est très complexe). Ainsi, la clé publique peut être copiée et diffusée alors que la clé privée sera conservée. Lors d’un échange, Alice chiffre son message avec la clé publique de Bob (librement disponible) et seul Bob sera en mesure de déchiffrer ce message avec sa clé privée.

Enfin, les modes mixtes (utilisés par exemple par SSL\*) se justifient par le fait que le chiffrement asymétrique est beaucoup plus lent que le chiffrement symétrique. Ils consistent à chiffrer la clé symétrique au moyen d’un algorithme asymétrique en préalable à une transmission.

Voir RSA.

**Clé USB à mémoire flash**  
*(Memory stick)*

Carte mémoire amovible qui se branche sur le port\* USB\* — *Universal Serial Bus*. Alimentée directement par le port, elle ne dispose d’aucun élément mécanique contrairement à un disque dur. Très résistante, la clé USB a des capacités de stockage de plus en plus importantes (plusieurs gigas) et est très répandues.

Ce succès entraine également le fait que la clé USB est un vecteur courant de propagation de codes malveillants. Allant de machines en machines, sans précautions particulières, les clés USB accumulent généralement de nombreux virus qu’elles diffusent vers leurs hôtes au gré de leurs connexions. Certaines entreprises ou administrations ont donc interdit leur usage afin de limiter les infections ou les attaques ciblées.

Voir également USB.

**Client**

*(Client)*

Le client, en informatique, regroupe les applications qui, sur une machine donnée, vont initier une connexion et effectuer des requêtes. Le client est, dans le mode « client-serveur », l’entité qui reçoit les données sollicitées ou accède à un service distant.

**Clonage de serveur DNS**

*(DNS Pharming)*

Voir Détournement de nom de domaine.

***Cloud computing***

(Informatique en nuages ou infonuagique)

Le journal Officiel du 6 juin 2010 donne du *cloud computing* la définition suivante : mode de traitement des données d'un client, dont l'exploitation s'effectue par l'internet, sous la forme de services fournis par un prestataire. L'informatique en nuage est une forme particulière de gérance de l'informatique, dans laquelle l'emplacement et le fonctionnement du nuage ne sont pas portés à la connaissance des clients[[50]](#footnote-51). Le *cloud computing* est une organisation des systèmes d’information permettant l’utilisation à distance de ressources matérielles ou logicielles via l’Internet. Concrètement, les entreprises peuvent faire appel à un service distant, dédié, permettant d’héberger des données ou des applications métiers. L’offre de service s’étoffe, et de plus en plus d’internautes font aujourd’hui appel à ce type de service pour le stockage de contenus multimédia (photo, vidéo, musique). Un *cloud* est dit public quand les ressources sont partagées entre plusieurs entreprises ou clients, privé lorsque les ressources sont mutualisées au sein d’une même entreprise, communautaire ou encore hybride (combinaison avec une technologie commune pour garantir l’interopérabilité).

**CMS - *Content Management System***

(Système de gestion de contenu)

Le CMS ou système de gestion de contenu est une suite logicielle utilisée pour la conception et l’administration de sites Web. Il offre différentes fonctionnalités dont le *workflow,* qui permet la mise en ligne de documents, le travail collaboratif, la structuration de contenu et la gestion des mises à jour. Les CMS sont l’objet de nombreuses attaques et sont souvent à l’origine des intrusions par l’exploitation de leurs vulnérabilités. Les principaux CMS à ce jour sont : SPIP, MAMBO, JOOMLA, TYPO3.

**CNIL - Commission Nationale Informatique et Liberté**

La Commission nationale informatique et liberté est une autorité française indépendante composée de parlementaires de fonctionnaires et de personnes qualifiées. Créée par la loi n° 78-17 du 6 janvier 1978 modifiée dite "informatique et libertés", la CNIL a pour mission essentielle de veiller à la protection des données personnelles, et au respect de la loi.

Sa mission est donc de veiller à ce que l’informatique soit au service du citoyen et qu’elle ne porte atteinte ni à l’identité humaine, ni aux droits de l’homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Elle exerce ses missions conformément à la loi informatique et libertés qui la qualifie d'autorité administrative indépendante[[51]](#footnote-52).

Dans le cadre de sa mission elle recense les fichiers, effectue des contrôles et garantit le droit d’accès des citoyens sur les données les concernant.

**Code**

*(Code)*

Ensemble de règles qui permettent de convertir de l’information afin de la rendre exploitable, copiable, transportable. Ainsi, la principale fonction d’un code est de représenter une information dans le but de pouvoir la transmettre. L’écriture est un code qui répond à cette définition.

En informatique, on parle généralement de code source, il s’agit ici d’une suite d’instructions qui seront exécutées par le microprocesseur de l’ordinateur une fois compilée. Un code source se présente sous la forme d’un texte écrit dans un langage de programmation (exemple C++, Java\*, Python). Ces textes ne sont pas directement exploitables par le processeur et doivent être convertis en suite de 0 et de 1, le code binaire\*.

Voir Compiler, Assembleur.

**Code malveillant**

*(Malware)*

Un code malveillant est un programme s’installant dans un système d’information à l’insu des utilisateurs légitimes, en vue de porter atteinte à l’un des piliers de la sécurité (confidentialité, intégrité, disponibilité).

Voir Logiciel malveillant.

**Commentaire**

*(Comment)*

Message dont la plupart des internautes pourraient se passer… Le commentaire est en général publié en réponse à un article ou un post de blog. Il peut être « modéré », c’est à dire passé au filtre d’un modérateur qui est chargé de supprimer les contenus haineux ou diffamatoires. En règle générale le commentaire est l’aliment préféré des Trolls\*.

**Communauté**

*(Community)*

Regroupement informel d’individus autour d’un sujet d’intérêt commun. Le terme est très répandu dans le monde numérique où l’on rencontre des communautés d’uti­lisateurs de systèmes particuliers, des communautés de développeurs… la nature du lien qui rassemble une communauté est assez spécifique, on peut ainsi appartenir à plusieurs communautés en même temps de façon non exclusive. L’appartenance à une communauté repose sur la volonté individuelle et rarement sur un processus formel de sélection, d’adhésion ou de cotisation.

**Commutation de circuits**

*(Circuit switching)*

La commutation de circuits est une technique de communication réseau dans laquelle un chemin est construit entre l’émetteur et le récepteur en s’appuyant sur les liaisons d’un réseau commuté. Le circuit est créé pour chaque transmission puis libéré pour permettre les autres communications (exemple de la téléphonie fixe RTC\*).

***Pour aller plus loin***

Dans un réseau à commutation de circuit, il est donc nécessaire d’établir la connexion lors de chaque appel. Dans cette phase, l’émetteur envoie une requête (demande de connexion) vers le nœud le plus proche du réseau. Ce dernier analyse la requête et réserve un canal vers le nœud suivant. De proche en proche un circuit est établi par les canaux réservés jusqu’à la station réceptrice.

Le circuit permet alors la transmission des données. L’une ou l’autre des stations peut prendre l’initiative de cesser la communication (libération de la ligne).

**Commutation de paquets**

*(Packet switching)*

Mode d’acheminement de messages dans un réseau de télécommunication, où les messages sont préalablement découpés en paquets munis d’une adresse ; dans les nœuds du réseau, ces paquets sont reçus, mis en mémoire et retransmis sur la ou les voies de transmission appropriées ; à l’arrivée, le message est reconstitué à partir des paquets reçus. Dans ce cas, un paquet n’occupe une voie que pendant sa durée de transmission, la voie étant ensuite disponible pour la transmission d’autres paquets appartenant soit au même, soit à d’autres messages[[52]](#footnote-53).

La commutation de paquets est apparue pour faire face aux contraintes de la transmission de données. En effet, la commutation de circuit, en réservant la totalité de la ressource au profit d’une seule voie de transmission, ne permet pas de supporter la charge liée à l’interconnexion de plusieurs équipements informatiques. La commutation de paquets est par ailleurs plus résiliente dans la mesure où elle ne dépend pas de la fiabilité d’un seul circuit et que des mécanismes de contrôle peuvent être implémentés. Pour les réseaux locaux, la commutation a permis d’étendre la taille des réseaux et d’augmenter les débits.

Voir TCP.

**Communications électroniques**

*(Electronic communications)*

En France, la loi du 9 juillet 2004 présente les communications électroniques comme : les émissions, transmissions, ou réceptions de signes, de signaux, d’écrits, d’images ou de son par voies électromagnétiques.

**Compiler**

(*Compile)*

Action qui consiste à traduire un programme écrit dans un langage évolué (code\* source) en un programme en langage machine en vue de son exécution[[53]](#footnote-54). La compilation est effectuée à l’aide d’un programme spécifique, le compilateur.

Voir Assembleur, Code.

**Compromission**

*(Compromission)*

Une compromission est une atteinte à l’intégrité ou à la confidentialité d’un objet désigné (information, ordinateur, individu). L’IGI 1300 en donne, pour le domaine du secret de la défense nationale, la définition suivante, prise de connaissance, certaine ou probable, d’une information ou support protégé par une ou plusieurs personnes non autorisées[[54]](#footnote-55).

***Computer Network Operations* - CNO**

(Opérations Informatiques)

Terminologie utilisée par la doctrine américaine de combat dans le cyberespace\*, les CNO regroupent le *Computer Network* *Attack*\* (CNA) ainsi que le *Computer Network Exploitation*\* (CNE) mais également le *Computer Network Defense* (CND).

Le terme de *Computer Network* *Operations* (CNO) a été remplacé, depuis 2009 par celui plus large de *Cyberspace* *Opérations* (CO). Il s’agit, selon la définition de la *Joint terminology for cyberspace operations* [CM-0856-09 1 Sep 09]de l’emploi de capacités cyber dans le but premier d’atteindre des objectifs dans ou par le cyberespace. De telles opérations comprennent les opérations en réseau CNO et les activités qui visent à défendre ou agir dans le spectre global de l’information.

***Computer Network Attack* - CNA**

(Lutte informatique offensive – lutte informatique active)

Terminologie utilisée par la doctrine américaine de combat dans le cyberespace\*, le CNA désigne suivant la *Joint terminology for cyberspace operations* [CM-0856-09 1 Sep 09] une catégorie de feux utilisés à des fins offensives et conduit en utilisant des ordinateurs en réseau dans le but de perturber, interdire, dégrader, manipuler ou détruire des informations dans le système d’information cible ou dans un réseau, ou le réseau et le système lui-même. L’effet final n’est pas nécessairement porté sur le système visé, mais peut appuyer un effort plus large tel que des opérations d’information ou de contre-terrorisme, i.e altérer ou mystifier des communications particulières ou créer un accès ou interdire l’accès aux communications adverses ou à leurs flux logistiques.

Note : cette définition modifie la précédente définition de CNA en 1) l’identifiant clairement à une forme de « feu » offensif, 2) établissant la différence entre CNA et les *counter-cyber ops* qui ciblent préférentiellement l’usage du cyberespace par l’adversaire, et 3) identifiant le CNA comme un élément essentiel des opérations d’information et des efforts qui lui sont reliés.

***Computer Network Defense* - CND**

(Lutte Informatique Défensive - LID)

Terminologie utilisée par la doctrine américaine de combat dans le cyberespace\*, le CND désigne suivant la *Joint terminology for cyberspace operations* [CM-0856-09 1 Sep 09] l’ensemble des actions qui utilisent les réseaux informatiques dans l’objectif de détecter, analyser et répondre aux intrusions, attaques et autres tentatives d’accès non autorisés.

***Computer Network Exploitation* - CNE**

(Action d’exploitation informatique)

Concept développé dans la doctrine américaine de combat dans le cyberespace\*, le *Computer Network Exploitation* (CNE) vise à développer les capacités de collecte d’information par l’exploitation de réseaux d’ordinateurs afin de recueillir des données sur des cibles ou sur les systèmes d’information adverses. La terminologie française parle pour sa part d’actions d’exploitation informatique\*.

Voir Action d’exploitation informatique.

**Concentrateur**

*(Hub)*

Un concentrateur est un équipement réseau qui concentre et distribue les communications de données\*. Un concentrateur n’assure pas de routage\* ni de commutation et répète la trame\* reçue sur l’ensemble de ses ports\*. Il Différent ainsi du *Switch\**.

**Confiance, tiers de confiance**

*(Trust – trusted third party TTP)*

La confiance est au cœur des problématiques de sécurité informatique. Le réseau n’est en définitive que le support des échanges entre machines et donc indirectement entre personnes physiques. L’échange implique la confiance. Dans toute transaction électronique (de la simple connexion à un site à l’achat en ligne en passant par les mécanismes de contrôle industriel) l’usager doit pouvoir se fier aux données qu’il reçoit. Lorsqu’un système est attaqué, la première victime est la confiance que les utilisateurs accordent à leur système d’information. Comment alors garantir la confiance dans l’ère numérique ? Comment et qui peut incarner ce rôle sans toutefois devenir omnipotent ?

La cryptographie\* nous permet de penser des mécanismes de confiance par l’intermédiaire des signatures électroniques\* par exemple. Dans ce cadre, un tiers de confiance*\** est une autorité habilitée qui met en œuvre ces signatures. Ce tiers peut être une autorité de certification\* (en charge de la politique de gestion des certificats, dite politique de certification), une autorité d’enregistrement\* (qui s’assure de l’identité du demandeur d’une signature électronique) ou encore un opérateur de certification (qui met en œuvre la gestion des certificats). En France, la FNTC[[55]](#footnote-56) (fédération nationale des tiers de confiance) regroupe les tiers de confiance et des acteurs du monde de l’économie numérique. La FNTC est donc une fédération de professionnels qui vise à structurer et normaliser les échanges et les moyens techniques associés.

Voir Autorité de certification, Certificat, Signature électronique.

**Confidentialité**

*(Confidentiality)*

La confidentialité est une notion essentielle en sécurité informatique, elle en est même le premier objectif. Aujourd’hui, la sécurité informatique poursuit trois objectifs principaux:

• la confidentialité des informations ;

• l’intégrité\* ;

• la disponibilité (ou accessibilité).

On rajoute souvent à ces objectifs, la non-répudiation (qui permet de garantir que l’on ne puisse nier une action ou une transaction) ainsi que l’authentification\*. Dans ce cadre, la confidentialité vise à s’assurer que seules les personnes autorisées peuvent accéder à l’information, pour les autres elle sera inintelligible ou inaccessible. Dans un système d’information, la confidentialité est atteinte par l’utilisation de la cryptographie\* et la mise en place d’une politique de sécurité qui détermine des droits d’accès et leur gestion.

La confidentialité est attachée à une donnée, elle la caractérise par rapport à l’ensemble des utilisateurs. Dans le langage commun on parle ainsi « d’informations confidentielles » pour souligner leur caractère « secret », c’est à dire non disponible au public.

L’instruction générale interministérielle 1300 en donne ainsi la définition suivante : caractère réservé d'une information ou d’un traitement dont l’accès est limité aux seules personnes admises à la (le) connaître pour les besoins du service, ou aux entités ou processus autorisés[[56]](#footnote-57).

**Conflit**

(*Conflict)*

Le conflit, qu’il se matérialise dans le monde physique ou numérique se caractérise par une violente opposition entre au moins deux parties. L’opposition peut naître d’intérêts ou d’opinions divergents et dégénérer en conflit. La forme la plus violente du conflit est l’agression armée.

Dans le domaine réseau, un conflit peut apparaître lorsque deux équipements ont la même adresse IP\* au sein d’un même réseau (on parle également de collision). On parle alors de conflit d’adressage, le réseau ne peut plus fonctionner normalement car la distribution des paquets ne peut se faire. Les conflits d’adressage résultent généralement de problèmes de configuration réseau (DHCP\*, passerelle par défaut). Voir Adresse IP, Routage.

**Connecteur**

*(Socket)*

Un connecteur est un mécanisme logiciel de communication entre processus informatiques, souvent utilisé entre une application et un réseau[[57]](#footnote-58).

**Connexion**

*(log in, log on)*

Une connexion est une procédure qui permet à un utilisateur d’accéder à une ressource informatique. Ce mécanisme peut regrouper les phases d’identification (l’utilisateur déclare qui il est) et d’authentification (l’utilisateur prouve qu’il est bien celui qu’il prétend être). Voir également Authentification.

**Constat d’audit**

Résultats de l’évaluation des preuves d’audit\* recueillies par rapport aux critères d’audit[[58]](#footnote-59). Voir Audit, Preuve d’au­dit.

**Contenu**

*(Content – User Generated Content)*

Le contenu désigne l’information véhiculée par un flux réseau. Ainsi, on distingue généralement le contenu du conte­nant (enveloppe, information supplémentaire rajoutée pour permettre l’acheminement de l’information).

En revanche, le contenu engendré par les usagers (*User Generated Content*) désigne un media participatif (en général sur Internet) où le produit final est directement le résultat de contributions d’usagers qui sont également les utilisateurs finaux du média (les *wiki*\* par exemple).

**Contournement de la politique de sécurité**

Toute action ayant pour conséquence la mise en échec des règles ou des mécanismes de sécurité mis en place[[59]](#footnote-60).

**Contrôle d’accès**

*(Access Control)*

Voir NAC – *Network Access Control.*

**Contrôle parental**   
*(Parental Controls)*

Le contrôle parental désigne un ensemble d’outils mis à la disposition des parents pour paramétrer leurs équipements afin d'éviter que les enfants n'accèdent à certains contenus Internet jugé inappropriés. Les outils de contrôle parental sont ainsi proposés par les fournisseurs d’accès, les navigateurs internet, éditeurs de logiciels, etc.

**Convention d’audit**

Accord écrit entre un commanditaire et un prestataire d’audit pour la réalisation d’un audit[[60]](#footnote-61). Cette convention décrit au minimum le périmètre de l’audit (délimite les systèmes et implantations physiques concernés par l’audit), ainsi que les règles desécurité liées à l’audit (protection des systèmes pendant l’audit, protection du rapport d’audit, etc.).

Voir Audit.

**Convergence**

*(Convergence)*

Caractéristique des évolutions technologiques qui se traduit par une fusion entre l’informatique, les télécommunications et l’audiovisuel. La convergence désigne ainsi le phénomène de rapprochement, rendu possible par la numérisation, entre les industries des télécommunications, de l’informatique et du « multimédia ».

***Cookie***

(Témoin de connexion)

Un *cookie* est un fichier texte envoyé par un serveur et stocké sur un client\* (votre machine) afin de conserver des informations liées au contexte de navigation. Cet outil permet, entre autre, de faciliter la navigation sur des sites déjà visités, le cookie peut en effet conserver vos paniers d’achats en cours (pour le commerce électronique), dans certaines conditions des éléments d’identification (identifiants – mots de passe)…

La gestion des *cookies* est un élément important en sécurité informatique car ils contiennent des éléments d’identification (donc des données personnelles) mais également car ils peuvent être utilisés afin de conduire la première phase d’une attaque informatique (ils fournissent en effet des informations sur les usages internet d’une cible et permettent d’établir un premier profil de cible). Si la plupart des navigateurs aujourd’hui permettent d’accep­ter ou de refuser les *cookies* les refuser systématiquement peut dégrader l’accès à certains sites ou certaines applications. Il convient donc de faire preuve de mesure. Il est également recommandé de supprimer régulièrement les cookies, ceux-ci étant parfois conservés indéfiniment.

**Corruption**

*(Corruption)*

Loin de la définition juridique, la corruption est ici une caractéristique d’un système ou d’une donnée soulignant son altération. Ainsi, en sécurité informatique une donnée corrompue est une donnée dont l’intégrité, la confidentialité ou encore la disponibilité a été modifiée, dégradée par rapport à son état souhaité ou initial. Ainsi, une donnée altérée chiffrée ou compressée ne pourra généralement pas être déchiffrée/décompressée.

**Couche physique**

*(Physical layer)*

La couche physique est la couche inférieure du modèle OSI\*. Dans ce modèle, cette couche assure la fonction de transmission physique du signal (signal électrique ou optique), elle génère et reçoit les bits\* qu’elle transmet sous la forme d’impulsions (lumineuse, électrique, électromagnétique). Cette couche regroupe également les mécanismes d’établissement de la connexion.

La description du cyberespace\* s’appuie également sur la notion de couche physique. Dans ce cadre, la couche physique soutient la couche logique ou logicielle sur laquelle se greffe la couche sémantique ou sociale (voir description du cyberespace\* en couche).

***Pour aller plus loin***

Appelée également couche matérielle, la couche physique fait référence au modèle OSI\* utilisé dans la théorie des réseaux[[61]](#footnote-62). Elle comprend les appareils terminaux (ordinateurs, téléphone, tablettes, systèmes électroniques), et toutes les infrastructures nécessaires à l’interconnexion (câbles, relais, routeurs, architecture de cœur de réseau). Il faut également inclure sur cette couche les lieux de stockage de l’information, les systèmes de contrôle et de supervision, les objets connectés, etc.

Sur cette couche sont donc regroupées les structures techniques qui seront ciblées par les opérations numériques. Ces dernières sont de fait totalement liées à un territoire géographique, et dépendent pour leur fonctionnement de ressources externes en énergie et eau (pour les systèmes de climatisation principalement). Cet enracinement géographique de la couche physique du cyberespace a une conséquence majeure pour les opérations : il est possible d’obtenir un effet sans pour autant utiliser de moyens « numériques ». L’affrontement dans le cyberespace ou pour la domination du cyberespace peut également avoir un volet tout à fait conventionnel.

La couche physique est également porteuse d’enjeux industriels et écologiques de long terme. Support des infrastructures de télécommunications, la couche physique peut voir s’affronter des puissances dans le cadre de la diffusion commerciales des équipements clés du réseau.

**Coupe-feu**  
*(Firewall)* Voir Firewall.

**Courrier électronique (courriel)**  
(E-mail *Electronic Mail*)

Le courriel est un service qui assure les échanges de messages électroniques entre individus par l’intermédiaire d’un réseau informatique. Le courriel se compose de texte, d’image, de vidéos ou de fichiers informatiques. Pour pouvoir communiquer il est nécessaire de s’appuyer sur un client\* de messagerie (généralement assuré par le fournisseur d’accès internet) ou sur un *webmail* (qui permet d’accéder à sa boite de messagerie par l’intermédiaire d’un navigateur internet). L’adresse de messagerie (ou adresse email) est un élément essentiel du service qui s’appuie également sur des protocoles de routage dédiés.

Ainsi, le protocole SMTP\* (*Simple Mail Transfer Protocol*) est un protocole qui permet de transférer le courrier entre deux serveurs en connexion point à point. S’appuyant sur le protocole TCP\* pour le transport des données, SMTP fonctionne en mode connecté (port\* 25 par défaut ou SMTP authentifié sur port 587). SMTP est décrit une première fois par la RFC 821 en 1982 puis RFC 2821 en 2001.

L’autre famille de protocoles de messagerie est regroupée sous l’acronyme POP\* (*post office protocol*). La version courante est la troisième on parle donc de POP3. Ce protocole est utilisé pour aller récupérer du courrier sur le serveur de messagerie et le rapatrier vers un client (votre machine). Une fois rapatriés sur une machine, les messages peuvent être lus même hors connexion. POP utilise le port 110 par défaut et est défini par la RFC 1939.

Enfin, le protocole IMAP (Internet *Message Acces Protocol*), décri par la RFC 3501, est également un protocole de récupération de courrier à l’image de POP mais qui dispose de fonctionnalités plus étendues (gestion de plusieurs boîtes, tri du courrier). Il utilise le port TCP 143.

Voir SMTP, POP3.

**CPE - *Common Platform Enumeration***

CPE est une initiative du MITRE\* dont les premières spécifications datent de 2007. La CPE a pour objectif la mise au point d’un système de nommage afin de désigner les différents composants d’un système informatique (un serveur, un système d’exploitation, etc.)[[62]](#footnote-63).

**CPL - Courant Porteur en Ligne**

*(Power Line Communication)*

Le principe du CPL consiste à utiliser les lignes de courant domestiques pour faire transiter des informations. Le CPL superpose un signal de haute fréquence sur le courant électrique déjà présent (50 Hz). Il permet de créer des réseaux locaux (à l’intérieur d’un logement par exemple) pour faire communiquer des équipements électroniques.

***Creative Commons (CC)***

Organisation à but non lucratif, *Creative Commons* propose des licences permettant de libérer les créations du droit de propriété intellectuelle. Selon la présentation du site français de l’association, *« Creative Commons* est une organisation à but non lucratif qui a pour dessein de faciliter la diffusion et le partage des œuvres tout en accompagnant les nouvelles pratiques de création à l’ère numérique. *»*

Il existe plusieurs licences *Creative Commons*, « elles viennent en complément du droit applicable, elles ne se substituent pas au droit d’auteur. Simples à utiliser et intégrées dans les standards du Web, ces autorisations non exclusives permettent aux titulaires de droits d’autoriser le public à effectuer certaines utilisations, tout en ayant la possibilité de réserver les exploitations commerciales, les œuvres dérivées et les conditions de redistribution. »[[63]](#footnote-64)

**Créneau temporel**

*(Time slot)*

Désigne un intervalle de temps à occurrence cyclique qu’il est possible de reconnaître et de définir sans ambiguïté[[64]](#footnote-65). L’expression est notamment utilisée dans la technologie GSM\* dans le cadre du multiplexage\* temporel. Dans ce contexte, chaque cellule du réseau dispose d’un certain nombre de fréquences (ou de canaux) à répartir entre utilisateurs, qui sont elles même divisées en *slot*.

**Critère d’audit**

Ensemble des référentiels, guides, procédures ou exigences applicables à la sécurité du système d’information audité[[65]](#footnote-66).

Voir également Audit\*, Constat d’audit\*, Prestataire d’audit\*.

**Critères communs (CC)**

*(Common criteria)*

Référentiel normé par l’ISO 15408 pour l’évaluation des propriétés de sécurité des produits et systèmes des technologies de l’information.

Les CC définissent notamment différents niveaux de profondeur dans l’évaluation permettant ainsi d’atteindre des niveaux d’assurance plus ou moins élevés dans la sécurité du produit : les EAL (*Evaluation Assurance Level*). Plus le niveau visé est élevé, plus les contraintes en termes d’éléments de preuve que doit fournir le développeur au laboratoire sont importantes et plus les coûts d’évaluation sont conséquents. Une évaluation CC dure en moyenne entre 6 et 18 mois (selon le type de produit, le niveau visé et la maturité du développeur) et nécessite des moyens financiers importants[[66]](#footnote-67).

***Cross Site Scripting - XSS***

(Injection de code indirecte)

Type d’attaque qui consiste à injecter du code malveillant sur un site Web dynamique. On peut ainsi faire exécuter du code par un navigateur qui visite la page Web. Ce type d’attaque permet de dérober des identifiants de connexion (session\*), et des redirections vers des sites compromis etc.

***Crowdfunding***

(Financement participatif)

Mode de financement de projets qui utilise les possibilités de mise en relation liées au Web participatif et aux réseaux sociaux. Ainsi, un projet personnel, qu’il soit artistique, humanitaire, caritatif ou entrepreneurial peut, par l’intermédiaire de plateforme de *crowdfunding* recevoir des financements privés d’une multitude d’internautes. Plusieurs modèles de *crowdfunding* existent, certain avec contrepartie, d’autre limités dans le temps etc. Ce mode de financement est particulièrement développé dans le domaine de la création de *start-up* et est un marqueur de la culture numérique.

Ce mode de financement est relativement jeune (moins d’une dizaine d’années) et est en forte croissance depuis deux ans en France. Ainsi, ***152 millions d'Euros*** *ont été levés par les 46 plateformes de crowdfunding qui ont communiqué leur collecte pour 2014. C'est deux fois plus qu'en 2013, où les fonds versés par les internautes avaient atteint 78,3 millions d'euros, un montant qui avait quasiment triplé par rapport à 2012. Le don, avec 38,2 millions d'euros collectés, l'investissement en capital (25,4 millions) et le prêt, rémunéré ou non, (88,4 millions) affichent des croissances respectives de 97, 146 et 84% sur une année[[67]](#footnote-68)*.

***Crowdsourcing***

(Production participative)

Le *crowdsourcing* désigne le phénomène qui consiste à faire appel à l’ensemble des internautes pour réaliser une tâche ou générer des contenus\* (voir Contenus et *User Generated Content*). Le principe s’appuie sur les outils développés depuis l’émergence du Web 2.0 (participatif). Il existe plusieurs sortes de *crowdsourcing* et plusieurs stratégies pour réaliser une tâche. Ainsi, on peut faire appel à une ressource spécialisée pour contribuer à un projet, ou au contraire laisser ouvert la participation. Par ailleurs, le projet peut être scindé en micro-tâches à répartir entre participants ou peut-être réalisé en parallèle par plusieurs contributeurs.

Le *crowdsourcing* a des applications nombreuses et contribue à la réappropriation de l’espace public par les citoyens. En France, l’association Regards citoyens a ainsi fait appel à plus de 8000 contributeurs pour saisir sous un format intelligible et exploitable les déclarations de patrimoines des parlementaires[[68]](#footnote-69) (manuscrites et parfois illisibles).

**Cryptanalyse**

*(Cryptanalysis)*

Processus de déchiffrement de données protégées au moyen de cryptographie sans être en possession des clés de chiffrement[[69]](#footnote-70)*.*

**Cryptographie**

*(Cryptography)*

Discipline incluant les principes, moyens et méthodes de transformation des données, dans le but de cacher leur contenu, d’empêcher que leur modification ne passe inaperçue et/ou d’empêcher leur utilisation non autorisée (ISO 7498-2)[[70]](#footnote-71). La conversion de l'information brute (ou claire) en cette nouvelle forme protégée s’appelle alors le chiffrement\*, le retour dans une forme intelligible et originale est le déchiffrement\*.

**Cryptologie**

*(Cryptology)*

Science englobant la cryptographie et la cryptanalyse.

**CSIRT - *Computer Security Incident Response Team***

Voir CERT.

**CSS – *Cascading Style Sheets***

(Feuilles de styles en cascade)

En conception de page Web, le CSS est un langage qui permet de décrire la présentation et la mise en page de documents HTML\* (et XML\*). Interprétées par les navigateurs, les pages CSS associées aux pages HTML permettent de définir totalement l’apparence d’une page. Si l’on peut insérer du CSS dans un code HTML, il est recommandé de rédiger les deux de façon séparée. Les CSS sont aujourd’hui un standard du W3C\*.

**CTR - *Common Technical Regulation***

Ensemble de règles techniques qui fixent les modalités d’accès au réseau des terminaux mobiles. Les CTR sont applicables à l’ensemble des pays membres de l’Union Européenne.

**Curation**

*(Curation – data curation – content curation)*

Le terme curation est un anglicisme pour décrire les activités et les logiciels qui visent à mieux appréhender les phénomènes d’infobésité\*. La curation consiste donc à présenter sous forme pertinente des contenus issus de différentes sources (sites Internet, blogs, réseaux sociaux). Cette forme de sélection thématique vise à agréger l’ensemble des informations utiles sur une même plateforme et éviter la perte de temps liée à la consultation aléatoire de sources. Voir Donnée.

**CVE - *Common Vulnerability Enumeration***

Les CVE sont un standard de nommage des vulnérabilités lancées en 1999 dont le principe est d’associer une référence unique à chaque vulnérabilité découverte. Ainsi, la CVE-2015-1637 fait l’objet du bulletin de sécurité de Microsoft MS 15-031 (en date du 10 mars 2015) et décrit une vulnérabilité dans *Schannel* qui pourrait permettre un contournement de la fonctionnalité de sécurité. Le site *CVE Details*[[71]](#footnote-72) présente chaque CVE en détail ainsi que son score CVSS\* associé.

Voir CVSS.

**CVSS – *Common Vulnerability Scoring System***

CVSS est un système de notation utilisé pour évaluer le niveau de dangerosité d’une vulnérabilité. Chaque référence CVE\* fait l’objet d’une note CVSS qui repose sur trois métriques principales :

• la métrique de base : porte sur la vulnérabilité elle-même, comment la vulnérabilité est exploitée (local, à distance), mais également la difficulté à exploiter cette vulnérabilité ;

• la métrique temporelle : qui caractérise l’existence d’un code d’exploitation ;

• la métrique environnementale : qui porte notamment sur les éventuels dommages collatéraux de l’exploitation de la vulnérabilité.

Un calculateur en ligne est disponible sur le site du NIST[[72]](#footnote-73).

**CWE - *Common Weakness Enumeration***

Projet du MITRE\* qui consiste à lister l’ensemble des types de vulnérabilités que l’on peut retrouver dans différents logiciels. Ainsi la CWE – 16 porte, par exemple, sur les vulnérabilités liées à la configuration (indépendamment du logiciel). La fiche liste les méthodes de détection et les CVE associées.

Voir <https://cwe.mitre.org/> qui présente le projet et <https://nvd.nist.gov/cwe.cfm> qui liste les CWE.

**Cyber**

*(Cyber)*

Préfixe issu de la contraction du terme cybernétique. Ce dernier apparaît en 1948 dans une publication de Norber Wiener[[73]](#footnote-74) et est défini comme *une science qui s’intéresse à l’étude des processus de commande et de communication chez les êtres vivants, dans les machines et les systèmes sociologiques et économiques*. Wiener découvrira plus tard que le terme avait déjà été utilisé par Ampère au début du XIXème siècle dans un cadre diffèrent. Le mot dérive du grec κῠβερνήτης (*kubernêtês*) « pilote, gouverneur ». Le préfixe est très largement utilisé à partir des années 2000 pour évoquer toute question se rapportant de près ou de loin à l’usage d’Internet, des télécommunications et au traitement automatique de l’information. Sans périmètre clair de définition, tout devient « cyber » et permet de rendre populaire des disciplines techniques parfois ardues (la sécurité des systèmes d’information, l’architecture de réseau, les processus de traitement industriels). Ainsi, parle-t-on de cybercriminalité\* pour évoquer l’usage des nouvelles technologies de l’information pour commettre des délits, de cyberattaques\* et de cyberdéfense\*. Enfin, les réseaux sociaux ont permis l’émergence du cyberharcélement\*. La multiplication de l’usage du préfixe cyber s’accompagne parfois d’un phénomène de rejet de la part des experts techniques qui n’y voient que l’expression de l’ignorance et un moyen de paraître « à la mode ».

**Cyberattaque**

*(Cyber Attack)*

La notion de cyberattaque n’est pas juridiquement définie, au contraire de *« l’accès ou du maintien de manière frauduleuse dans un système automatisé de traitement de données*»[[74]](#footnote-75). Dans la terminologie militaire française on la présente comme une action volontaire, offensive et malveillante, menée au travers du cyberespace et destinée à provoquer un dommage (en disponibilité, intégrité ou confidentialité) aux informations ou aux systèmes qui les traitent, pouvant ainsi nuire aux activités dont ils sont le support. Elaborée dans le but d’atteindre un objectif, une cyberattaque peut être ponctuelle ou s’inscrire dans la durée. Elle peut alors être évolutive et capable de s’adapter aux mesures défensives qu’elle rencontre[[75]](#footnote-76). Dans ce cas, une cyberattaque pourrait donc être une forme d'attaque informatique, qui vise à endommager, détruire, modifier ou subtiliser tout ou partie d’un système de traitement automatique de données. La cyberattaque est conduite via des moyens numériques qui peuvent être qualifiés d’armes informatiques. Dans ce cadre, une arme informatique est un code malveillant, spécifiquement développé afin de produire un effet visant à neutraliser ou perturber le fonctionnement normal d’une cible. Le mode de transmission ou d’infection importe peu (clé USB, Wifi, site Internet…), c’est l’intention spécifique du développeur qui confère le statut d’arme au code malveillant [BOYER, 2014]. L’arme informatique n’est donc que l’outil de la cyberattaque, elle même n’étant qu’une forme particulière de combat numérique.

***Cybercommand***

*(Cybercommand)*

L’*United* *States Cyber* *Command* (USCYBERCOM) est un sous commandement interarmées des forces américaines, placé sous l’autorité de l’US *Strategic Command*. Actif depuis le 21 mai 2010 et placé initialement sous le commandement du général Keith B. Alexander (alors également directeur de la NSA) puis de l’amiral Rogers en 2014, il a pour mission de :

Planifier, coordonner, intégrer, synchroniser et conduire des activités pour : diriger les opérations et la défense de certains réseaux d’information du Département de la Défense, et préparer et, au besoin, conduire, tout le spectre d’opérations militaires du cyberespace dans le but de permettre des actions dans tous les domaines, assurer la liberté d’action des États-Unis et de leurs alliés dans le cyberespace, et la dénier à leurs adversaires.

Il compte au début de l’année 2013 environ 900 personnes et devrait voir ses effectifs croître très nettement dans les années à venir.

**Cybercriminalité**

*(Cybercriminality)*

Actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d’information comme moyen de réalisation d’un délit ou d’un crime, ou les ayant pour cible[[76]](#footnote-77).

**Cyberdéfense**

*(Cyberdefence)*

Ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace\* les systèmes d’information jugés essentiels[[77]](#footnote-78).

Pour le ministère français de la Défense, ensemble des activités qu’il conduit afin d’intervenir militairement ou non dans le cyberespace pour garantir l’efficacité de l’action des forces armées, la réalisation des missions confiées et le bon fonctionnement du ministère[[78]](#footnote-79).

**Cyberdéfense militaire**

*(Millitary Cyberdefence)*

Au sein du ministère de la défense français, le concept de cyberdéfense militaire est présenté comme, l’ensemble des actions défensives ou offensives conduites dans le cyberespace en préparation ou dans la planification et la conduite des opérations militaires, notamment pour garantir l’efficacité de l’action des forces armées et le bon fonctionnement du ministère.

*Note :* La cyberdéfense militaire complète les mesures de protection des réseaux, des systèmes et de l’information (cyberprotection\*, ou SSI) par une capacité d’opérations dans le cyberespace et une capacité de gestion de crise cybernétique, couplées aux capacités de résilience des systèmes d’information[[79]](#footnote-80).

**Cyberdissuasion**

*(Cyberdetterence)*

Le débat stratégique s’est très tôt intéressé au parallèle entre la dissuasion nucléaire et le concept de cyberguerre. En évoquant le spectre d’un Hiroshima numérique, ou encore en développant de scénarios catastrophe dans lesquels des pays entiers étaient plongés dans le chaos par des vagues de cyberattaques\*, la pensée stratégique a d’abord cru à l’apparition d’une nouvelle forme de guerre s’appuyant sur des armes (numériques) dont la puissance des effets serait comparables à une explosion nucléaire. Quel peut-être alors le sens d’une cyberdissuasion ? Peut-on dissuader dans le cyberespace ? S’il est clair qu’une forme de dissuasion émerge, notamment dans le discours sur les capacités offensives et défensives, on peut douter de son efficacité face à certains adversaires moins sensibles à des formes de rétorsion numériques. Par ailleurs, le problème de l’attribution\* demeure central dans un mécanisme de dissuasion. Cette dernière doit être appliquée sur une structure identifiée (Etat, groupe, voire individus). Le modèle de la cyberdissuasion comme simple transposition de la théorie classique de la dissuasion nucléaire semble donc défaillant. On ne peut en revanche nier la contribution du domaine cyber à la dissuasion générale. Disposer de capacités (offensives et défensives) dans ce domaine participe à renforcer la posture globale de défense d’un Etat.

**Cyberespace**

*(Cyberspace)*

Il existe plusieurs définitions du terme cyberespace, chacune insistant sur un volet particulier ou une notion spécifique en fonction de l’organisme rédacteur. En France, l’ANSSI\* en donne la définition suivante : Espace de communication constitué par l’interconnexion mondiale d’équipements de traitement automatisé de données numériques[[80]](#footnote-81).

Les Armées retiennent pour leur part : Le cyberespace est un domaine global constitué du réseau maillé des infrastructures des technologies de l’information (dont internet), des réseaux de télécommunications, des systèmes informatiques, des processeurs et des mécanismes de contrôle intégrés. Il inclut l’information numérique transportée ainsi que les opérateurs des services en ligne[[81]](#footnote-82).

Enfin, Olivier Kempf dans son *Introduction à la cyberstratégie :* Le cyberespace est l’espace constitué des systèmes d’infor­matiques de toute sorte connectés en réseaux et permettant la communication technique et sociale d’informations par des utilisateurs individuels ou collectifs.

**Les trois niveaux du cyberespace**

Même s’il n’est pas complètement borné juridiquement, le cyberespace est toutefois structuré autour de trois niveaux qui sont tous soumis à des droits spécifiques :

La **couche physique\***, qui comprend les systèmes porteurs d’Internet et les infrastructures réseaux. Sur cette couche apparaissent les serveurs racines, les *data center,* les réseaux de téléphonie mobile, les câbles sous-marins et les fibres optiques terrestres. Cette couche physique dépend pour une large part des législations nationales. Les compagnies opérant les infrastructures de la couche physique sont liées aux pratiques et réglementations des États qui les accueillent. Cette couche peut être attaquée soit via le réseau soit par des vecteurs plus classiques. Ces installations sont en général jugées d’importances vitales et font l’objet de mesures de sécurité particulières de la part des États. Les besoins en énergie et les accès physiques sont les principales vulnérabilités de cette couche ;

la **couche logique**, englobe pour sa part l’ensemble des programmes permettant d’accéder au réseau, d’effectuer des requêtes, d’obtenir des services et d’assurer le transport des données (routage). Les logiciels sont, par ailleurs, les éléments fondamentaux de cette couche et permettent d’utiliser la puissance de calcul d’un système électronique en vue de lui faire effectuer les actions prescrites. Le mot logiciel est apparu en France au début des années 70 pour servir de traduction au terme anglais « software ». Typiquement on les classe suivant deux catégories distinctes, les logiciels systèmes et les logiciels applications. Concernant cette couche particulière, la législation est balbutiante mais les instances de régulation œuvrent pour harmoniser cet espace. C’est bien évidement sur cette couche que l’on compte les vulnérabilités les plus classiques et où les hackers et les spécialistes de développement de solutions sécurisées se livrent une bataille quotidienne. Loin de l’image romanesque, les enjeux de la sécurisation de la couche logique sont énormes et les préjudices financiers qui peuvent en découler difficilement chiffrables ;

la **couche cognitive**, qui s’attache au contenu, à l’infor­ma­tion qui est véhiculée sur les pages Internet ou à l’aide des diverses formes d’interaction possible sur le Web 2.0. Cette couche est la couche « haute » du cyberespace celle où se mêlent les perceptions de la réalité et les capacités de gestion de la connaissance. Le développement de cette couche s’est d’abord effectué au travers des systèmes de messagerie (mail, *Webmail*) et des contenus de pages adressées puis a connu une mutation profonde avec l'émergence de réseaux sociaux (myspace, facebook\*...) et du microblogging (twitter). Les vulnérabilités de cette couche sont légion. En premier lieu, le nombre de pages interdit un contrôle systématique de la part des hébergeurs et laisse donc ouverte la possibilité de diffuser à peu près tout et n’importe quoi. Par ailleurs, les capacités de duplication de l’information permettent une « tra­ça­bilité » accrue des usagers des réseaux. Les infractions liées à l’usurpation d’identité ou les atteintes à la réputation en ligne (e-réputation) ont atteint un niveau préoccupant. Les législations nationales s’adaptent difficilement à cette couche par nature « supra-nationale » et où la distinction entre vie privée et vie publique n’est pas toujours clairement fixée. Dans ce domaine, les bonnes intentions ne franchissent que rarement les frontières...

**Cyberguerre**

*(Cyberwar)*

Il n’existe pas à proprement parler de définition de la « cyberguerre ». Cette notion est souvent confondue avec les cyberattaques. Ainsi, les intrusions informatiques et les vols de données sont régulièrement qualifiés de « cyberguerre ». Dans *Cyberstratégie, l’art de la guerre numérique*, nous proposions la définition suivante :

La cyberguerre (guerre numérique) regroupe l’ensemble des actions militaires visant à la maîtrise du cyberespace afin, soit d’y conduire des opérations spécifiques soit de préparer l’exploitation vers un autre espace de conflit (terre, air, mer). Dans ce cas, la guerre numérique agit comme un démultiplicateur de forces au profit des armées. Elle est conduite par des services de l’État et prend des formes diverses qui embrassent les trois couches du cyberespace : physique, logique et cognitive.

Selon cette approche, la cyberguerre est donc un domaine réservé de l’action étatique, elle est conduite par des forces armées (donc dans un cadre légal strict). Ces opérations visent le contrôle du milieu et sont intégrées à l’action globale sur les trois couches du cyberespace. Ainsi, les actions conduites par des groupes d’activistes plus ou moins doués techniquement, ne rentrent pas dans ce cadre *stricto sensu*.

**Cyberharcèlement**   
*(Cyberstalking)*

Forme de harcèlement en ligne (généralement via des réseaux sociaux) qui comprend l’usage du dénigrement répété et des menaces.

Des premiers cas de suicide d’adolescents ayant été victimes de cette forme de harcèlement ont été signalés dès 2013 amenant les autorités de plusieurs pays à prendre en compte ces phénomènes.

**Cyberprotection**

*(Cyberprotection)*

Ensemble des mesures techniques et non techniques de protection permettant à un système d’information de résister à des évènements susceptibles de compromettre la disponibilité, l’intégrité ou la confidentialité des données stockées, traitées ou transmises, et des services connexes que ces systèmes offrent ou qu’ils rendent accessibles.

Synonyme :

Sécurité des systèmes d’information\* (SSI)[[82]](#footnote-83).

**Cyberrésilience**

*(Cyber résilience)*

La résilience se définit comme la capacité d’une organisation à faire face à des évènements (incident ou agression), à leur résister et à se rétablir. Appliquée au cyberespace, elle est appelée cyberrésilience et (se) définit comme la capacité d’un système d’information à résister à une panne ou une cyberattaque et à revenir à son état initial après l’incident[[83]](#footnote-84).

**Cybersécurité**

*(Cybersecurity)*

État recherché pour un système d’information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l’intégrité ou la confidentialités des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu’ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d’infor­mation et s’appuie sur la lutte contre la cybercriminalité et sur la mise en place d’une cyberdéfense[[84]](#footnote-85).

**Cybersquat**

*(Cybersquatting)*

Le *cybersquat* est une pratique qui consiste à acquérir des noms de domaines d’une marque, d’un pseudonyme, ou proche afin d’en tirer un profit (matériel ou moral). Ainsi, un particulier peut enregistrer un nom de domaine\* s’appuyant sur le nom d’une personnalité ou d’une entreprise en vue de lui revendre (spéculation au nom de domaine). Pour l’heure cette pratique n’est pas sanctionnée au pénal en France mais peut faire l’objet d’une plainte dans le cadre du respect de la propriété intellectuelle. Le *cybersquat* peut aussi être utilisé pour nuire à l’image d’une personnalité. Cette pratique est courante en politique et exponentielle en période électorale. Ainsi, le domaine sarkozy2017.fr et hollande2017.fr ont été enregistrés dès le mois d’octobre 2011.

# D

***Darknet***

(Réseau sombre ?)

Le terme *Darknet* a été médiatisé récemment dans le cadre du démantèlement de réseaux de cybercriminels ou de pédopornographies. Ainsi, le terme a été associé auprès du public à une forme d’Internet caché où se retrouvent les criminels. Le terme est pourtant plus ancien et caractérisait initialement un réseau non directement atteignable depuis ARPANET\* (ossature initiale d’Internet). Aujourd’hui on peut définir le *Darknet* comme un ensemble de réseaux pairs à pairs distribués anonymes. Ces réseaux sont ainsi créés par des utilisateurs qui souhaitent partager librement sans subir la surveillance d’Internet. L’usage de ces réseaux est généralement développé dans les milieux contestataires où au sein des communautés *underground.* Pour autant, le *Darknet* offre également des possibilités pour développer la liberté d’expression et l’échange d’information dans les pays pratiquant une censure violente de l’Internet, il est donc également utilisé par des journalistes et des citoyens engagés. Ainsi, le *Darknet* n’est pas si noir…

**DARPA - *Defense Advanced Research Projects Agency***

La DARPA est une agence du département de la défense américain. L’agence est principalement en charge de la recherche et du développement de nouvelles technologies pour une application militaire. Héritier du *National Defense Defense Research Committee* (1940), la DARPA a pris sa forme actuelle en 1958 créée en réaction au lancement du satellite Russe Spoutnik. Les premiers axes de recherche touchent principalement le domaine spatial (dont déjà la défense anti-missiles) et le nucléaire. La DARPA finance également des projets plus originaux et futuristes, dans le domaine de l’intelligence artificielle par exemple. En matière de réseaux et d’informatique l’agence est à l’origine du projet ARPANET\* lancé en 1969 et qui préfigure l’architecture décentralisée de l’Internet.

Voir ARPANET.

***Data center***

(Centre de traitement de données)

Lieu physique regroupant un ensemble d’ordinateurs et des systèmes de télécommunications afin de stocker, traiter et diffuser des informations. Sa fonction principale est d’assurer une bonne connexion réseau et un haut niveau de disponibilité des ressources. Les *datacenters* sont, par exemple, un élément essentiel des entreprises de l’Internet au premier rang desquelles figure *Google*. Ces centres regroupent des centaines ou des milliers de machines, principalement des serveurs qui sont disposés sur des « racks ». Leur besoin en énergie est considérable, pour d’une part alimenter les serveurs mais surtout assurer la climatisation des salles.

***Data mining***

(Exploration des données – Analyse intelligente des données)

L’exploitation de données, ou fouille de données, est un ensemble de processus et de technologies qui vise à dégager une information d’une quantité importante de données. Le *data mining* s’impose avec l’apparition de bases de données importantes et la numérisation constante de nombreux segments d’activités (commerce, santé, énergie, éducation). Les applications du *data* *mining* sont nombreuses et débouchent sur de l’analyse statistique et prédictive. Ainsi, est-il possible de déterminer des comportements de consommation, de séquencer le génome humain, de prévoir des pics de trafic routier ou encore d’améliorer la gestion des stocks d’une entreprise. Dans le domaine du marketing[[85]](#footnote-86), « Le *data* *mining* client est un processus de management des données client qui opère à partir des données élémentaires pour produire de l’information, de la connaissance en vue d’une action bien déterminée vis à vis des clients »[Michel Jambu, 2000].

***Data scientist***

Fonction liée à l’émergence des données de masse dans le monde de l’entreprise. Le *data scientist* (l’expression ne connaît pas encore de traduction en français) est ainsi responsable de l’analyse et de la gestion des données de masse au sein de sa structure. Mais au-delà, il est chargé de « créer de la valeur » à partir de ces données, il utilise ainsi des compétences issues du monde de la statistique mais il doit élargir son profil avec de la connaissance métier, de la communication, et des compétences techniques. Il n’existe pas à proprement parler de formation à cette fonction dont le périmètre est encore en pleine évolution.

Voir *Big data*.

**Datagramme**

*(Datagram)*

Élément structuré de données réseaux. L’usage du terme est réservé traditionnellement au protocole de communication de la couche liaison de données du modèle OSI\*, ou couche accès réseau du modèle TCP/IP\*. Pour les protocoles de plus haut niveau on parlera de « paquet\* » pour le protocole IP, de « segment » pour TCP\*.

Un datagramme contient des données (on parlera de charge\* utile ou *payload\**) ainsi qu’un en-tête permettant l’acheminement et le traitement du datagramme sur le réseau (adresse origine, adresse destination, etc.) et des informations de contrôle. Le datagramme IP est la « brique élémentaire » des échanges sur les réseaux TCP/IP. Voir également TCP\*.

Ci-dessous, la description du format d’un datagramme du protocole IP (communément appelé paquet IP).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **32 bits** | | | | |
| Version  (4 bits) | Longueur d'en-tête  (4 bits) | Type de service  (8 bits) | Longueur totale  (16 bits) | |
| Identification  (16 bits) | | | Drapeau  (3 bits) | Décalage fragment  (13 bits) |
| Durée de vie (8 bits) | | Protocole (8 bits) | Somme de contrôle en-tête (16 bits) | |
| Adresse IP source (32 bits) | | | | |
| Adresse IP destination (32 bits) | | | | |
| Données | | | | |

**Débit**

*(Flow – rate)*

Exprimé en Bit\* par seconde, ou en bauds, le débit correspond à la quantité d’information transmise par unité de temps dans un media. Dans les transmissions numériques on distingue alors le débit montant du client vers le serveur (*upload\**) et descendant du serveur vers le client (*download\**). Par commodité on exprime souvent le débit en Mo/s soit avec un facteur huit par rapport au Mbit/s (rappel un octet = 8 bits)

Voir Bit, Bande passante.

**Déception (manœuvre de)**

*(Deception)*

Dans la terminologie militaire une manœuvre de déception est un ensemble de mesures visant à induire l’ennemi en erreur. Ces manœuvres utilisent des trucages, de la désinformation des falsifications, en vue d’inciter l’adver­saire à réagir d’une manière préjudiciable à ses propres intérêts[[86]](#footnote-87). Un exemple parfaitement illustratif de manœuvre de déception est l’opération Fortitude qui fut conduite par les forces Alliés durant l’année 1944 et qui avait pour objectif de laisser penser à un débarquement dans la région du Pas de Calais et non en Normandie.

**Déchiffrement**

*(Decryption)*

Transformation d'un message chiffré en un message clair (donc intelligible) à l’aide de la clé de déchiffrement. Il est ainsi assez courant de confondre déchiffrement et décryptement alors que la première action suppose d’avoir la clé et que la seconde est le résultat d’un long processus et de multiples tentatives. Ce processus, pas toujours déterministe, est appelé cryptanalyse\*.

**Décrypter**

(*Decipher*)

Action qui consiste à retrouver un texte clair à partir du chiffré sans disposer de la clé secrète associée.

**DECT - *Digital Enhanced Cordless Telecommunication***

DECT est une norme pour la radiocommunication numérisée point à point [EN 300 175]. Elle est principalement utilisée pour la téléphonie sans-fil numérique qui équipe les particuliers comme les entreprises. La norme prévoit le transfert entre cellule ce qui permet dans le cadre professionnel par exemple de se déplacer dans des espaces plus grands en configurant plusieurs points d’accès dans un bâtiment. Cette souplesse est la conséquence de l’utilisation d’une bande de fréquence dédiée (1880-1900 Mhz) et relativement peu utilisée.

**Défacement - défaçage - défiguration**

*(Defacing)*

Les sites Web représentent des cibles de choix pour les attaquants qui souhaitent obtenir une forme de reconnaissance au sein de leur communauté. Les défigurations consistent à modifier le contenu d’un site. La modification peut être visible (modification de la page d’accueil) ou plus discrète. Dans ce dernier cas, seul les utilisateurs expérimentés et les administrateurs découvriront que des contenus ont été modifiés.[[87]](#footnote-88)

Des opérations de défacement ont été conduites par des hackers russes contre les sites gouvernementaux géorgiens en 2008 et plus récemment par l’Armée Syrienne Electronique (SEA) contre des sites d’information occidentaux. Le défacage est un mode d’action régulièrement employé par des groupes cherchant à produire un effet médiatique immédiat.

**Défaut**

*(Default)*

Une valeur attribuée automatiquement par un programme ou un ordinateur et qui demeure jusqu'à ce que l'utilisateur établisse un autre réglage.

**DEFCON** **- DEFense CONdition**

Le DEFCON désigne le niveau d’alerte des forces américaines, il est établi sur une échelle de 1 à 5. Le DEFCON 1 correspondant au plus haut niveau d’alerte et le DEFCON 5 au niveau normal de préparation du temps de paix.

La DEFCON est aussi une conférence de sécurité informatique qui rassemble des *hackers*\* du monde entier. Elle se tient annuellement à Las Vegas dans le prolongement de la *black hat\*.*

**Défense en profondeur**

*(In depth defense - defense in depth)*

Le concept de défense en profondeur puise son origine dans la tactique militaire. Il s’agit de protéger un lieu par la mise en place de *lignes de défense\** successives et autonomes. Ce concept sera ensuite utilisé plus largement dans tous les domaines liés à la sureté (industrie, transport). Le concept se développe progressivement dans le milieu de la sécurité des systèmes d’information et nécessite encore des ajustements. Le Mémento de la défense en profondeur de l’ANSSI propose la définition suivante.

La défense en profondeur du système d'information est une défense globale et dynamique, coordonnant plusieurs lignes de défense couvrant toute la profondeur du système. Le terme profondeur doit être compris au sens le plus large, c’est à dire dans l’organisation du SI, dans sa mise en œuvre et enfin dans les technologies utilisées. Il s’agit alors de permettre des actions de neutralisation des atteintes contre la sécurité, à moindre coût, grâce à une gestion des risques, un système de renseignement, une planification des réactions et l'enrichissement permanent grâce au retour d'expérience. Cette défense en profondeur a un double but : i) renforcer la protection du système d'information par une approche qualitative permettant de vérifier la complétude et la qualité du dispositif, ii) donner un moyen de communication fort permettant aux décideurs et aux utilisateurs de prendre conscience de la gravité des incidents de sécurité[[88]](#footnote-89).

**Déni de service**

*(Denial of service - DOS)*

Voir DOS.

**Dématérialisation**

*(Dematerialization)*

La dématérialisation est l’opération qui consiste à remplacer les supports physiques de stockage ou de transport de l’information par des moyens numériques. En France les marchés publics passés avec l’administration sont dématérialisés, il y a possibilité de conclure des marchés par voie électronique.

Ce processus de dématérialisation pose toutefois de nouvelles contraintes aux structures ou entreprises qui le mettent en œuvre. En effet, il suppose de mettre en place des moyens de stockage et d’archivage permanents et redondants, de disposer d’un système fiable de signature numérique\* (afin de garantir l’identité\* des émetteurs de documents) et d’une politique de sécurité\* adaptée.

**Démultiplexage**

*(Demultiplexing)*

Action de restituer les signaux à partir d’un signal composite obtenu par multiplexage[[89]](#footnote-90).

Voir Multiplexage.

**Dépassement ou débordement de mémoire**

*(Buffer overflow)*

Le *buffer overflow* est une technique d’exploitation de vulnérabilité dans le code d’un programme qui ne vérifie pas correctement la taille de certaines données qu’il manipule[[90]](#footnote-91).

En langage C, par exemple, certaines fonctions comme *strcpy* (copie d’une chaine de caractères) ne contrôlent pas que la zone de mémoire de destination soit de taille suffisante pour accueillir les données à copier. Il est alors possible d’écraser (ou de déborder) des zones mémoire du processus en cours d’exécution, en entrant plus de données que ce que la zone mémoire de destination pouvait contenir. Pour exploiter une telle vulnérabilité, il s’agira de parvenir à écraser la zone de mémoire qui contient l’adresse de la prochaine instruction à exécuter pour le processus, permettant ainsi à l’attaquant de contrôler le flot d’exécution du programme en cours et ainsi lui offrir la possibilité d’exécuter son propre code.

Des mesures correctrices existent pour éviter ces dépassements de mémoire tampon. Il convient par exemple d’utiliser la fonction *strlcpy* au lieu de *strcpy* car elle prend en paramètre la taille de la zone mémoire de destination, et peut ainsi vérifier que les données à copier ne débordent pas.

Le *buffer overflow* est la vulnérabilité la plus courante (et donc la plus exploitée par les attaquants informatiques). Les éditeurs de logiciels, de compilateurs, de systèmes d’exploitation et de matériel informatique ont donc mis en place des mécanismes de protection tel que les restrictions d’usage des zones mémoires (bit « NX » pour les processeurs Intel) par exemple, mais également des outils de vérification lors de la compilation de code ( outil « canari » dans le compilateur GCC).

**DES - *Data Encryptions Standard***

Algorithme de chiffrement symétrique par bloc. DES, décrit dans les années 70, est considéré aujourd’hui comme obsolète. Il utilise des clés de 56 bits, et manipule des blocs de données de 64 bits suivant un processus itératif de transformation après avoir subit une permutation initiale. Les implémentations de DES sont vulnérables à la cryptanalyse (notamment différentielle) et son usage est aujourd’hui limité, il est remplacé par le triple DES et AES.

Voir Triple DES, AES.

**Désinformation**

*(Disinformation)*

Selon la terminologie militaire française, la désinformation est une manœuvre consistant à tromper l'ennemi en lui fournissant délibérément des informations erronées dans le but de lui faire modifier, éventuellement, son dispositif militaire[[91]](#footnote-92).

Les outils numériques (en particulier les médias sociaux) se prêtent parfaitement à la mise en œuvre de ce type de manœuvre par leur simplicité d’usage, leur rapidité de diffusion et leur capacité à toucher des audiences importantes.

**Détection**

*(Detection)*

En sécurité informatique, une détection consiste à rechercher et identifier dans une masse de données issues du système d’information, celles qui sont caractéristiques d’un incident de sécurité (tentative d’attaque, communication vers un serveur de commande et de contrôle connu, exécution de code malveillant, etc.). En théorie du signal, la détection est une étape du traitement du signal.

Voir IDS, Logiciel malveillant.

**Détection d’erreur**

La détection d’erreur regroupe les opérations qui consistent à identifier les informations numériques erronées après transmission et réception. Les erreurs sont généralement générées par les mécanismes de transmission.

**Détournement de DNS**

*(DNS Tunneling)*

Le détournement de DNS est un type d’exploitation du DNS\* qui consiste à utiliser le trafic DNS comme un canal caché\* pour contourner les mécanismes de sécurité classiques (*firewall\**). Ainsi, un programme malveillant installé sur un poste client pourra communiquer vers son donneur d’ordre (le serveur de commande et de contrôle) en encapsulant son trafic dans des requêtes DNS. Ces dernières ne sont que très rarement filtrées et ainsi, un canal de communication discret existe entre la machine infectée et le pirate.

**Détournement de nom de domaine**  
*(Pharming)*

Le détournement de domaine, ou encore *pharming* en anglais, est un type d’attaque du DNS\* qui consiste à rediriger les requêtes internet des utilisateurs vers un faux domaine (site Web) généralement piégé. L’objectif de cette opération consiste à récupérer des informations personnelles de l’utilisateur ainsi redirigé (information de connexion comme, login et mot de passe). Mise en œuvre, un détournement DNS est une attaque du type « homme du milieu » (*man in the middle\*)*

Ce type d’attaque est également appelé **clonage de serveur DNS** (DNS *Pharming*), l’ANSSI en donne alors la définition suivante : activité malveillante visant à modifier un serveur DNS (serveur de noms de domaine), dans le but de rediriger un nom de domaine vers une adresse IP différente de l’adresse légitime. En croyant aller sur un site connu, l’internaute navigue en réalité sur un site factice. Le trafic envoyé au domaine souhaité (organisme bancaire, messagerie électronique, etc.) peut être capturé par un utilisateur malveillant, qui, par exemple, a déjà copié des pages du domaine visé à l’adresse nouvellement indiquée par le DNS. La personne qui se connecte au domaine risque alors d’entrer des informations confidentielles sur le site factice, même si elle a pris la précaution de renseigner l’adresse correcte.

**DHCP - *Dynamic Host Configuration Protocol***

Le protocole DHCP assure l’affectation et la configuration dynamique du paramétrage IP\* des éléments d’un réseau. Concrètement, à la connexion d’une nouvelle machine dans un réseau IP, cette dernière doit disposer d’une adresse unique dans ce réseau (et appartenant au même réseau logique que toutes les autres machines), d’un masque de sous-réseau, d’une adresse de DNS\* (pour pouvoir effectuer les résolutions de noms d’hôtes) et une adresse de passerelle (qui permet de communiquer avec d’autres réseaux, comme ceux accessibles via Internet par exemple). Sans adresse initiale, la nouvelle machine va donc envoyer un message général (*broadcast\**) sur tout le sous-réseau pour identifier le serveur DHCP (celui qui va lui fournir les informations nécessaires). Ce message, appelé le DHCPDISCOVER, attend en réponse une proposition d’adresse de la part du serveur DHCP. Ce dernier répond donc avec un DHCPOFFER qui permet à la machine demandeuse de se préparer à la configuration. La machine demandeuse répond alors avec un message DHCPREQUEST pour valider son adresse IP, normalement le serveur répond avec un message DHCPACK. A l’issue de ce dialogue la nouvelle machine dispose d’une configuration locale lui permettant de communiquer sur le réseau.

**Diffie-Hellman**

Portant le nom de ses deux créateurs, la méthode DH est, en cryptographie, une méthode d’échange de clés\* dans un système à clé publique\*. Cette technique permet donc à deux utilisateurs (Alice\* et Bob\*) d’échanger des clés via un support non sécurisé. L’IETF\* standardise la méthode pour l’Internet en 1999 dans la RFC\*2631.

Le principe repose sur des notions d’arithmétique élémentaires et l’existence de fonctions dites « à sens unique ». Ainsi, il est facile d’élever un nombre à une puissance mais il est beaucoup plus difficile de faire l’opération inverse. Ce problème dit du calcul du logarithme discret devient particulièrement difficile avec des nombres très grands dans des ensembles mathématiques possédant des propriétés limitées. Dans l’échange Diffie-Hellman c’est un nombre choisi en commun et élevé à la puissance « n » qui sera transmis sur le canal non sécurisé. Ainsi, il sera très difficile à Eve\* de retrouver le nombre partagé entre Alice et Bob car il lui faudra factoriser le grand nombre intercepté.

***Pour aller plus loin***

Un peu de mathématiques…

*Rappel sur les nombres premiers et le modulo :*

Un nombre est dit premier si et seulement si c’est un entier naturel qui n’admet que deux diviseurs entiers positifs (1 et lui-même). Les nombres premiers sont essentiels en arithmétique car le théorème de factorisation unique (ou théorème fondamental de l’arithmétique) stipule que : tout entier strictement positif peut être écrit comme un produit de nombres premiers d’une unique façon, à l’ordre près des facteurs.

Une autre notion est essentielle dans la méthode Diffie-Hellman, il s’agit du reste de la division euclidienne : cette opération est appelé *modulo*. Ainsi, si a et n sont deux entiers naturels, on notera *a mod n* le reste de la division euclidienne de a par n.

*Le déroulement de l’échange entre Alice et Bob :*

Pour engager leur échange, Alice et Bob doivent préalablement choisir un nombre premier p et une base g.

- Alice choisit un nombre secret a (une clé secrète)

- Alice effectue le calcul ga mod p (donc élève g à la puissance a, puis calcule le reste de la division euclidienne de ga par p). Le résultat de ce calcul, noté A est envoyé à Bob sur le canal non sécurisé.

- De son côté Bob choisit également un nombre entier secret b, il effectue un calcul identique à Alice avec cet entier : gb mod p et transmet vers Alice le résultat de son calcul noté B.

- Alice reçoit B et calcule k=(B)a mod p qui deviendra la clé de chiffrement (clé secrète partagée)

- Bob effectue de son côté le calcul k=(A)b mod p.

Alice et Bob ont maintenant calculés une clé de chiffrement commune (clé secrète partagée) car (B)a mod p = (gb mod p)a mod p = gab mod p = (ga mod p )b mod p = (A)b mod p !

Ainsi pour un observateur malveillant, présent à l’écoute sur le canal de communication (Eve ou Max), et ayant intercepté cet échange il sera extrêmement difficile (au sens mathématique) de factoriser A et B pour espérer en déduire la clés commune k. Ainsi la sécurité de la méthode repose sur la difficulté de calculer k à partir de gamod p et de gbmod p lorsque p est grand car la fonction f(x) = gx mod p est une fonction à sens unique.

*Les limites du Diffie Hellman ?*

Si les mathématiques qui sous tendent la méthode sont solides, la procédure d’échange de clé Diffie Hellman est toutefois sensible aux attaques dites homme du milieu\* (man in the middle). En effet si Eve ne peut, par la simple interception des échanges « casser » la clé, il lui suffit de calculer sa propre clé k1 et de la transmettre à Alice puis une clé k2 pour la transmission vers Bob. Lorsqu’Alice croyant communiquer avec Bob envoie son message chiffré, Eve le déchiffre, puis le chiffre à nouveau vers Bob. De ce fait, Eve intercepte la totalité du flux chiffré entre Alice et Bob.

**Diffusion de Rayleigh**

*(Rayleigh scattering)*

Phénomène physique présent dans les transmissions par fibres optiques. La diffusion de Rayleigh entraîne, en raison de l’hétérogénéité des matériaux, des pertes lorsque la longueur de la fibre est importante (pertes linéiques) ainsi qu’une réfraction vers la source du signal (rétrodiffusion).

**Dispersion**

*(Dispersion)*

Lors de la transmission par fibre, la dispersion représente la différence de temps de parcours dans une même fibre. Le phénomène entraine une limitation de la bande passante\*. Il existe plusieurs type de dispersion en fonction des modes (polarisation, chromatique, chromatique décalée).

**Disponibilité**

*(Availability)*

La disponibilité d’un système traduit généralement son accessibilité au moment voulu. C’est un paramètre essentiel de la qualité de service. En matière de sécurité informatique, la disponibilité est un des critères de la sécurité (avec la confidentialité, l’intégrité et la non-répudiation). Il s’agit alors de la propriété d’un objet qui est accessible et qui fonctionne de la façon souhaitée pour les autres objets avec lesquels il doit interagir.

**Disque dur**  
*(Hard disk)*

Le disque dur est un disque magnétique qui permet de conserver les données sur les ordinateurs et autres supports électroniques. Le disque dur, inventé en 1956 par Reynold Johnson, a vu ses capacités de stockage augmenter exponentiellement pour atteindre aujourd’hui plusieurs Téra-octets. Le système étant mécanique (le disque tourne sur un lecteur entre 3 600 et 15 000 tours par minutes) ce système demeure fragile et sensible aux chocs.

**Distribué**

*(Distributed)*

Dans une architecture réseau distribuée, une même fonction peut être assurée par plusieurs nœuds. Le mode distribué s’oppose au mode centralisé où, par exemple, le traitement d’une information est réalisé par un seul et unique équipement.

**DLCI- *Data Link Channel Identifier***

(Identifieur de voie logique)

Dans un réseau commuté de type « relayage de trames » ou *frame relay\**, le DLCI permet l’acheminement des trames au niveau de chaque commutateur. Au sein du réseau, l’adressage est donc réalisé par l’intermédiaire du champ DLCI, ce champ étant modifié au passage de chaque nœud du réseau.

**DLL- *Dynamic Link Library***

(Bibliothèque de liens dynamiques)

La DLL est une librairie de fonctions exécutables ou de données qui peuvent être utilisées par des applications Windows. Ce mécanisme permet de stocker des fonctions communes dans des composants logiciels réutilisables, qui seront appelés par les programmes qui en ont besoin. Ceci allège la taille des logiciels (par opposition à une compilation statique).

**DMZ - *Demilitarized zone***

(Zone démilitarisée)

Terminologie clairement empruntée au registre militaire, la DMZ dans un réseau représente la partie située entre le LAN\* (réseau interne) et le WAN\* (réseau externe). La DMZ est donc une interface entre l’extérieur et l’intérieur d’un système d’information, une zone intermédiaire qui peut contenir différents équipements comme des pare-feu, un serveur Web et un serveur de messagerie.

**DNS - *Domain Name System***

(Système de noms de domaine)

Le système de noms de domaine permet aux utilisateurs une navigation plus simple sur Internet en associant un nom à une adresse IP\*. Chaque ordinateur relié à Internet dispose d’une adresse unique appelée « adresse IP » (adresse de protocole Internet). Étant donné que les adresses IP (qui sont codées sur 4 ou 6 octets) sont difficiles à mémoriser, le DNS permet d’utiliser à la place une série de lettres familières (le nom de domaine). Le système de noms de domaine est dit « hiérarchisé », son sommet est appelé « racine » et on le figure par un point. Chaque domaine peut être subdivisé en sous-domaines, les sous-domaines immédiatement sous la « racine » sont appelés *Top Level Domain (TLD)* ou domaines de premier niveau. Les autres domaines particuliers sont :

gTLD pour *generic* TLD il s’agit des .com .org ;

ccTLD pour *contry code TLD* regroupant les extensions pays (.fr, .uk etc).

Le système de nommage, outre la subdivision de domaines, met en œuvre également un système de délégation. Une délégation indique que les informations relatives au sous-domaine considéré sont enregistrées sur un autre serveur. Ainsi sur un serveur particulier, il existe un ensemble de domaines et sous-domaines associés qui seront non délégués. Cet ensemble est appelé zone. Une telle organisation hiérarchique avec délégation est essentielle dans le processus de résolution de nom de domaine qui permet d’accéder à une ressource.

**DNSSEC**

Extension sécurisée du protocole DNS.

**Domaine**

*(Domain)*

Un domaine (Internet) est une entité qui représente un ensemble de machines reliées au réseau qui présentent les mêmes caractéristiques. Ainsi, le domaine est une entité logique permettant la gestion de plusieurs machines. Le système de noms de domaine (DNS) est organisé de façon hiérarchique et permet ainsi une gestion décentralisée des ressources.

Voir également DNS et Nom de domaine.

**Domotique**

La domotique regroupe l’ensemble des technologies utilisées pour assurer la gestion et le pilotage de nombreux services liés à l’habitat. S’appuyant sur le concept de « maison connectée », la domotique offre aujourd’hui des solutions de pilotage et de supervision de la sécurité (alarmes, vidéosurveillance), de l’efficacité énergétique, de l’entretien des espaces verts, de la maintenance de certains équipements, etc.

**Données**

*(Data)*

En théorie de l’information, une donnée est une description élémentaire d’une réalité. Cette description est généralement codée pour favoriser son classement, sa conservation et sa manipulation. La définition officielle parle alors d’une représentation d’une information sous une forme conventionnelle destinée à faciliter son traitement[[92]](#footnote-93).

Les données sont aujourd’hui au cœur des enjeux du cyberespace, leur quantité, leur stockage, leur sécurité, leur valeur, autant de sujets qui ne trouvent pas de réponses simples et intuitives. Les données peuvent ainsi être « ouvertes », « personnelles », « massives », « structurées ou non », il existe même des « métadonnées\* »…

**Données massives**

*(Big data)*

Voir *Big data.*

**Données ouvertes**

*(Open data)*

Données qu'un organisme met à la disposition de tous sous forme de fichiers numériques afin de permettre leur réutilisation. Les données ouvertes n'ont généralement pas de caractère personnel, elles sont accessibles dans un format favorisant leur réutilisation (qui peut être soumise à conditions)[[93]](#footnote-94).

**Données personnelles**

*(Personnal data)*

Elément permettant d’identifier ou rendant identifiable une personne, directement ou non. Ainsi en France la Loi propose la définition suivante :

Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d’identification ou à un ou plusieurs éléments qui lui sont propres[[94]](#footnote-95).

**Données sensibles**

En droit français, les données sensibles ont une définition particulière liée à la notion de données personnelles (ou données à caractère personnel). Cette notion peut donc avoir un sens diffèrent lorsqu’elle est employée dans un contexte particulier (industrie, sécurité informatique, etc.). Ainsi, les données sensibles sont des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l’appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci[[95]](#footnote-96).

**Dorsale Internet**

*(Internet Backbone)*

De façon générale, une dorsale est la partie principale d'un réseau de télécommunication, celle qui dispose du plus grand débit, celle encore vers qui convergent les réseaux secondaires (affluents). Voir *Backbone.*

**DoS et DDoS :**

*(Denial of service - Deny Of Service)*

Un déni de service est un acte de malveillance portant atteinte à la disponibilité\* d’un objet. Dans un contexte réseau, il s’agit de rendre indisponible, durant une certaine période, l’accès aux services ou ressources d’un serveur cible. Trivialement, la saturation du réseau est obtenue par génération d’un trafic important non désiré, d’origine malveillante provoquant alors l’indisponibilité totale ou partielle de la cible.

Cette attaque peut être conduite depuis une source unique (mono source) ou utiliser de nombreux ordinateurs (distribuée), le plus souvent à l’insu des utilisateurs légitimes. On parle alors de déni de service distribué (DDoS).

***Downlink***

(Lien descendant)

En télécommunication spatiale, le *downlink* (lien descendant) désigne une communication entre le satellite et une station sol.

Voir *Uplink.*

***Download***

(Téléchargement)

Voir Téléchargement, Télécharger.

***Doxing***

Le *doxing* est une pratique liée à la collecte, sur Internet, d’informations ciblées pouvant, par la suite, faire l’objet d’une révélation publique. La pratique a été rendue populaire par certains groupes d’activistes qui ont publié des données à caractère personnel. Ainsi, le collectif Anonymous a, entre autres, divulgué, au mois de novembre 2014, les identités de membres du Ku Klux Klan. Le *doxing* est régulièrement utilisé pour dénoncer des utilisateurs de réseaux sociaux qui postent des contenus à caractère raciste ou discriminatoire.

**DPI - *Deep Packet Inspection***

(Contrôle en profondeur des paquets)

Le DPI est une technique de contrôle en profondeur des paquets de données échangés sur un réseau. Sur un équipement d’infrastructure réseau il permet de contrôler le contenu et les en-têtes de paquets (IP en général). Cette technique est utilisée pour générer des statistiques d’utilisation, la mise en œuvre de filtres (contrôle *anti-spam*), la détection des attaques mais également la lutte contre le « piratage » (propriété intellectuelle) et les systèmes de censure et de contrôle de l’Internet.

**Drapeau**

*(flag)*

Bit\* de données utilisé pour décrire deux états (0 ou 1) afin de délimiter un bloc de données ou de spécifier l’état « activé » ou « désactivé » d’une fonction (également appelé délimitateur ou fanion). Le terme *flag* est également utilisé pour certains concours organisés par les hackers (*capture the flag\* – CTF)*, succession de défis à réaliser sur un système cible.

Voir *Capture the flag.*

**DRM - *Digital Right Management***

Système assurant la gestion numérique des droits d’auteurs. Les DRM limitent ainsi parfois la copie de certains supports ou leur lecture sur un nombre déterminé de terminaux.

**DSL – *Digital Subscriber Line***

(Ligne d’abonné numérique)

Techniques qui permettent, sur un réseau filaire (ligne téléphonique), la transmission de données numériques. Ces techniques permettent une meilleure exploitation des fils de cuivre en optimisant les possibilités de transmission sur l’ensemble du spectre. Il existe plusieurs mécanismes et l’on utilise souvent l’acronyme xDSL pour évoquer les différentes normes DSL. La plus courante étant ADSL\*

**DSLAM - *Digital Subscriber Line Multiplexer***

(Multiplexeur d’accès à la ligne d’abonné numérique)

Le DSLAM est un équipement de multiplexage qui permet l’accès des abonnés aux services DSL par une ligne téléphonique. Placé généralement dans les centraux téléphoniques NRA\*, le DSLAM permet de regrouper le trafic DSL des abonnés qui y sont rattachés et de le transférer vers le réseau de l’opérateur internet.

**DSS - *Digital Signature Standard****)*

Ensemble standardisé d’algorithmes de signature numérique\* adopté par le NIST\* - *National Institute of Standards and Technology* aux Etats-Unis. La dernière modification a été adoptée le 19 juillet 2013 sous la référence FIPS 188-4.

***Dump***

(Cliché)

Le verbe anglais *to dump*, a donné par extension l’expression *dumper*, action qui consiste à recopier le contenu (à un instant donné) d’une mémoire (ou d’un disque). Le résultat de cette action est également appelé un *dump* ou cliché suivant la terminologie française.

***Duplex***

*(*Duplex*)*

Technique de transmission des informations qui permet d’échanger dans les deux sens de communication sur un même canal. On parlera de communication *half-duplex* lorsque la communication ne peut s’établir que dans un seul sens à la fois, et de *full-duplex* lorsqu’elle peut être menée dans les deux sens simultanément.

**Duqu**

Logiciel malveillant\*, dont certaines caractéristiques se rapprochent de *Stuxnet*\*, qui a été une première fois découvert au mois de septembre 2011 par le laboratoire CrySyS Lab. Baptisé *Duqu*, car le cheval de Troie\* créait des fichiers avec des extensions de type DQ dans leur nommage, son objectif est de collecter des informations sur les systèmes de contrôle industriels dans le but de conduire ultérieurement des attaques. Offrant une large gamme de services, il s’agit clairement d’un outil de « reconnais­sance », étant du type RAT\* (cheval de Troie). L’outil ne se reproduit pas mais semble, selon les recherches conduites pas Symantec, avoir visé un nombre très limité de machines et donc être particulièrement ciblé. En dépit de sa première détection au mois de septembre 2011, les analystes estiment que des attaques utilisant cet outil ont pu être lancées dès le mois de décembre 2010 (rendant alors la filiation avec *Stuxnet* encore plus probable). *Duqu* se présente en effet comme un module adaptable avec une architecture assez souple. Les informations ainsi collectées étaient ensuite placées et chiffrées dans un fichier compressé, stocké localement, avant d’être exfiltré. L’étude a révélé l’utilisation de fichiers photos au format JPG\* pour conduire l’exfiltration de données. En revanche, *Duqu* présente une caractéristique notable d’auto-désinstallation. En effet, le *trojan\** était configuré pour fonctionner durant 36 jours avant de se désinstaller du système. Enfin, le vecteur d’attaque n’avait, une fois encore, rien d’extra­ordinaire puisqu’à l’origine de la diffusion on retrouve une campagne de « *spear-phishing*\* » ciblée avec un document Microsoft Word corrompu. Une fois la pièce jointe ouverte par l’utilisateur, deux fichiers exécutables sont déchiffrés, un lecteur (driver) et un module d’installation d’une bibliothèque de liens dynamiques (DLL\*). Le lecteur injecte alors le code qui exécute l’installation. Ce mécanisme utilise, à l’image de Stuxnet[[96]](#footnote-97), une vulnérabilité du noyau Windows de type « zéro-day »\*.

Enfin, au mois de juin 2015 une nouvelle variante a été découverte par le laboratoire Kaspersky dans ses propres systèmes d’information, mais également chez une centaine d’autres victimes (dont certaines en lien avec les négocia-  
tions sur le nucléaire iranien). Cette dernière variante est appelée *Duqu 2.0*.

***Duqu***

Au mois de septembre 2011, *Duqu*, un outil de cyberespionnage est détecté en Iran et au Soudan.

Type de malware : RAT, Remote Access Trojan.

Objectif : Cyberespionnage.

Cible : Programme nucléaire iranien.

Date de création : estimée au mois de novembre 2010.

Date de détection : septembre 2011, par le laboratoire de cryptographie et de sécurité de l’université polytechnique et économique de Budapest[[97]](#footnote-98) (CrySyS Lab). Symantec[[98]](#footnote-99) et F-Secure ont également analysé cette attaque et produit des rapports très élaborés.

Versions connues : Une quinzaine.

Taille : 300 kb.

Caractéristiques principales : Duqu est rapidement présenté comme « très proche » de Stuxnet mais avec un objectif totalement différent. Symantec conclut dans son rapport qu’il s’agit ici du précurseur du futur Stuxnet. Duqu, serait donc une opération de reconnaissance avant une nouvelle opération de sabotage. Plusieurs systèmes de commande et de contrôle (C&C) ont pu être identifiés en Inde, Belgique et Vietnam. La localisation de ces serveurs n’apporte toutefois aucun élément sur la nationalité de l’attaquant.

# E

**EAP - *Extensible Authentication Protocol***

EAP est un protocole d’authentification\* décrit dans la RFC\* 3748. Il s’agit d’une extension du protocole PPP\* qui est utilisée pour authentifier l’accès réseau pour les connexions distantes, les réseaux privés virtuels ainsi que les points d’accès sans fil.

Une architecture EAP repose sur trois éléments distincts :

• Un client d’accès (ordinateur qui cherche à accéder à un réseau) ;

• Un point d’accès qui nécessite une authentification EAP (appelé authentificateur EAP) ;

• Un serveur d’authentification dont la fonction est de négocier la méthode EAP avec le client\*, de valider les informations d’identification et d’autoriser, ou pas, l’accès au réseau. On utilise le plus souvent un serveur RADIUS\* — *Remote Authentication Dial-In User Service*.

EAP dispose d’une quarantaine de méthodes d’authen­tification (ce qui explique la phase de négociation avec le client). Parmi les plus connues ont peut citer : MD5\* - *Message Digest* 5, PEAP, LEAP, PSK, TLS\* et TTLS.

**EBIOS (méthode) – Evaluation des besoins et identification des objectifs de sécurité**

La méthode EBIOS est une méthode utilisée en sécurité des systèmes d’information et développée par l’ANSSI, Agence Nationale de Sécurité des Systèmes d’Information. Elle permet d’apprécier et de traiter les risques relatifs à la sécurité des systèmes d’information (SSI). Elle permet aussi de communiquer à leur sujet au sein de l’organisme et vis-à-vis de ses partenaires, constituant ainsi un outil complet de gestion des risques SSI[[99]](#footnote-100). La méthode est itérative et repose sur cinq modules :

• Module 1 : Établissement du contexte ; vise à fixer le cadre de la gestion des risques, les métriques et le périmètre de l'étude.

• Module 2 : Étude des événements redoutés ; il contribue à l'appréciation des risques. Il permet d'identifier et d'estimer les besoins de sécurité des biens essentiels (en termes de disponibilité, d'intégrité, de confidentialité...), ainsi que tous les impacts (sur les missions, sur la sécurité des personnes, financiers, juridiques, sur l'image, sur l'environnement, sur les tiers et autres...) en cas de non respect de ces besoins et les sources de menaces (humaines, environnementales, internes, externes, accidentelles, délibérées...) susceptibles d'en être à l'origine, ce qui permet de formuler les événements redoutés.

• Module 3 – Étude des scénarios de menaces ; il s'inscrit également dans le cadre de l'appréciation des risques et consiste à identifier et estimer les scénarios qui peuvent engendrer les événements redoutés, et ainsi composer des risques. Pour ce faire, sont étudiées les menaces que les sources de menaces peuvent générer et les vulnérabilités exploitables.

• Module 4 – Étude des risques ; le quatrième module met en évidence les risques pesant sur l'organisme en confrontant les événements redoutés aux scénarios de menaces. Il décrit également comment estimer et évaluer ces risques, et enfin comment identifier les objectifs de sécurité qu'il faudra atteindre pour les traiter.

• Module 5 – Étude des mesures de sécurité ; le cinquième et dernier module s'inscrit dans le cadre du traitement des risques. Il explique comment spécifier les mesures de sécurité à mettre en œuvre, comment planifier la mise en œuvre de ces mesures et comment valider le traitement des risques et les risques résiduels[[100]](#footnote-101).

**Échantillonnage**

Lors de la conversion d’un signal analogique\* en un signal numérique\*, action qui consiste à prélever de façon périodique un échantillon du signal analogique source.

Voir Numérique, Numérisation, Shannon (Théorème), Analogique.

**EFF- *Electronic Fontier Foundation***

L’EFF est une organisation non gouvernementale dont l’objectif est de défendre « les droits et libertés des citoyens dans un monde numérique ». Fondée en 1990 aux Etats-Unis, l’EFF œuvre quotidiennement pour la liberté d’expression sur Internet et l’accompagnement du développement des nouvelles technologies pour préserver les droits fondamentaux. L’EFF défend, à ce titre, le droit des journalistes à préserver l’identité de leurs sources. Depuis les révélations d’Edward Snowden en 2013 sur les programmes de surveillance de masse, l’EFF s’est engagé dans des campagnes de sensibilisation et de dénonciation de ce type d’activités jugées liberticides.

**EGP - *Exterior Gateway Protocol***

EGP est une famille de protocoles utilisés par les routeurs périphériques pour interconnecter des réseaux et systèmes

autonomes (AS\*) distincts. BGP\* est un protocole EGP utilisé entre AS pour le routage\* internet.

Voir BGP, Routage, EIGRP.

**EIGRP- *Enhanced Interior Gateway Routing Protocol***

EIGRP est un protocole de routage\* dynamique développé en 1985 par CISCO. Améliorant IGRP (également propriétaire CISCO), il converge plus vite que ce dernier. EIGRP envoie les informations de routage vers ses voisins puis les mises à jour de table (IGRP envoie lui la totalité de sa table de routage\* toutes les 90 secondes). Enfin, EIGRP fonctionne avec Novell IPX\* et Apple TalK. Il utilise un algorithme spécifique (DUAL - *Diffusing* *Update Algorithm*) vecteur distance mais intègre des améliorations qui prennent en compte l’état des liaisons. Cœur du protocole, l’algorithme de diffusion DUAL prend en compte de nombreux paramètres pour calculer la meilleure route (bande passante, nombre de nœuds, charge, fiabilité). En matière de sécurité, EIGRP utilise un système de signature\* afin d’authentifier les émetteurs de mise à jour de routes.

L’en-tête des messages EIGRP contient :

• *Datalink frame header*: les adresses MAC\* source et destination ;

• *IP Packet Header*: les adresses IP\* source et destination ;

• EIGRP *packet header*: le numéros de système autonome (Autonomous system AS) ;

• *Type/length/Values*: données propres aux messages EIGRP.

Enfin, EIGRP utilise cinq types de messages :

• Hello packets ;

• Update packets ;

• Acknoledgement packet ;

• Query packets ;

• Reply packets.

**EIR - *Equipement Identity Register***

Dans un réseau mobile, l’EIR est un équipement qui contient la base de données des identités des mobiles (IMEI\*). L’EIR permet d’autoriser ou non l’accès au réseau à un terminal. Il renferme des listes, blanches (mobiles autorisés), grises (mobiles avec dysfonctionnement) ou noires (mobiles non autorisés).

**EIR- *Excess Information Rate***

Débit autorisé au-dessus duquel toute trame\* peut être détruite.

**Elévation de privilège**

*(Privilege Escalation)*

L’élévation de privilège est une technique qui consiste à obtenir, sur un système, des droits supérieurs à ceux normalement accordés. Trivialement le mécanisme consiste, à partir de droits utilisateurs, à obtenir des droits d’admi­nistration par l’exploitation d’une vulnérabilité. L’élé­vation de privilège est utilisée par des attaquants qui cherchent à prendre le contrôle total d’un système d’infor­mation. Pour autant, l’élévation de privilège peut également être nécessaire à certaines applications qui nécessitent la modification de paramètres systèmes. Dans ce cas, une invite de commande permet de procéder à cette élévation et autorise l’exécution en mode administrateur (*root*).

**Embrouillage**

*(Scrambling)*

L’embrouillage est une transformation réversible d’un signal numérique\*, en vue d’en faciliter la transmission ou l’enregistrement, en un signal numérique de même signification et de même débit binaire[[101]](#footnote-102).

**Emulation**

*(Emulation)*

L’émulation est une technique qui permet d’imiter le fonctionnement d’un équipement spécifique sur un autre équipement. En phase de test, l’émulation permet ainsi de corriger les défauts de conception logicielle et améliorer la sécurité. On peut ainsi, sur un ordinateur personnel émuler des téléphones portables de différentes marques et modèles pour tester des applications avant leur mise en ligne. Enfin, il est également possible d’émuler un réseau complet de machines.

**En ligne**

*(On line)*

L’expression « en ligne » désigne tout objet ou ressource directement accessible via l’Internet.

**ENISA  - *European Network for Information Security Agency***

Agence européenne de cybersécurité\*, l’ENISA a été créée, le 10 mars 2004, par le Règlement CE n°460/2004 du Parlement Européen. L’agence est ainsi chargée de la sécurité des réseaux et de l’information. Sa mission est d'assurer un niveau élevé de sécurité des réseaux et de l'information. Elle agit de différentes façons:

* en intervenant en tant qu'expert en matière de sécurité des réseaux et de l'information auprès des autorités nationales  et des institutions européennes;
* en favorisant l’échange de meilleures pratiques;
* en facilitant les contacts entre les institutions (nationales et européennes) et les entreprises.

L'ENISA, en collaboration avec les instances nationales et les institutions européennes, s’emploie à développer une culture de la sécurité des réseaux d'information dans toute l'Union[[102]](#footnote-103).

**Enregistreur de frappe**

*(Keystroke Logger - Keylogger)*

Composant matériel ou Logiciel qui permet d’enregistrer les frappes clavier à l’insu de l’utilisateur. Les informations sont stockées puis transmise en vue d’une utilisation ultérieure (surveillance ou vol d’informations personnelles). Très simple d’utilisation, ils peuvent être utilisés dans un cadre familial (pour surveiller les activités de ses enfants ou de son conjoint) ou dans un cadre professionnel (la CNIL a toutefois rappelé, dans une note du 20 mars 2013, que l’emploi de *keylogger* est interdit pour surveiller des employés[[103]](#footnote-104)). Des logiciels sont pourtant aisément disponibles pour quelques dizaines d’euros.

**Entrepôt de données**

*(Data warehouse)*

Ensemble de données collectées dans une entreprise ou un organisme pour être exploitées par des outils d’aide à la décision[[104]](#footnote-105).

**E-réputation**

*(E-reputation)*

L’e-réputation est une notion utilisée pour qualifier la notoriété d’un individu, d’une entreprise ou d’une administration sur Internet. L’e-réputation fait aujourd’hui l’objet d’une véritable attention car l’image d’une structure peut être durablement dégradée par des propos négatifs diffusés sur les réseaux sociaux où dans les commentaires clients.

**Erlang**

*(Erlang)*

Il existe plusieurs usages pour le terme Erlang. En premier lieu il est le patronyme de Agner Krarup Erlang (1878-1929), mathématicien danois qui a notamment travaillé sur la théorie des files d’attente et la modélisation des réseaux téléphoniques. Cherchant à réduire les coûts d’exploitation et à optimiser le dimensionnement des réseaux en fonction du nombre d’appel, il élabore un modèle statistique et une loi de probabilité : la distribution d’Erlang. Ce modèle s’appuie sur la loi des évènements rares. Ainsi, en référence au chercheur, l’Erlang est l’unité de mesure (sans dimension) utilisée en téléphonie pour indiquer la charge d’un équipement. Par charge il faut ici comprendre « taux d’occupation de l’équipement durant une période considérée ». Un Erlang (E) correspond donc au fait qu’un équipement est occupé durant la période d’observation (typiquement un appel téléphonique).

Enfin, l’Erlang est également un langage de programmation créé par Ericsson (dont il tire son nom *ERicsson LANguage*).

**ESN – Entreprise de Service du Numérique**

L’acronyme désigne aujourd’hui les SSII\* (Société de Service en Ingénierie Informatique). Elles offrent des services d’externalisation informatique à leurs clients. Ainsi, une ESN assure généralement des fonctions de conseil, d’intégration de systèmes, d’infogérance, voire de formation. Elle accompagne ainsi les projets informatiques d’un client et en assure la maîtrise d’œuvre.

**ESSID - *Extended Service Set Identifier***

L’ESSID est l’identifiant de 32 caractères (maximum) permettant d’identifier un réseau Wi-Fi. C’est ainsi le nom qui apparaît sur votre terminal lors de la connexion au réseau.

**État de l’art**

*(State of the art)*

Ensemble des bonnes pratiques, des technologies et des documents de référence relatifs à la sécurité des systèmes d’information publiquement accessibles à un instant donné, et des informations qui en découlent de manière évidente. Ces documents peuvent être mis en ligne sur Internet par la communauté de la sécurité des systèmes d’information, diffusés par des organismes de référence ou encore d’origine réglementaire[[105]](#footnote-106).

**Ethernet**

Ethernet est un standard de communication sur un réseau local\*. Conçu par Xerox et DE CET Intel, il est normalisé par l’IEEE 802.3 et connaît de nombreuses variantes. Le principe général veut que les machines d’un réseau Ethernet soient reliées entre elles par une même ligne de communication (câble physique). La nature du câble a une influence directe sur le débit disponible. L’Ethernet classique fonctionne à 10Mbps (câble coaxial ou paire torsadée) mais il se décline également à 100Mbps (double paires torsadée ou fibre optique). L’accès se fait à l’aide d’un protocole à contention avec détection de collisions (CSMA/CD - *Carrier Sense Multiple Acces with Collision Detection)*.Chaque machine vérifie que la ligne de communication est libre avant d’émettre (lorsque deux machines émettent simultanément, il y a collision). Les paquets sont de taille limitée et il existe un temps d’attente entre deux émissions (pour vérifier la disponibilité de la ligne). Dans cette version il y a donc partage de la bande passante\*, une évolution dite « Ethernet commuté » permet de contourner cette contrainte. L’Ethernet commuté s’appuie sur un équipement réseau particulier, le commutateur\* (*switch*). Celui-ci filtre les communications, dresse une liste de correspondance entre les adresses des machi-  
nes connectées et les ports\* utilisés et ne transmet les messages que sur le port nécessaire.

***Ethical hacking***

(Hacking éthique)

Terme qui désigne l’usage ou l’apprentissage des techniques d’attaque afin de mieux contribuer à la sécurité d’un système. Ainsi, l’*éthical hacking* vise-t-il à fournir aux spécialistes de la sécurité informatique une bonne connaissance des techniques et outils utilisés par les attaquants.

Voir Chapeau blanc - *White hat.*

**Étiquette du Net, nétiquette**   
*(Netiquette)*

Ensemble de règles informelles de savoir-vivre en ligne.

**ETCD - Equipement de Terminaison de Circuits de Données**

*(DCE – Data Communication Equipement)*

Un ETCD ou DCE en anglais (*Data Communication Equipement)* est, en télécommunication, un équipement qui permet d’adapter les signaux binaires des terminaux ETTD\* aux caractéristiques des lignes de communication.

Voir ETTD.

**ETSI - *European Telecommunications Standard Institute***

L’ETSI est l’organisme de normalisation des télécommunications en Europe. Il est ainsi principalement en charge de la production de normes et standards\* pour les télécommunications au sein des pays européens. Basé en France, à Sophia Antipolis, l’ETSI coopère notamment avec le Comité Européen de Normalisation (CEN) lui-même membre de l’organisation internationale de normalisation (ISO\*). Réunissant près de 55 pays ainsi que des centres de recherche, des industriels, des fournisseurs d’accès et des opérateurs, l’ETSI est à l’origine de plusieurs normes qui ont ensuite été déployées au-delà des frontières européennes. Ainsi, la norme GSM\*, pour la bande des 900 Mhz, ou encore l’UMTS, pour la téléphonie cellulaire haut débit, ont été normalisées par l’ETSI. Enfin, l’organisme produit quantité de standards, recommandations et spécifications[[106]](#footnote-107).

**ETTD - Equipement Terminal de Traitement de Données**

*(DTE – Data Terminal Equipement)*

Un ETTD ou DTE en anglais (*Data Terminal Equipement*) désigne dans le vocabulaire des télécommunications un appareil capable de recevoir et/ou d'émettre des données sans connexion directe à la ligne de transmission\*. Ainsi, un ordinateur, une imprimante etc, sont des ETTD car ils ne se connectent pas directement à la ligne de communication (ligne téléphonique), ils doivent s’appuyer pour cela sur un autre équipement (modem, par exemple).

**Evanouissement**

*(Fading)*

En radiocommunication, l’évanouissement ou le *fading*, est une diminution momentanée de la puissance d’un signal radioélectrique à l’entrée d’un récepteur ; par extension, variation de la puissance du signal, due aux conditions de propagation des ondes[[107]](#footnote-108). Les causes de l’évanouissement peuvent être une dérive de l’oscillateur local (petites ondes et ondes courtes) ou une interférence destructrice entre l’onde directe et l’onde réfléchie par l’ionosphère (grandes ondes). Ce phénomène est aléatoire et varie dans le temps[[108]](#footnote-109).

**Evénement lié à la sécurité de l’information**

Au cœur de la sécurité des systèmes d’information, de la détection et du traitement d’incident, la notion d’événement lié à la sécurité de l’information se définit comme une occurrence identifiée de l’état d'un système, d'un service ou d'un réseau indiquant une faille possible dans la politique de sécurité de l’information ou un échec des mesures de sécurité ou encore une situation inconnue jusqu’alors et pouvant relever de la sécurité de l’information[[109]](#footnote-110).

**Exfiltration**  
*(Exfiltration)*

L’exfiltration est, lors d’une attaque informatique, l’action qui consiste à extraire d’un système cible des données ou des fichiers sans autorisation.

**Exploit**  
*(Exploit)*

Dans le domaine de l’attaque informatique, un exploit est la description d’une méthode permettant de contourner les barrières de sécurité sur un système en s’appuyant sur une vulnérabilité. Ainsi, pour chaque vulnérabilité logicielle connue, il est possible de trouver un « exploit » associé. Ces exploits sont des programmes qui peuvent être lancés sans connaissances particulières poussées. Le site <http://www.exploit-db.com/> propose une base de données très dense qui est couramment utilisée par les chercheurs et les auditeurs en sécurité.

**Exploitation**

*(Exploitation)*

Dans une séquence d’attaque informatique, l’exploitation est en général la dernière phase et elle consiste à conduire l’action prévue sur la cible. Cette action peut être une exfiltration\* de données ou autre.

Dans l’industrie, et donc pour les télécommunications, l’exploitation recouvre l’ensemble des activités nécessaires à la mise en œuvre d’une installation. Elle comprend donc

les phases d’installation, de commande et de contrôle, la surveillance et la maintenance[[110]](#footnote-111).

**Exposé**   
*(Outed)*

Ce dit lorsqu’une personne partage, via les réseaux sociaux, des données personnelles d’une autre.

L’expression peut également être utilisée pour qualifier un équipement qui serait accessible depuis l’Internet.

**Externalisation**

*(Outsourcing)*

Démarche qui consiste à confier à un tiers tout ou partie d’une activité jusqu’alors réalisée en interne[[111]](#footnote-112).

**Extranet**

*(Extranet)*

Un Extranet est une extension d’un réseau intranet vers des organismes extérieurs privilégiés (clients, fournisseurs). Il permet d’accéder depuis l’extérieur, à certaines ressources de l’entreprise. L’accès se fait généralement à l’aide d’un portail sécurisé.

# F

**Faille**

*(Breach)*

Vulnérabilité\* dans un système informatique permettant à un attaquant de porter atteinte à son fonctionnement normal, à la confidentialité ou à l’intégrité des données qu’il contient[[112]](#footnote-113). Les failles de sécurité sont donc essentielles pour conduire des attaques informatiques. La recherche de vulnérabilité est permanente, que l’on cherche à attaquer ou à défendre un système.

**FAI - Fournisseur d’Accès à Internet**

*(Internet Service Provider - ISP)*

Le fournisseur d’accès à Internet (FAI) est un organisme offrant une connexion au réseau Internet. En France les principaux FAI sont également des opérateurs de télécommunications. Il existe également des FAI associatifs, qui se reconnaissent dans des valeurs de neutralité du Net, de bénévolat et de solidarité[[113]](#footnote-114). L’acronyme anglais pour désigner ces entreprises est ISP (*Interne Service Provider*).

**Faisceau Hertzien**

Voir FH

**Fanion**

Voir Bannière (*flag)*

***Fast Ethernet***

Le *Fast Ethernet* désigne un réseau Ethernet\* 100 BASE TX à 100 Mbits.

Voir Ethernet.

***Fast Packet Switching* - FPS**

(Commutation de paquets rapide)

Le *fast packets switching* est une technique de communication qui cherche à pallier les limites de la commutation de paquets\*. Cette technologie améliore le débit en négligeant les en-têtes de correction d’erreur et de contrôle de flux (celles-ci sont traitées par des protocoles de couches supérieures). Les réseaux ATM\* et *Frame Relay*\* sont deux exemples de réseaux qui implémentent le FPS.

Voir *Frame Relay*, Mode de transfert asynchrone (ATM).

**FDM - *Frequency Division Multiplexing***

Voir Multiplexage en fréquence.

**FDMA - *Frequency Division Multiple Access***

Technique de multiplexage d’information utilisant la division de fréquence. Dans ce cas, la bande passante est divisée pour permettre à chaque utilisateur de disposer d’une partie du spectre. Ainsi, généralement un utilisateur (ou du moins l’équipement – téléphone) se voit attribuer une bande de fréquence pour la réception et une pour l’émission.

Voir Accès multiples.

**FEC - *Forwarding Equivalence Class***

Dans le standard MPLS\* le *Forwarding Equivalent Class* désigne un groupe de paquets IP\* acheminés et traités de la même manière. Les paquets d’une même classe reçoivent la même étiquette (label).

Voir MPLS\*

**FECN - *Forward Explicit Congestion Notification***

Dans un réseau *Frame Relay*\*, le FECN est un bit d’en-tête de trame\* transmis par l’émetteur (source) pour avertir le destinataire (client) de problèmes de congestion. Le destinataire doit donc limiter ou réduire le nombre de requêtes vers la source. Le BECN\*, *backward explicit congestion notification*, est le mécanisme inverse.

**Femtocell**

*(Home NodeB – Home eNodeB)*

En téléphonie mobile, dans un réseau de troisième génération (3G), une Femtocell désigne un équipement qui permet d’améliorer la couverture radio du réseau. Les boitiers peuvent ainsi être déployés chez des particuliers afin de permettre l’accès au réseau mobile 3G dans des zones peu ou pas couvertes (à l’intérieur des habitations par exemple). Les équipements existent pour les versions 3G (CDMA), 3,5G (HSDP / HSUPA).

**Fenêtre contextuelle -** **Fenêtre intruse**

*(Pop-up Window – Pop-up)*

Un *pop-up* est un message, le plus souvent non sollicité (généralement publicitaire), qui apparaît  à l'intérieur d'une autre fenêtre lors de la navigation Internet.

**FH- Faisceau Hertzien**

Un faisceau hertzien est un système de transmission radio utilisant une liaison à haute fréquence point à point (à vue directe). Une liaison FH peut donc transmettre de l’information en vue directe, elle est sensible aux masques (végétal, géographique etc.), elle transmet sur une seule porteuse harmonique un signal analogique\* ou numérique\*. La FH exploite des fréquences entre 1 GHz et 40 GHz, et utilise des antennes caractéristiques (en forme de disque) qui concentrent le signal. Les opérateurs télécoms utilisent des liaisons FH pour assurer le raccordement des sites radio avec les équipements de cœur de réseau mais il existe de multiples applications qui exploitent la ressource hertzienne (les armées, la télédiffusion, la radiotéléphonie).

**FHSS – *Frequency Hopping Spread Spectrum***

*(Etalement de spectre par saut de fréquence)*

La technologie d’étalement de spectre par saut de fréquence permet de transmettre un signal radio en utilisant plusieurs canaux\* d’une bande de fréquence. L’utilisation de ces canaux se fait en suivant une séquence de « sauts » pseudo-aléatoires partagée entre l’émetteur et le récepteur. Développé pour les besoins militaires (ce type de transmissions est plus difficiles à intercepter car le signal « saute » de fréquence suivant un schéma aléatoire), le FHSS est aujourd’hui présent dans les standards des réseaux locaux sans-fil (Wi-fi, 802.11). Dans ce contexte, le FHSS permet de réduire les interférences entre les différentes stations d’un même réseau car il permet de créer près de 79 canaux différents dans la bande de fréquence 2,4 – 2,4835 GHz.

**Fibre noire**

*(Dark Fiber)*

Fibre en réserve ou inactive.

**Fibre optique**

*(Optical Fiber)*

Fil (en verre ou plastique) qui a la propriété d’être un conducteur de la lumière. Le faisceau lumineux est confiné dans le cœur de la fibre optique en utilisant les propriétés de réfraction de la lumière. La fibre optique permet un débit d’information nettement supérieur aux câbles co-axiaux métalliques, elle est donc utilisée largement pour les liaisons intercontinentales par câbles sous-marins (l’absence de couplage et la faible atténuation du signal explique son utilisation dans ce type de liaisons). Il existe deux types de fibre optique qui se distinguent par le diamètre de leur cœur et la longueur d’onde utilisée. Ainsi, les fibres multimodes (*Multi Mode Fiber* - MMF) sont utilisées pour les trajets courts ou les faibles débits. Elles se caractérisent par un cœur de diamètre allant de quelques dizaines à une centaine de micromètres. Les plus performantes permettent un débit de l’ordre du Gbit/s sur environ 1000 m. A l’inverse les fibres monomodes (*Single Mode Fiber* - SMF) ont un diamètre de cœur très limité (inférieur à la dizaine de micromètres) ce qui permet un seul mode de propagation et limite les pertes (il n’y a pas de dispersion intermodale). Ce type de fibre est utilisé pour les câbles sous-marins.

**FIFO - *First in First out***

*(Premier en entrée, premier en sortie)*

Mode de gestion des files d’attente dans lequel les messages sont traités dans leur ordre d’arrivée dans la file. L’expression est également utilisée pour les méthodes de gestion des stocks en logistique ou encore en comptabilité analytique.

**Fichier exécutable**

*(Executable file)*

En informatique un exécutable désigne un fichier contenant un programme directement exécutable par la machine. Le fichier est reconnu par le système d’exploitation\* et lance un processus système puis l’exécution du programme. L’exécutable est donc à distinguer d’un fichier source\* qui doit être compilé avant de pouvoir être exécuté. Dans un système d’exploitation *Window*, les fichiers exécutables possèdent une extension en .exe. Pour autant, il existe d’autre forme de fichiers exécutables tel que les binaires\*, les *scripts\** (qui sont des fichiers texte) exécutés par un interpréteur.

Voir Code source.

**Filoutage**

*(Phishing)*

Voir également Hameçonnage.

**Filtrage**

*(Filter)*

Action qui permet de trier suivant des critères spécifiques le trafic pouvant être accepté ou refusé. Le filtrage opère sur certaines caractéristiques du trafic réseau (adresse source, destination, type de protocole).

Voir ACL, *White list.*

***Firewall***

(Pare-feu)

Egalement appelé pare-feu ou coupe-feu, le firewall est un système qui permet de protéger un ordinateur ou un réseau d’ordinateurs des intrusions originaires d’un réseau tiers. Le *firewall* agit comme une passerelle filtrante entre deux systèmes. Il analyse les paquets de données échangés et détermine les autorisations d’accès en fonction d’une politique fixée.

***FireWire***

*FireWire* est un protocole de transmission de données (IEEE 1394) à haut débit (400 Mbits/s – 800 Mbits/s). Il peut assurer l’interface pour les périphériques vidéo, audio mais également disques durs externes.

***Firmware***

(Micrologiciel – logiciel embarqué)

Un *firmware* est un logiciel qui permet le contrôle d’un équipement et qui est directement fourni par le constructeur. Ce logiciel est en général stocké dans la mémoire ROM\* de l’équipement. Un exemple de *firmware* est le *driver* d’un périphérique USB\* ou encore les programmes de gestion d’une console de jeu.

**Flame**

Logiciel malveillant détecté par le laboratoire d’Eugène Kaspersky le 28 mai 2012. Stuxnet étant encore dans tous les esprits, la comparaison est immédiate, Flame serait ainsi « vingt fois plus puissant que Stuxnet [[114]](#footnote-115)». La découverte de cet outil résulte en fait d’une recherche liée à *Wiper* (un autre programme malveillant). Peu après sa découverte au mois d’avril, plusieurs pays du Moyen-Orient dont les installations pétrolières avaient été touchées sollicitent l’intervention de l’Union Internationale des Télécommunications (UIT), agence des Nations Unies. L’UIT mandate alors le laboratoire Kaspersky pour conduire une investigation numérique. Détecté au mois de mai 2012, ce cheval de Troie collecte des informations issues d’ordinateurs infectés de par le monde. L’attaque semble principalement viser le Moyen-Orient (des ordinateurs infectés ont été découverts en Iran, Israël, Syrie, Liban). Kaspersky ainsi que le laboratoire hongrois CrySys débutent alors les travaux qui aboutiront à la découverte de Flame. Beaucoup plus volumineux que Stuxnet\*, Flame se révèle être une sorte de « couteau suisse » de l’espionnage numérique. Il est ainsi capable de collecter des données, de procéder à des enregistrements audios et vidéos, des captures d’écran, d’enregistrer les frappes clavier, le trafic réseau, de lire les courriers électroniques. Il disposait en outre d’une fonction permettant de corrompre des appareils dans le voisinage d’une station infectée par l’activation du système *Bluetooth*. Enfin, Flame est capable d’effacer la totalité des informations sur un disque dur. Espionnage donc, mais également sabotage. Les objectifs de l’attaque demeurent encore mal connus, il semble que le virus cherche essentiellement des fichiers AutoCAD, logiciel utilisé pour réaliser des plans et dessins industriels, des documents au format PDF ainsi que des fichiers texte. Le *malware\** semble actif depuis au moins 2007, soit 5 ans avant sa découverte. Le 6 juin 2012, moins d’un mois après la première détection « accidentelle » du virus, l’entreprise Symantec confirme avoir intercepté une commande particulière entre un serveur de commande et de contrôle (C&C) du virus et un système compromis. Cette commande (browse32.ocx) avait pour but d’effacer toute trace et toute preuve potentielle de l’existence du virus au sein du système cible. Un ordre d’autodestruction après nettoyage en quelque sorte.

Comme Stuxnet\* et Duqu\*, Flame est associé à l’opération *Olympic Games* visant à réduire le potentiel nucléaire iranien. Ils feraient ainsi parti d’une vaste campagne de cyber-sabotage (la première du genre) soutenue par des actions d’espionnage numérique de longue haleine.

**FM** – ***Frequency Modulation***

(Modulation de fréquence)

La modulation de fréquence est un mode de modulation utilisé pour transmettre un signal. Dans ce cadre, on utilise une porteuse (signal sinusoïdal) dont on va moduler la fréquence pour transmettre le signal. L’autre type de modulation consiste à moduler l’amplitude du signal on parle alors de modulation d’amplitude (AM).

***Follower***

(Suiveur)

Désigne la personne qui s’abonne au compte Twitter d’une autre. Cette action permet de voir apparaître sur son « fil » (flux d’actualité) personnel, les *tweet* de la personne suivie.

**Fonction de sécurité**

Une fonction de sécurité est une fonction à mettre en œuvre pour atteindre les objectifs de sécurité. Elles sont matérialisées par le choix de moyens et de mesures de nature technique et organisationnelle[[115]](#footnote-116).

**Fonction de hachage**

*(Hash function – One-way hash function)*

Le hachage est une opération qui consiste à déterminer une information de taille fixe et réduite à partir d’une donnée de taille indifférente, de telle façon que deux données quelconques aient une faible probabilité de produire le même résultat[[116]](#footnote-117). Une fonction de hachage produit donc un condensé (empreinte) quasi unique d’un document. La fonction de hachage doit satisfaire deux propriétés mathématiques :

* être à sens unique : il est difficile pour une image de la fonction donnée de calculer un antécédent associé ;
* être « sans collision » : il est difficile de trouver deux antécédents différents de la fonction ayant la même image.

Ce condensé (l’image par la fonction) permet d’identifier de façon certaine le document qui lui est rattaché mais il ne permet pas de le reconstituer. Le hachage est utilisé pour vérifier l’intégrité d’un document (si le hachage d’arrivée correspond au hachage de départ, la donnée n’a pas été corrompue) et indirectement son authenticité. Des fonctions de hachage sont utilisées pour les mécanismes de signature électronique\*. Il existe plusieurs fonctions de hachage qui produisent des empreintes (ou condensés) de taille différente. Les plus courantes sont : MD 4 et MD5\*, SHA\* 1, SHA 2 et RIPEMD-160.

Voir MD5, SHA.

**Forensique**

*(Forensic)*

Le forensique regroupe l’ensemble des techniques d’analyse des traces d’une attaque qui contribuent à l’identification de l’auteur. Ainsi, en sécurité des systèmes d’information, le forensic regroupe la retro ingénierie, l’analyse des *logs*\*, l’analyse des traces réseau, etc. Le terme est plus généralement utilisé en criminologie pour désigner les apports de la science dans les affaires judiciaires.

Voir Preuve numérique, *Log*.

**Format**

*(Format)*

En informatique, un format désigne un agencement structuré d’un support de données mais également la disposition des données elles-mêmes[[117]](#footnote-118). On distinguera ainsi les formats de données des formats de fichiers.

Voir XML.

**Forme**

*(Pattern)*

Ensemble de caractéristiques retenues pour représenter une entité en fonction du problème à résoudre. Cette entité peut être une figure géométrique, une image, un son, un signal, un texte, etc[[118]](#footnote-119).

**Forum**

*(Fora - Newsgroup)*

Un forum est un service qui permet des discussions et des échanges sur un thème donné. Les utilisateurs inscrits peuvent alors participer à des fils de discussions orientées vers des questions spécifiques.

**Fournisseur d’accès**

*(Access provider)*

Organisme offrant à des clients d’accéder à l’internet, ou, plus généralement, à tout réseau de communication. Le fournisseur d’accès peut aussi offrir des services en ligne[[119]](#footnote-120).

Voir FAI.

***Frame Relay***

(Relai de trame)

Frame Relay est un protocole réseau de niveau 2 du modèle OSI\* (couche liaison de données) qui assure la transmission de trames\* de données avec un débit entre 64Kbits/s et 40 Mbits/s. Le protocole a été développé pour les liaisons WAN\* entre sites, il est plus économique car permet de mutualiser les liaisons au lieu de disposer de liaisons dédiées pour chaque client. Il offre ainsi de la bande passante « à la demande » grâce à un multiplexage statistique. Son fonctionnement s’appuie sur des équipements réseau spécifiques :

• Le DTE\* (*Data terminal equipment)* équivalent d’un routeur ;

• Le DCE\* *(Data circuit terminating equipment)*.

***Framework***

(Cadre d’application – socle d’application – cadriciel)

Le terme *framework* désigne un ensemble d’outils logiciels organisés qui forment l’architecture d’un programme. Il se compose donc d’une bibliothèque logicielle mais également d’une architecture qui permet aux développeurs (programmeurs) de capitaliser leurs travaux. Le *framework* permet la réutilisation de codes et l’adaptation aux différents besoins client par la création d’architectures spécifiques, il est donc faiblement spécialisé.

On trouve ainsi des *framework* d’intégration *middleware\** qui permettent de rassembler des applications diverses sous une interface unique. Largement utilisés par les ingénieurs, les *framework* assurent ainsi des gains de productivité conséquents.

***Freeware***

(Gratuiciel)

Voir Gratuiciel\*.

**Fréquence**

*(Frequency)*

La fréquence d’un phénomène périodique correspond au nombre de fois que ce phénomène se produit durant un laps de temps donné. Dans le cas d’une onde électromagnétique, la fréquence correspond donc au nombre d’oscillations par seconde. Elle s’exprime en Hertz.

**Fréquence d'Echantillonnage**

*(Sampling Frequency)*

La fréquence d’échantillonnage correspond au nombre d’échantillons d’un signal prélevé par unité de temps. Cette notion est essentielle pour le traitement numérique de la voix ou de la musique. En effet, le microphone transforme l’onde acoustique de la voix en signal analogique qu’il faut alors échantillonner pour assurer la transmission numérique. Une fréquence d’échantillonnage suffisante est essentielle pour ne pas perdre de l’information (théorème de Nyquist-Shannon).

Le théorème de Nyquist Shannon ou encore théorème de l’échantillonnage indique que pour assurer l’échantil­lon­nage d’un signal (donc pour pouvoir le représenter sous forme discrète), la fréquence d’échantillonnage doit être supérieure au double de la fréquence de ce signal.

Voir Shannon, Numérisation.

**FTP - *File Transfert Protocol***

(Protocole de transfert de fichiers)

FTP est un protocole, de niveau application du modèle OSI\*, qui permet le transfert de fichiers entre un client\* et un serveur\*. Il est donc l’un des plus vieux protocole de l’internet et a été développé pour faciliter les échanges de fichiers entre universités américaines dans les années 70. Le protocole, spécifié par la RFC\* 959, s’appuie sur une connexion TCP\* et sur la suite protocolaire TCP/IP\* pour assurer le transport des fichiers sur le réseau. Par convention FTP utilise les ports\* 20 pour les données et 21 pour les commandes. La version qui utilise le protocole sécurisé SSL\* est appelée FTPS et utilise le port 990.

**Fuite d’information**

*(leak)*

L’expression peut être utilisée dans plusieurs contextes. De façon conventionnelle, une fuite d’information (un *leak*) est une révélation publique de documents à caractère confidentiel. L’expression a été popularisée par le site *wikileaks*\* qui a été rendu célèbre par la mise en ligne de télégrammes diplomatiques américains confidentiels au mois de novembre 2010 puis au court de l’année 2011.

Dans le domaine informatique, on parle de systèmes ou d’applications qui laissent fuiter l’information. L’expression traduit ainsi un défaut de sécurité qui peut être exploité pour recueillir des données confidentielles ou normalement non publiques. La fuite d’information est ainsi le mécanisme de diffusion d’une information de façon non désirée.

***Full-duplex***

(Bidirectionnel simultané)

Le *Full-duplex* est un mode de transmission dans lequel les informations transitent simultanément dans les deux sens sur un même canal de communication.

Voir Duplex.

# G

**Gain**

*(Gain)*

En télécommunication, le gain fait partie des paramètres fondamentaux d’une antenne (avec l’impédance, la puissance maximale admissible, la bande de fréquence de fonctionnement et le diagramme de rayonnement). Le gain et le diagramme de rayonnement permettent de définir la manière dont l’antenne rayonne. Classiquement on caractérise une antenne en comparant son rayonnement à celui d’une antenne isotrope idéale. La différence entre la puissance maximale rayonnée et celle de l’antenne isotrope de référence est appelée « gain » (gain de l’antenne, gain d’antenne)[[120]](#footnote-121). Le gain est exprimé en décibel (dB) l’usage veut que l’on utilise la notation dBi pour isotrope.

***Gateway***

(Passerelle)

Une *gateway* est un équipement réseau qui permet de relier deux réseaux distincts sur le plan architectural ou protocolaire. Une passerelle applicative assure ainsi une interface entre protocoles différents. Une passerelle est par exemple nécessaire pour connecter un réseau local à Internet.

**Gestion des droits numériques – GDN**

*(Digital Rights Management – DRM)*

Mise en œuvre des différents procédés destinés à protéger les droits afférents à la diffusion de contenus sur supports numériques[[121]](#footnote-122).

**Gestionnaire de communauté**

*(Community manager)*

Profondément lié à l’émergence des réseaux sociaux et au Web participatif, le métier de gestionnaire de communauté est en évolution rapide et son périmètre est toujours en pleine mutation. De façon générale, un gestionnaire de communauté est en charge de l’animation des communautés virtuelles associées à une entreprise ou une entité. Cette animation consiste à fédérer la communauté autour d’un message positif, de valoriser l’entreprise en proposant des contenus adaptés et personnalisés. L’émergence de cette profession est liée à l’impact économique de la réputation en ligne (e-réputation\*) et des nouvelles interactions directes possibles par l’usage des outils numériques.

**Gratuiciel**  
*(Freeware)*

Logiciel\* distribué gratuitement sur lequel le programmeur conserve ses droits d'auteur. Le *freeware* est donc un logiciel propriétaire qui ne doit pas être confondu avec un logiciel libre pour lequel l’étude, la copie, la modification et la diffusion sont autorisées.

**GGSN - Gateway GPRS Support Node**

Au sein d’un réseau de télécommunication, le GGSN est un équipement qui assure la connexion entre le réseau GSM\* et d’autres types de réseaux comme l’Internet par exemple.

**Gigabit Ethernet**

Dans un réseau local câblé utilisant le protocole Ethernet\*, le Gigabit Ethernet est une famille de technologies qui permet un transfert de données pouvant atteindre plusieurs Gbit/s. Utilisant des fibres torsadées (cuivre) ou de la fibre optique, les différentes solutions sont standardisées par l’IEEE 802.3z (1000BASE-X), IEEE 802.3ba (pour les réseaux Ethernet 40 et 100 Gbit/s) et surtout IEEE 802.3ab. Cette dernière, dite 1000BASE-T permet le déploiement du Gigabit Ethernet sur des réseaux limités (longueur de câble maximale de 100 m).

**Gigue**

*(Jitter)*

Voir *Jitter*.

***Global Internet eXchange –* GIX**

Voir IXP.

**GMSC – *Gateway Mobile Switching Center***

(Centre de commutation mobile)

Dans un réseau GSM\*, le GMSC est une passerelle\* de commutation (à l’image du MSC\*) positionnée en bordure du réseau et qui assure l’interconnexion avec d’autres réseaux.

Voir GSM.

**GMSK – *Gaussian Minimum Shift Keying***

(Modulation à déplacement minimum gaussien)

Le GMSK est une technique de modulation numérique utilisée pour la transmission radio dans un réseau GSM\*.

***Google***

Société américaine créée en 1998 rendue célèbre par la création d’un moteur de recherche Internet. Outre son moteur de recherche l’entreprise a rapidement investi le champ des données et services en ligne. Avec près de 50 000 employés et une valorisation de 108 milliards de dollars en 2014, Google est l’une des plus importantes sociétés mondiale et fait partie des « *big four*» de l’Internet (Google, Apple, Facebook, Amazon). On parle également des « *big* *five* » en ajoutant *Twitter*.

Les nombreux services gratuits que propose l’entreprise sont très largement utilisés (blog, réseaux sociaux, partage en vidéos, stockage *cloud*…) ce qui fait de Google le premier dépositaire au monde de données personnelles (sur près de 900 000 serveurs). Les révélations des liens de ces grands groupes de l’Internet avec l’agence de renseignement américaine (NSA\*) ont contribué à une prise de conscience sans pour autant véritablement modifier les pratiques individuelles (Google est toujours le moteur de recherche utilisé par 95% des français).

***Google en chiffres (2014)***

L’usage du moteur de recherche :

Monde : 90,35%

Europe : 93,64%

France : 95,46%

Google indexe 30 milliards de milliards de pages Internet ;

Les robots de Google visitent 20 milliards de sites par jour ;

3,3 milliards de requêtes quotidiennes ;

Android\* : 900 millions de *smartphones* et tablettes équipées, 48% de part de marché en France ;

Google Play : 48 milliards d’applications installées via le market Google ;

Gmail : 425 millions d’utilisateurs ;

Google Maps : 200 pays cartographiés, dont 50 avec Street View ;

Aujourd’hui, 1 million de sites Web intègrent une carte Google Maps ;

Google Chrome : 750 millions d’utilisateurs actifs mensuels ;

Google Analytics : 15 millions de sites trackés ;

Google Wallet : 5 millions d’installations de l’application ;

Google Drive : 10 millions d’utilisateurs ;

53 861 employés à temps plein à travers le monde

source : <http://www.blogdumoderateur.com/chiffres-google/>

***Google Dorks***

Les *Google Dorks* sont des méthodes qui permettent d’utiliser un moteur de recherche (généralement Google, mais pas uniquement) dans les phases de reconnaissance de cible lors d’une attaque informatique. Ces requêtes spécifiques permettent de collecter des informations sensibles. Les informations sont alors accessibles via une requête particulière utilisant des opérateurs spécifiques. Ainsi est-il possible, par exemple, de chercher tous les documents au format pdf présents sur un site Web particulier en combinant la commande *site* et *file* dans la barre de recherche d’un navigateur :

site :example.com file:pdf

On utilise également la commande *intext* qui permet de rechercher une chaine de caractère dans le texte d’une page ou son code source. *Inurl* permet de retrouver de chaines de caractères dans un URL. Un site rassemble de nombreux exemples de Google Dorks : GHDB (*Google Hacking DataBase*) sur le site : http://www.exploit-db.com/google-dorks/

**GPRS - *Global Packet Radio System***

Le standard GPRS est une technique de commutation de paquets pour la téléphonie mobile. Evolution du GSM\* permettant la transmission de données avec un débit compris entre 40 kbit/s et 171 kbit/s. GPRS est généralement connu sous l’appellation 2,5G ou encore 2G+ il préfigure la norme *Edge* (à partir des années 2000).

**GPS - *Global Positioning System***

(Système de géolocalisation mondial)

Le système GPS est une technologie américaine permettant de localiser un récepteur (avec une précision sub-métrique dans certaines applications). Ce système repose sur une constellation de 24 satellites synchronisés (NAVSTAR) en orbite moyenne (20 200 km) qui diffusent un signal interprété par les récepteurs terrestres. Aujourd’hui largement utilisé dans tous les systèmes de navigation (aérien, maritime et terrestre) le GPS est également employé par les particuliers (GPS de voiture). La taille des récepteurs ne cesse de diminuer et ils sont aujourd’hui intégrés dans les montres ou les téléphones mobiles. Le système étant sous le contrôle des Etats-Unis, la dépendance stratégique qui en découle a conduit au développement de plusieurs autres infrastructures. Ainsi, du côté russe, le système *Glonass*, un temps tombé en désuétude, est de nouveau opérationnel et se présente comme une alternative au système américain. L’Europe pour sa part développe le système *Galiléo* en test depuis 2005. Les premiers satellites de la constellation ont été lancés en 2011 et le déploiement final est prévu en 2019 environ. On peut également noter les initiatives régionales de l’Inde et de la Chine qui cherchent à se doter de systèmes de géolocalisation par satellite géostationnaire ne couvrant qu’une partie du globe (projet *Beidou* et IRNSS)

**Gravité**

En sécurité informatique, la gravité d’un événement de sécurité mesure l'impact réel de l'événement en fonction de la criticité du bien (cas où un événement a une conséquence directe sur un bien) ou l'impact potentiel de cet événement sur le bien menacé en fonction du nombre de lignes de défense restantes et de la criticité de ce bien (cas ou l'événement n'a pas d'impact sur le bien mais sur ses moyens de défense) [[122]](#footnote-123).

**GRE - *Generic Routing Encapsulation***

(Routage Générique par encapsulation)

GRE est un protocole propriétaire développé par CISCO permettant d'encapsuler, dans des tunnels IP\*, des paquets\* qui utilisent de nombreux protocoles différents. GRE permet ainsi de créer un lien point à point virtuel via un réseau IP il est présenté dans plusieurs RFC\* 1701, 1702, 2784 et 2890. C’est un mécanisme d’encapsulation simple et extrêmement rependu. GRE est aujourd’hui spécifié également pour IP V6 par la RFC 7676.

**GSM - *Global System for Mobile communications***

(Système global de communication mobile)

Le GSM est une norme de téléphonie mobile qui s’est progressivement imposée au niveau mondial. En 1982, la Conférence Européenne des administrations des Postes et Télécommunications (CEPT) réunit un groupe de travail pour élaborer des normes pour les communications mobiles en Europe sur la bande de fréquence 890 à 915 MHz. La première expérimentation a lieu en 1991 et les spécifications couvrent également les systèmes fonctionnant sur la bande 1800 MHz et 1900 MHz (DCS 1800 et 1900). Le GSM est un réseau commuté, il y a donc une allocation de ressources pour la durée de la communication. Pour contourner les problèmes liés à ces allocations, la technologie introduit la notion de cellule\*. Il s’agit ainsi de diviser le territoire en petites zones entre lesquelles sont partagées les fréquences radio. Au sein de chaque cellule une station de base (BTS)\* à laquelle est associée un certain nombre de canaux de fréquence\*. Ces fréquences ne peuvent être utilisées par les cellules\* voisines afin d’éviter les interférences\*.

L’architecture d’un réseau GSM est divisée en trois sous-ensembles distincts :

• Le système radio avec la station mobile (le téléphone), la station de base (BTS) ainsi que le contrôleur de station de base (BSC\*), qui gère l’accès radio ;

• Le sous-système d’acheminement (ou réseau), ou *Network Switching Center Center* (NSS\*) ; Au sein de ce sous-système on trouve des équipements caractéristiques tels que le centre de commutation mobile (MSC\*) qui, relié au sous-système radio (via l’interface A) assure la commutation entre abonnés du réseau mobile et ceux du réseau commuté public (RTC) ou RNIS\*. Il participe également à la fourniture de services supplémentaires et à la mise à jour des bases de la HLR\* et de la VLR\*. Le cœur du sous-système réseau est l’enregistreur de localisation (*Home Location Record* HLR). La HLR est une base de donnée qui regroupe les principales informations relatives aux abonnés, la clé secrète partagée avec la carte SIM\* du mobile, la localisation de l’abonné et l’état du terminal ; On trouve également le centre d’authentification\* (AuC) qui permet à l’opérateur de s’assurer qu’un usager du réseau est légitime ; L’enregistreur des visiteurs (*Visitor Location Register* VLR) est une base de donnée qui contient des informations dynamiques liées à un MSC. Elle permet de communiquer vers le HLR les données de localisation lorsqu’un mobile se rattache au réseau ou entre dans la zone de couverture d’une cellule (cette action permet d’établir une communication) ; L’enregistreur des identités des équipements (EIR) est une base de données qui regroupe les identifiants des équipements. Chaque terminal peut changer de carte SIM (en fonction des opérateurs) en revanche, il reçoit un identifiant unique *(International Mobile Station Equipment Identity* IMEI) ;

• Le sous-ensemble d’exploitation regroupe les activités liées à la gestion du réseau tant sur un plan commercial que technique.

Le GSM est dit de deuxième génération, il préfigure les systèmes de troisième génération (UMTS\*) qui permettent des débits plus importants nécessaires pour les flux de données.

# H

1. **Hack**
2. Un « hack » désigne une méthode, ou une technique originale qui repose sur le détournement d’un objet de son usage principal afin de résoudre un problème. Il peut s’agir également d’une méthode ou un ensemble de techniques utilisées pour obtenir un accès non autorisé et non coopératif à un réseau ou un système d’information. Un *hack* sanctionne alors la démonstration effective du contournement des barrières mises en place pour garantir la sécurité et l’intégrité d’un système.
3. **Hacker**
4. De façon triviale, un « hacker » désigne la personne qui réalise un hack\*, un exploit technique. Le mot est sujet à de nombreuses controverses, improprement traduit, en français, pas le terme « pirate », la figure du hacker a ainsi très tôt été associée à l’action criminelle et illégale. Toutefois, une autre interprétation du terme se rapproche de son origine (les courants de la contre culture américaine des années 60) et contribue à donner une image plus acceptable du terme. Il est d’ailleurs intéressant de noter que le mot n’est que rarement utilisé par les intéressés eux-mêmes, ainsi un spécialiste de la sécurité informatique ou un informaticien chevronné ne se présentera quasiment jamais en utilisant le terme de *hacker*. Une interprétation plus large du mot désigne une personne qui cherche à comprendre et maitriser une technologie. Il existe une typologie des *hackers*, établie en fonction de leur motivation ou de leur niveau technique. On trouve ainsi les *white hats* (animés d’intentions positivies et cherchant à améliorer la sécurité d’un produit) auxquels on oppose les *black hats\**. Le terme *skripkiddies* désigne des personnes qui se contentent d’utiliser des outils d’attaque informatique sans en maitriser totalement le fonctionnement. Enfin on évoque également les *newbie* ou *n00b* termes qui désignent les débutants dans le domaine du hack\*.
5. **Hachage**
6. *(Hash code)*
7. Voir Fonction de hachage.
8. **HADOPI - Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet**.
9. La Loi Création et Internet (loi n°2009-669 du 12 juin 2009, complétée par la loi n°2009-1311 du 28 octobre 2009) instaure en France une haute autorité (HADOPI), organisme indépendant de régulation, dont la mission est la diffusion des œuvres et la protection des droits sur Internet. La loi vise essentiellement à lutter contre le téléchargement illégal de productions soumises au droit d’auteurs. Cette forme de téléchargement a d’ailleurs été improprement qualifiée de « piratage » contribuant en France à ternir l’image du *hacker*\*, devenant *de facto* un criminel. Or, le hacker n’est pas toujours un pirate et l’internaute qui télécharge illégalement des films est lui-même rarement un hacker…
10. La mise en œuvre de la HADOPI a été l’occasion de débats et a suscité de vives oppositions au sein de la communauté des internautes. La loi ne sanctionne en effet pas directement le fait de partager des œuvres soumises au droit ‘auteur mais la négligence caractérisé de l’internaute qui ne sécurise pas son accès à internet et rend possible le téléchargement illégal. C’est ce volet de la loi qui est le plus critiqué. « La réponse graduée » pouvait aller jusqu’à la suppression de l’accès à Internet, cette mesure n’est plus possible depuis 2013 et le contrevenant s’expose aujourd’hui à des amendes allant jusqu’à 1500 Euros. Outre cette mission de protection des œuvres sur Internet, La HADOPI doit également encourager le développement de l’offre légale (label PUR), réguler les DRM\* et labéliser des moyens de sécurisation des accés Internet pour les usagers.
11. ***Half-Duplex***
12. (Bidirectionnel non simultané – Alternat)
13. Le *half-duplex* désigne un mode de communication où l’information peut circuler sur un même canal dans un sens comme dans l’autre de façon alternée.
14. Voir *Duplex*, *Full duplex.*
15. **Hameçonnage**
16. *(Phishing)*
17. Le hameçonnage désigne une technique qui vise à se procurer les informations personnelles d’un groupe d’individu ou d’une organisation. Classiquement il s’agit, par l’intermédiaire d’un mail frauduleux, d’amener la victime à communiquer ses identifiants personnels de connexion (par exemple bancaires). Ces données permettent ainsi à l’attaquant d’usurper l’identité de la victime sans avoir recours à des techniques de *hacking* complexes. La même technique peut être utilisée avec des messages textes (SMS\*) on parle alors de *smishing*.
18. **Hameçonnage ciblé**
19. *(Spearphishing)*
20. Technique d’attaque qui utilise l’hameçonnage\* contre un nombre limité de victimes. Le *spearphishing* est utilisé dans les attaques à fin d’espionnage (APT\*). On parle également d’harponnage.
21. **Pour aller plus loin**
22. Dans sa présentation des principales menaces, l’ANSSI décrit l’hameçonnage ciblé comme une attaque qui repose généralement sur une usurpation de l’identité de l’expéditeur, et qui procède par ingénierie sociale\* forte afin de lier l’objet du courriel et le corps du message à l’activité de la personne ou de l’organisation ciblée.
23. Généralement, le courriel usurpe l’identité d’une personne morale (établissement financier, service public, concurrent) ou d’une personne physique (collègue de travail, famille, ami…) dans le but de duper le destinataire qu’il invite à ouvrir une pièce jointe malveillante ou à suivre un lien vers un site Web malveillant. Une fois cette première machine contaminée, l’attaquant en prend le contrôle pour manœuvrer au sein du système d’information de l’organisation constituant la véritable cible (on parle ici « d’infiltration »).
24. Une fois sa première victime compromise, l’attaquant cherchera à obtenir des droits « d’administrateur » (on parle alors « d’escalade de privilèges ») pour pouvoir rebondir et s’implanter sur les postes de travail et les serveurs de l’organisation où sont stockées les informations convoitées. Cette manœuvre est également appelée « propagation latérale ». Une fois ses cibles atteintes, il recherchera les informations qu’il s’efforcera de capter le plus discrètement possible (on parle alors ici « d’exfiltration ») soit en une seule fois, en profitant d’une période de moindre surveillance du système (la nuit, durant les vacances scolaires, lors d’un pont…), soit de manière progressive plus insidieuse. Il prend généralement soin de toujours effacer derrière lui toute trace de son activité malveillante[[123]](#footnote-124).
25. ***Handover***
26. (Transfert inter-cellulaire)
27. En téléphonie mobile, le *handover* désigne un mécanisme qui permet à un mobile de transférer sa connexion d’une station de base vers une autre ou, au sein de la même station d’un canal radio vers un autre. Le *handover* permet donc à un mobile de changer de cellule de rattachement sans rupture de la communication.
28. **Harponnage**
29. *(Spear Phishing)*
30. Voir Hameçonnage ciblé.
31. ***Hash***
32. (Empreinte)
33. Un *hash* est l’empreinte issue de la fonction de hachage.
34. Voir fonction de hachage.
35. ***Hashtag - #***
36. (Mot dièse)
37. Un *hashtag* désigne un mot clé qui permet de marquer un contenu échangé sur un réseau social. L’utilisation de ce marqueur a été popularisée par *Twitter*. Son origine remonte au langage C ou un mot clé désigné par # fait l’objet d’un traitement spécifique. L’usage a ensuite été repris sur les canaux de communication IRC\* avant de servir de marqueur principal sur *Twitter*. L’usage du *hastag* a été introduit par les utilisateurs de *Twitter* et non par ses concepteurs.
38. **HD - Haut Débit**
39. Dans les technologies numériques, le haut débit désigne un accès dont le débit est typiquement supérieur à celui d’un modem 56k (soit 56ko/s). Les technologies Wi-Fi\*, WiMax\*, ADSL\*et ADSL2 sont ainsi qualifiées de liens HD car elles permettent des débits entre 11 et 75Mbit/s. Les génération suivantes, notamment les réseaux de fibres optiques supportent des débit supérieur (100Mbits/s) et sont qualifiées de THD (très haut débit).
40. **HDLC - *High Level Data Link Control***
41. *(Commande de liaison de données à haut niveau)*
42. Protocole de liaison normalisé[[124]](#footnote-125) de niveau 2 du modèle OSI\* (couche liaison de données) qui utilise le mode connecté\*. Il permet d’assurer le contrôle de la liaison et un transfert de données fiable entre deux équipements distincts. Ce protocole était très utilisé dans les réseaux X25\* ou RNIS\*.
43. ***Heartbeat***
44. (Balisage)
45. Synonyme de *Beaconing.*
46. Voir Balisage.
47. **Heuristique**
48. *(Heuristics)*
49. Méthode de résolution de problèmes non fondée sur un modèle formel et qui n’aboutit pas nécessairement à une solution[[125]](#footnote-126).
50. Dans le contexte de la sécurité informatique, l’analyse heuristique est utilisée pour la détection de nouveaux programmes malveillants. Dans ce contexte, un « module d’analyse heuristique » permet d’émuler l’exécution d’une application et d’analyser les comportements suspects (ouverture et écriture de fichiers par exemple). Cette méthode permet de signaler des fichiers potentiellement infectés par un virus dont la signature n’est pas connue (et qui est donc indétectable sur la base d’une analyse statique).
51. Voir également IDS.
52. **HIPS – *Host-based Intrusion Prevention System***
53. Un HIPS est un système de prévention d’intrusion qui s’attache à la protection d’un hôte\* (équipement terminal, ordinateur) en détectant et neutralisant les processus malveillants. Un antivirus est une forme d’HIPS.
54. Voir IPS, IDS.
55. **HLR - *Home Location Register***
56. La HLR est la base de données centrale d’un réseau de téléphonie mobile. Elle contient l’ensemble des informations abonnés tels que IMSI\*, numéro de téléphone MSISDN\*, les services optionnels souscrits et l’ensemble des données permettant la facturation. Cette base contient en outre les données de localisation (qui transitent via les VLR\*).
57. Voir GSM.
58. ***Hoax***
59. (Faux - canular)
60. Information vraie ou fausse, souvent transmise par messagerie électronique ou dans un forum, et incitant les destinataires à effectuer des opérations ou à prendre des initiatives, souvent dommageables.
61. Remarques : Il peut s’agir d’une fausse alerte aux virus, de chaîne de solidarité, pétition, promesse de cadeaux, etc. Quelques canulars fréquents sont répertoriés sur des sites dédiés comme « *Hoaxbuster*» ou « *Hoaxkiller*».[[126]](#footnote-127)
62. **Homologation de sécurité**
63. Processus d’information et de responsabilisation qui aboutit à une décision, prise par le responsable de l’organisation. Cette décision constitue un acte formel par lequel il atteste de sa connaissance du système d’information et des mesures de sécurité (techniques, organisationnelles ou juridiques) mises en œuvre et il accepte les risques qui demeurent, qu’on appelle risques résiduels[[127]](#footnote-128).
64. ***Honey Pot***
65. (Pot de miel)
66. En sécurité informatique un *honeypot* est une méthode de défense qui consiste à leurrer l’attaquant en l’attirant vers une réplique de sa cible. Cette technique permet d’observer l’attaquant, ses outils et méthodes sans rentrer en conflit avec les systèmes en production.
67. ***Honey words***
68. *(*Leurre de mots de passe*)*
69. Les *Honeywords* sont des faux mots de passe destinés à détecter une tentative d’intrusion. Ces faux mots de passe sont stockés dans le même fichier que les véritables dans un espace normalement protégé. Si un pirate vole l’ensemble du fichier, il lui est impossible de discerner les vrais mots de passe des faux. Il faudra donc que l’attaquant teste ces mots. Dans ce cas, une alerte est paramétrée et détecte la tentative d’intrusion. Cette technologie est encore relativement jeune et ne change rien pour les utilisateurs légitimes. Par ailleurs elle ne protège pas contre une intrusion mais permet une remontée d’alerte plus rapide et donc un traitement de l’attaque plus efficace.
70. ***Hot Spot***
71. (Borne WiFi publique)
72. Un *hot spot* est un point de connexion WiFi\* déployé dans un lieu public. Les opérateurs déploient ce type de borne afin de permettre à leurs clients de se connecter en WiFi dans des zones plus vastes. Des mesures d’hygiène informatique doivent être prises lors de l’utilisation de ce type de connexion publiques (par exemple utilisation d’un VPN\*) car il est relativement aisé pour un pirate de recueillir passivement les données personnelles des utilisateurs en « écoutant le réseau ».
73. **Hôte**
74. (*Host)*
75. Le terme désigne un ordinateur relié à un réseau qui assure des fonctions de niveau applicatif.
76. ***Hosts (fichier)***
77. La plupart des systèmes d’exploitation utilisent le fichier *hosts* lors d’une connexion à l’Internet. Ce fichier associe des adresses IP\* à des noms de domaine ce qui évite d’effectuer systématiquement une requête DNS\*. A l’origine conçue comme une table d’équivalence embarquée dans chaque équipement, le fichier *hosts* ne peut aujourd’hui se substituer au DNS\* en raison de la taille des réseaux. Ainsi son utilisation demeure aujourd’hui limitée aux réseaux locaux\* de faible taille mais également pour assurer une fonction de filtrage des connexions Internet. Pour assurer cette fonction, il suffit, dans le fichier hosts d’attribuer une adresse locale (de type 0.0.0.0 ou 127.0.0.1) au site à filtrer. Dans ce cas, aucune page n’est renvoyée si l’on cherche à joindre le site. Ce système relativement simple de « re-direction » possible des requêtes d’un usager via la simple modification d’un fichier texte sur la machine hôte, pose des problèmes de sécurité et offre des opportunités pour des attaquants malveillants. Ainsi, en modifiant dans le fichier *hosts* l’adresse IP d’un site fréquenté régulièrement par la cible, il est possible de rediriger celle-ci vers un autre serveur contrôlé par l’attaquant. Pour se prémunir de ces pratiques il convient de protéger le fichier *hosts* en écriture.
78. **HSDPA - *High Speed Download Packet Access***
79. Dans l’évolution des normes et des débits de la téléphonie mobile, le HSDPA (3G+) correspond à une évolution de l’UMTS (3G) afin d’améliorer les débits en réception. Il est alors théoriquement possible d’atteindre des débits de 7,2 Mbit/s ou 14,4 Mbit/s contre environ 2 Mbit/s pour la 3G. Au niveau transmission, le HSDPA utilise le multiplexage par division de code large bande WCDMA\* - *Wideband Code Division Multiple Access*. Au niveau radio, l’amélioration consiste en l’ajout de nouveaux canaux de transport partagés : *High Speed Downlink Shared Chanel* - HS-DSCH. Sur le plan physique, la voie descendante est ainsi subdivisée en deux canaux, un pour le contrôle (signalisation\*) et un pour le transport des données.
80. **HSN – *Hopping Sequence Number***
81. Dans la norme GSM\*, le HSN est une classe de paramètres qui servent à configurer la séquence de porteuse dans le mécanisme de saut de fréquence.
82. **HSUPA – *High Speed Uplink Packet Access***
83. Alors que l’HSDPA améliorait le lien descendant de la norme UMTS (3G), HSUPA s’attache pour sa part au lien montant (entre le mobile et le réseau) et améliore sensiblement les débits. Ce dernier permet ainsi d’atteindre 5,8 Mb/s. HSUPA est décrit dans la 3GPP\* *release* *6*.
84. Voir HSPDA.
85. **HTML - *HyperText Markup Language***
86. Langage simple utilisé pour la mise en forme de documents hypertexte\* (pages Web). Largement utilisé, HTML utilise un système de balises qui indique au navigateur comment interpréter un document. HTML est progressivement supplanté par des outils plus performants comme xHTML\* ou encore XML\*. La version HTML 5 est d’ailleurs maintenant reconnue comme un véritable standard du Web par la W3C\* (*World Wide Web* *Consortium*) qui en a fait une « recommandation ».
87. **HTTP - *Hyper Text Transmission Protocol***
88. Protocole de la couche application du modèle OSI\*, HTTP repose généralement sur TCP\* au niveau transport. Le protocole permet la communication entre un client et un serveur en utilisant des méthodes (commandes) pour les requêtes spécifiques. Ainsi, pour obtenir une ressource particulière (une page Web par exemple) HTTP utilise la méthode GET à quoi le serveur répond par un POST.
89. Une version sécurisée du protocole, combine HTTP et un protocole de chiffrement (SSL/TLS\*). Cette version permet de vérifier l’identité du serveur sur lequel l’utilisateur se connecte ainsi que la confidentialité des échanges. HTTPS est ainsi très utilisé pour des sites de commerce en ligne ou dès que l’utilisateur doit fournir des informations personnelles ou bancaires.
90. Voir SHTTP\*.
91. **Hypertexte**
92. *(Hypertext)*
93. Système de renvois permettant de passer directement d’une partie d’un document à une autre, ou d’un document à d’autres documents choisis comme pertinent par l’auteur[[128]](#footnote-129).
94. Voir Ancre\*.
95. **Hypertrame**
96. Dans la norme GSM\*, le temps est divisé en segments, l’hypertrame est l’unité de temps la plus longue (3h 28mn 53s 760ms). L’hypertrame est composée de 2048 supertrames, qui rassemblent 1326 multi-trames.

# I

**IAB – *Internet Activities Board – Internet Architecture Board***

Créée en 1983, *l’Internet Activities Board*, est un comité en charge du suivi et du contrôle du développement des protocoles liés à l’Internet (typiquement ceux de la pile TCP/IP\*). Son fonctionnement est décrit dans la RFC\* 1120 (qui n’est pas un standard). Devenu *Internet Architecture Board\**, l’organisation se compose de deux comités distincts : *l’Internet Engineering Task Force* (IETF\*) et *Internet Research Task Force* (IRTF\*).

**IANA - *Internet Assigned Numbers Authority***

L’IANA est une fonction particulière de l’ICANN\* en charge de la cohérence de certains éléments clés pour le fonctionnement du réseau Internet. Il assure ainsi une partie de la gouvernance technique de l’Internet dans les trois domaines suivants :

• Noms de domaine : l’IANA supervise le DNS *Root*, les domaines .int et .arpa ;

• S’assure de la cohérence des adresses utilisées, des ressources en adresses IP\* et du suivi des AS\*, IANA transmet ces données aux *Regional Internet Registries* (RIR\*).

• Sur l’aspect protocolaire, IANA s’assure du respect des règles de nommage en liaison avec les organismes de standardisation.

Sur son site Internet, l’IANA présente sa mission comme suit :

L'IANA est responsable des aspects opérationnels de la coordination des identifiants uniques d'Internet et du maintien de la confiance de la communauté pour fournir ces services de manière impartiale, responsable et efficace[[129]](#footnote-130).

**ICANN - *Internet Corporation for Assigned Names and Numbers***

Selon la présentation officielle du site de l’ICANN[[130]](#footnote-131), l’Internet Corporation for Assigned Names and Numbers (ICANN) est une organisation de droit privé à but non lucratif. Son personnel et ses participants viennent du monde entier. Elle est chargée d’allouer l’espace des adresses de protocole Internet (IP), d’attribuer les identificateurs de protocole, de gérer le système de nom de domaine de premier niveau pour les codes génériques (gTLD) et les codes nationaux (ccTLD), et d’assurer les fonctions de gestion du système de serveurs racines. Ces services étaient initialement assurés dans le cadre d’un contrat avec le gouvernement fédéral américain par l’Internet Assigned Numbers Authority (IANA) et d’autres organismes. L’ICANN assume à présent les fonctions de l’IANA.

En tant que partenariat public-privé, l’ICANN a pour mission de *préserver la stabilité opérationnelle d’Internet*, de promouvoir la concurrence, d’assurer une représentation globale des communautés Internet, et d’élaborer une politique correspondant à sa mission suivant une démarche consensuelle ascendante.

L’ICANN est chargée de coordonner la gestion des éléments techniques du DNS\* pour assurer la « résolution universelle » (*universal resolvability*), de sorte que tous les internautes puissent trouver toutes les adresses valables. Pour ce faire, l’ICANN supervise la distribution des identificateurs techniques uniques utilisés dans les opérations Internet et l’affectation des noms de domaine de premier niveau (tels que .com, .info, etc.).

Les autres questions concernant les internautes, telles que les règles relatives aux transactions financières, le contrôle du contenu sur Internet, les messages électroniques à caractère commercial non sollicités (“*spam*”) et la protection des données n’entrent pas dans le cadre des responsabilités de coordination technique de l’ICANN.

**ICMP - *Internet Control and error Message Protocol***

Protocole de la suite TCP/IP\*, ICMP sert essentiellement à communiquer des messages d’erreur vers l’émetteur d’un message. Ainsi, lorsqu’un datagramme\* ne peut atteindre sa destination, un message ICMP est envoyé vers l’émetteur. ICMP est utilisé par tous les routeurs, il n’apporte pas de solutions aux problèmes mais permet simplement de les signaler.

**Identification**

*(Identification)*

L’identification permet à une identité de se faire reconnaître du système au moyen d’un élément dont on l’a doté. S’identifier consiste donc à communiquer une identité préalablement enregistrée[[131]](#footnote-132). Elle est suivie (généralement) d’une authentification\*.

L’identification est déclarative donc c’est une fonctionnalité, l’authentification inclut un mécanisme de vérification donc c’est une fonction de sécurité. Voir Authentification.

**IDoT – *Identity of things***

(Identité des objets)

Le concept d’IDoT est un corolaire de l’Internet des objets\* (IoT). Pour pouvoir communiquer entre eux, les objets connectés doivent pouvoir être identifiés et s’identifier entre eux (il est régulièrement également nécessaire de s’authentifier\*). En outre on doit pouvoir relier un objet à son propriétaire. Ainsi, l’IDoT regroupe les mécanismes d’affectation d’une identité à un objet communicant, sa gestion et sa sécurité. Cette problématique est donc au cœur du développement des objets connectés, dont le nombre, qui augmente exponentiellement, est sans commune mesure avec la population humaine par exemple.

**IDP – *Internet Datagram Protocol***

Protocole réseau qui fournit un service de transport de datagrammes\* non orienté connexion et non fiable. IDP est un des protocoles standard du *Xerox Network Specification* (XNS) développé à la fin des années 70 pour les réseaux locaux\*. IDP utilise un système d’adressage qui comprend l’adresse du réseau (sur 4 octets – assignée à chaque segment Ethernet\* du LAN\*) ainsi que l’adresse du nœud (codé sur 6 octets). Il n’y a pas de notion de sous-réseau. Novell développera son propre système basé sur le XNS en améliorant IDP et le renommant IPX\*.

Voir IPX, Netware.

**IDS - *Intrusion Detection System***

(Système de Détection d'Intrusion )

Un IDS est un système de sécurité en temps réel qui analyse les flux afin de détecter les intrusions ou les tentatives d’accès non autorisés. Il existe plusieurs types d’IDS en fonction de leurs spécialisations. On distingue ainsi les NIDS (*Network Intrusion Detection System*) qui assurent une surveillance au niveau réseau, les HIDS (*Host based IDS*) au niveau des hôtes\* ainsi que des systèmes hybrides qui assurent les deux fonctions. Le principe de fonctionnement repose sur la comparaison entre les données recueillies en temps réel (capture) et des signatures d’attaque\* ou un modèle de comportement « normal ». La base de l’IDS repose donc sur deux approches, l’une comportementale et l’autre dite par scénarios. Dans l’approche comportementale on cherche à déterminer, via des méthodes statistiques, si un utilisateur a un comportement conforme à ses habitudes. Cette approche permet ainsi de détecter des attaques non encore référencées ou connues. L’autre approche, plus statique, revient à rechercher dans les flux captés des « signatures » d’attaque.

Voir Heuristique.

**IEC - *International Electrotechnical Commission***

(Commission électrotechnique internationale)

Voir CEI.

**IEEE - *Institute of Electrical and Electronics Engineers***

(Institut des ingénieurs électriciens et électroniciens)

Organisation professionnelle de droit américain et à but non lucratif, l’IEEE a pour ambition de promouvoir la connaissance dans le domaine de l’électronique et de l’électricité. L’association regroupe environ 400 000 personnes dans le monde et est très active dans les questions de normalisation. Elle joue en effet un rôle moteur en fournissant une vaste base de données documentaire et se révèle être un forum de discussion incontournable. L’association a ainsi porté l’élaboration de plusieurs normes centrales pour les réseaux locaux (IEEE 802.3, Ethernet\*).

**IETF – *Internet Engineering Task Force***

Groupe de travail qui dépend de l’IAB\* dont la fonction est d’assurer la publication des *Request for Comments* (RFC\*), les standards techniques de l’Internet. L’IETF a un rôle central dans la proposition et la description de nouvelles procédures et protocoles.

Voir IAB.

**IGP - *Interior Gateway Protocol***

IGP regroupe l’ensemble des protocoles de routage\* à l’intérieur d’un même système autonome\* (AS).

Voir BGP, Routage.

**IHM - Interface homme machine**

Le terme IHM regroupe l’ensemble des matériels et logiciels qui permettent à un être humain d’interagir avec une machine. La qualité de l’IHM est primordiale pour assurer une productivité optimale et éviter le rejet de la machine par un opérateur humain.

**IMEI - *International Mobile station Equipment Identity***

Numéro unique qui identifie un terminal GSM\*. L’IMEI se présente sous la forme d’un nombre de 15 chiffres. Lié à l’équipement et non à l’abonné, cet identifiant permet à l’opérateur de désactiver un terminal volé par exemple.

Voir GSM, IMSI.

**Implémenter**

*(Implement)*

En informatique, implémenter consiste à effectuer l’ensemble des opérations qui permettent de définir un projet et de le réaliser, de l’analyse du besoin à l’installation et la mise en service du système ou du produit[[132]](#footnote-133).

**Imputation**

*(Charge)*

En télécommunication, l’imputation consiste à déterminer et enregistrer, pour une communication donnée, des éléments servant à calculer le prix à payer par chacun des clients. L’imputation est à distinguer de la facturation (*billing*) qui prend en compte la nature des abonnements souscrits, les forfaits et réductions particulières[[133]](#footnote-134).

L’imputation est également une fonction de sécurité permettant de lier une action à une identité (imputabilité). Cette fonction est indispensable pour rendre les individus responsables de leurs actes dans le cyberespace.

**IMS – *IP Multimédia Subsystem***

L’IMS est une technologie qui vise, dans les architectures de cœur de réseau télécom, à faire converger les systèmes classiques vers ceux issus du monde de l’IP\*. C’est une architecture dite « orientée service » car elle permet de passer du mode « circuit » vers un mode d’appel « session\* » en s’appuyant sur des protocoles de signalisation SIP\* mais également IP et RTP\*. IMS est standardisé par le 3GPP (rel 5,6 et 7)[[134]](#footnote-135), l’ETSI\* et l’IETF\*. Cette évolution permet d’accéder à des services multimédias depuis plusieurs supports, elle facilite le *roaming* et l’itinérance\* et est très adaptée à la mutualisation des plateformes chez les opérateurs. Le concept repose sur l’identification de l’abonné par un unique « *user* ID privé » qui est associé à plusieurs identités publiques qui seront utilisées pour le routage (numéro de téléphone, user ID SIP).

**Pour aller plus loin**

Le système IMS se présente sous la forme d’une architecture en couches et fonctionnelles qui peut être représentée comme suit :

Couche application ;

Couche service ;

Couche contrôle de session ;

Couche accès.

L’architecture repose également sur des fonctionnalités et des équipements spécifiques tel que :

• Le HSS - *Home Subscriber Server*: Base de donnée centrale su système qui regroupe les informations clients et les services. Le HSS intègre les fonctions de HLR du réseau GSM\*.

• Le CSCF – *Call Session Controm Function* qui rassemble plusieurs sous fonctions :

• P-CSCF : *Proxy- CSCF*, serveur proxy qui permet d’identifier les différents types d’appels entrants, premier point de contact client, il assure l’authentification et gère également la qualité de service (QoS)

• I-CSCF – *Interrogating CSCF*, point d’entrée de messages SIP qui assure donc les fonctions de la couche transport entre les différents opérateurs ;

• S-CSCF, *Service-CSCF*, serveur qui assure le contrôle de session, identifie l’appelant et les types de services associés.

**IMSI – *International Mobile Subscriber Identity***

Numéro unique international attribué à un abonné GSM\* (également UMTS et LTE). Ce numéro, de 13 à 15 chiffres, est inscrit sur la carte SIM\* de l’abonné. La norme ETSI TS 123 003[[135]](#footnote-136), précise en outre qu’il se décompose en trois champs :

- Le MCC *Mobile Country Code,* code de trois chiffres qui identifie de façon unique le pays de domiciliation de l’abonné ;

- Le MNC *Mobile Network Code,* deux ou trois chiffres qui identifient l’opérateur de télécommunication ;

- Le MSIN *Mobile Subscriber Identification Number,* 10 chiffres qui sont le numéros de l’abonné au sein du réseau de son opérateur.

**IMT 2000 – *International Mobile Telecommunications 2000***

L’Union Internationale des Télécommunication (UIT) a, au milieu des années 80, lancé un projet collaboratif pour fixer des standards pour les téchnologies d’accès radio des systèmes cellulaires de troisième génération (3G). L’objectif étant de favoriser des standards communs pour le plus grands nombres de terminaux, garantissant la compatibilité au niveau mondial (notammment la possibilité de *roaming\**) et une qualité améliorée.

Ce projet a abouti, début 2000, à la recommandation ITU-3 M.1457[[136]](#footnote-137) qui retient 5 standards :

• IMT-DS ou W-CDMA pour les réseaux UMTS\* ;

• IMT- MC ou CDMA 2000 ;

• IMT-TD qui regroupe TD-CDMA et TD SCDMA ;

• IMT-SC ou UWC ;

• IMT-FT ou DECT\*.

Depuis l’assemblée des radiocommunications de 2007, IMT 2000 intègre également la technologie OFDMA.

**Incident**

*(Incident)*

En sécurité des systèmes d’information, un incident est un événement non désiré susceptible de porter atteinte à la sécurité d’un système d’information. L’atteinte potentielle doit donc porter sur la confidentialité\*, l’intégrité\* ou la disponibilité\* du système.

La norme ISO 27000 en propose la définition suivante : un incident de sécurité est un ou plusieurs événements indésirables ou inattendus, liés à la sécurité de l’information, et présentant une forte probabilité de compromettre les opérations liées à l’activité de l’organisation et de menacer la sécurité de l’information.

Lorsque l’on détermine la nature et la gravité\* d’un incident de sécurité on parle alors de qualification\*.

**Infobésité**

*(Information overload)*

L’accès aisé à l’information, la multiplication des sources et des supports, entraine progressivement une saturation des processus décisionnels. L’infobésité est donc un concept qui illustre cette surabondance de l’information. Ce « trop plein » paralyse la prise de décision car les organisations passent plus de temps à « gérer leurs flux d’information » qu’à analyser et produire des décisions. Les nouvelles technologies de l’information et de la communication n’ont pas créé ce problème mais elles en ont sensiblement augmenté les conséquences et génèrent aujourd’hui de nombreux dysfonctionnements.

**Infogérance**

*(I.T. Management)*

L’infogérance est un service d’externalisation\* qui permet à une entreprise de confier la gestion de son système d’information à un prestataire. L’infogérance est donc un produit régulièrement proposé par des SSII\* ou ESN\*. Ce service est formalisé dans un contrat pluriannuel, à base

forfaitaire, avec un niveau de services et une durée définis[[137]](#footnote-138).

**Information classifiée**

*(Classified Information)*

Si le terme est régulièrement utilisé à tort, l’information classifiée est définie de façon très précise dans le Code pénal français, art 413.9 : Information intéressant la défense nationale, qui a fait l’objet de mesures de classification destinées à restreindre leur diffusion ou leur accès.

Une information classifiée n’est donc pas nécessairement un « scoop » sulfureux, il s’agit d’une information dont on cherche à limiter la diffusion. En outre l’Instruction Générale Interministérielle 1300 (IGI 1300) précise que l’apposition de la marque de classification, telle que définie aux articles R.2311-2, R.2311-3 et R.2311-4 du code de la défense, confère matériellement le caractère de secret aux informations ou supports concernés et justifie, en cas de violation de la réglementation applicable, la mise en œuvre de règles pénales spécifiques.

**Informatique dans les nuages, infonuagique**

Voir *Cloud Computing.*

**Infrastructure**

*(Infrastructure)*

Dans le domaine des télécommunications, les infrastructures désignent les équipements physiques qui permettent l’interconnexion des systèmes.

**Infrastructure de clés publique – ICP**

Outil cryptographique, technique et organisationnel permettant de garantir l’authenticité des clés publiques par la signature électronique\* d’autorités de certification\* organisées de façon hiérarchique. Une ICP est l’un des outils fondamentaux d’une IGC\*[[138]](#footnote-139).

Voir IGC, PKI, Signature électronique, Autorité de certification.

**Infrastructure de gestion de clés – IGC**

*(Public Key Infrastructure – PKI)*

Ensemble organisé de composantes fournissant des services de gestion des clés\* cryptographiques et des certificats\* de clés publiques au profit d’une communauté d’utilisateurs[[139]](#footnote-140).

Voir PKI.

**Ingénierie sociale**

*(Social engineering)*

L’ingénierie sociale est une pratique qui vise à acquérir des informations personnelles d’un utilisateur en interagissant avec lui. Ces techniques font appel aux techniques de manipulation psychologique. Ainsi, « la peur du patron » et « l’effet de l’expert » sont régulièrement utilisés. Il s’agit, le plus souvent par téléphone, de se faire passer pour un dirigeant de l’entreprise ou un responsable technique pour rapidement extorquer des mots de passes personnels d’un utilisateur. L’hameçonnage\* tire parti des techniques d’ingénierie sociale au même titre que l’exploitation de sources ouvertes afin de déterminer des vulnérabilités\* au sein d’une structure cible. L’ingénierie sociale est ainsi bien souvent la première phase d’une attaque ciblée. La sécurité d’un système d’information passe également par une vigilance accrue des utilisateurs.

**Injection SQL**:

Une injection SQL\* est une exploitation de vulnérabilité\* qui repose sur le principe de l’injection de requêtes SQL non prévues et qui compromettent la sécurité d’un système. Ce type d’attaque est particulièrement redoutable car il permet, par exemple, de contourner les systèmes d’authentifications\* de page Web (c’est à dire d’usurper des identités) ou encore d’altérer des données ou enfin de contourner des règles de gestion. L’injection SQL exploite généralement un défaut de vérification des champs SQL afin d’écraser des données, élever ses privilèges, etc.

**Inmarsat - *INternational MARitime SATellite Organisation***

Compagnie de télécommunication de droit britannique qui exploite onze satellites géostationnaires et propose des services de téléphonie, transfert de données, télex et télécopie. Le système est utilisé notamment pour les télécommunications maritimes et est approuvé pour les systèmes de détresse et de sécurité en mer.

**Intégrité**

*(Integrity)*

L’intégrité est la propriété assurant qu’une information ou un traitement n’a pas été modifié ou détruit de façon non autorisée[[140]](#footnote-141). L’intégrité peut s’appliquer aux données ou au réseau lui-même. L’intégrité des données désigne alors le fait qu’aucune altération n’est intervenue durant le processus de transport via le réseau. L’intégrité du réseau traduit le fait qu’il n’y a aucune activité ou aucun service actif en contradiction avec la politique de sécurité.

**Intelsat - *INTernational TELecommunication SATelitte consortium***

Historiquement consortium international regroupant onze pays pour fournir des services de communication par satellite, Intelsat est aujourd’hui une société privée implantée aux Bermudes. Elle gère une flotte de 53 satellites géostationnaires et offre de nombreux services : communications par satellites (*satcom)*, diffusion télévisuelle, interconnexion IP, etc.

**Interconnexion**

*(Interconnection)*

L’interconnexion est une fonction essentielle du réseau, on peut en donner plusieurs définitions en fonction de l’approche adoptée. Ainsi l’interconnexion peut être vue comme la capacité à connecter différents réseaux de télécommunications afin de relier les abonnés d’opérateurs différents. Le Code des Postes et des communications électroniques en offre la description suivante : On entend par interconnexion la liaison physique et logique des réseaux ouverts au public exploités par le même opérateur ou un opérateur différent, afin de permettre aux utilisateurs d'un opérateur de communiquer avec les utilisateurs du même opérateur ou d'un autre, ou bien d'accéder aux services fournis par un autre opérateur. Les services peuvent être fournis par les parties concernées ou par d'autres parties qui ont accès au réseau. L'interconnexion constitue un type particulier d'[accès](http://www.marche-public.fr/Marches-publics/Definitions/Entrees/acces.htm) mis en œuvre entre opérateurs de réseaux ouverts au public.

Occupation centrale pour un architecte de réseau, l’interconnexion s’entend tout autant sur le plan logique que physique, elle utilise alors des infrastructures dédiées (routeurs, passerelles).

**Interface**

*(Interface)*

Une interface désigne une « frontière » entre deux parties d’un même système. Il s’agit ainsi de tout dispositif permettant l’adaptation de deux équipements ainsi que les liaisons entre ceux-ci. Pour autant cette première approche est impropre pour les systèmes de télécommunication. En effet, dans ce contexte une interface désigne des modes d’adaptation normalisés entre des terminaux de transmission de données et un réseau. On parle ainsi « d’interface radio » pour décrire le dispositif qui permet à un terminal mobile de communiquer avec le réseau.

L’interface A se situe, pour sa part, entre le sous-système radio (BSS\*) et le sous-système réseau (NSS\*). Elle assure la transmission des messages de signalisation\*. Si l’on quitte les télécommunications pour se tourner vers les langages de programmation informatique, une interface désigne une tout autre notion. Dans les langages orientés objet\* une interface désigne un équivalent d’une classe qui ne contient que des signatures de méthodes, propriétés ou événements sans jamais les implémenter\*.

Ainsi en langage C# ou Java\*, une interface est l’équi­valent d’une classe abstraite qui ne décrit que des méthodes, sans les implémenter. Une interface, pour être utile, doit donc être implémentée par une classe\* ou une structure. Par convention le nom d’une interface commence toujours par un I, elle est toujours publique.

**Interférence**

*(Wave interférence)*

Phénomène résultant de la superposition d’au moins deux oscillations ou ondes cohérentes de même nature et de fréquences égales ou voisines ; ce phénomène se manifeste par une variation dans l’espace ou dans le temps de l’amplitude de la résultante des ondes ou oscillations superposées. Le phénomène se manifeste dans l’espace par des franges et dans le temps par des battements. Le terme ne doit pas être utilisé dans le sens de brouillage[[141]](#footnote-142).

Parce qu’elles dégradent un signal radio, les interférences doivent être évitées autant que possible. Dans un cadre domestique, certains équipements peuvent générer des interférences avec le signal WiFi\*, il est alors conseillé de changer de canal ou d’éloigner la source d’interférence lorsqu’elle est connue. Voir Brouillage.

**Internet – *Interconnected Networks***

Réseau mondial associant des ressources de télécommunication et des ordinateurs serveurs et clients, destiné à l’échange de messages électroniques, d’informations multimédias et de fichiers. L’internet fonctionne en utilisant un protocole commun qui permet l’acheminement de proche en proche de messages découpés en paquets\* indépendants. L’acheminement est fondé sur le protocole IP (Internet Protocol), spécifié par l’Internet Society. L’accès au réseau est ouvert à tout utilisateur ayant obtenu une adresse auprès d’un organisme accrédité. La gestion est décentralisée en réseaux interconnectés[[142]](#footnote-143).

Au-delà de cette définition, Internet désigne en fait un ensemble décentralisé qui regroupe plusieurs réseaux reposant sur une famille unique de protocole TCP/IP\* (*Transmission Control Protocol*/*Internet Protocol*). Ce protocole unique permet l’acheminement de paquets entre un serveur\* et un client\*. On rattache communément l’origine d’Internet au projet ARPANET\* conduit aux Etats-Unis à partir des années 60. Aujourd’hui, « le réseau des réseaux » interconnecte environ 45 000 systèmes autonomes\* (réseaux) et permet un accès à près de 3 milliards de personnes (ce chiffre est en croissance exponentielle depuis le début des années 2000). Cette croissance rapide pose des problèmes tant techniques que sociaux et sociétaux. Sur le plan technique, les questions de gouvernance sont devenues essentielles pour maintenir une architecture fiable, robuste et sûre. Les problèmes de routage\*, de DNS\* d’allocations de noms de domaine\* etc. ne sont plus réservés à une frange d’experts marginaux mais ont un impact direct sur l’activité économique et la « vraie » vie. Sur le plan social, un accès quasi permanent et en haut débit à l’Internet modifie profondément les fondements de certains groupes sociaux. Ainsi, les habitudes de consommation changent, de nouveaux services « en ligne » émergent et bousculent les circuits classiques de production et de distribution. Enfin, le partage, l’échange et le savoir disponible contribuent à un éveil de la conscience politique et favorise les revendications démocratiques. Internet n’est pas seulement un ensemble de réseaux, il est un objet social.

**Internet des objets**

*Internet Of Things (IOT)*

L’Internet des objets est une notion relativement jeune dont la définition n’est pas encore totalement stabilisée. Le concept repose sur le fait de relier au réseau des objets ou des entités qui n’avaient pas vocation à y entrer et d’assurer un flux d’information entre ces entités « physiques » et le monde virtuel. Ainsi, les premières applications voient le jour dans la domotique où des objets comme des congélateurs peuvent aujourd’hui gérer leurs stocks en temps réels voire demander des réapprovisionnements directement sans intervention humaine. Les puces RFID\* permettent de relier au réseau des objets et garantissent la traçabilité et le suivi des envois postaux par exemple. Dans leur étude *L’internet des objets, quels enjeux pour l’Europe ?* Pierre-Jean Benghozi, Sylvain Bureau et Françoise Massit-Folléa proposent une définition large qui permet de concilier l’approche technique et fonctionnelle.

L’internet des objets est un réseau de réseaux qui permet, via des systèmes d’identification électronique normalisés et unifiés, et des dispositifs mobiles sans fil, d’identifier directement et sans ambiguïté des entités numériques et des objets physiques et ainsi de pouvoir récupérer, stocker, transférer et traiter, sans discontinuité entre les mondes physiques et virtuels, les données s’y rattachant.[[143]](#footnote-144)

**Internet Protocol – IP**

(Protocole IP)

Voir IP v4, IP v6.

**Intranet**

Un réseau intranet est un réseau interne (entreprise, organisation, administration) s’appuyant sur le protocole IP\*. Il propose des services et n’est accessible, par définition qu’aux membres du réseau local (sauf pour les ressources partagées dans la DMZ\* et les accès par VPN\*). Une architecture d’Intranet se divise typiquement en trois parties :

• les clients, en général des navigateurs internet sur des postes utilisateurs (*Firefox*, *Internet* *explorer*, etc.) ;

• des serveurs d’applications (*middleware*\*) ;

• des bases de données.

Voir LAN, VPN, DMZ.

**Intrusion**

*(Intrusion)*

En sécurité des systèmes d’information, une intrusion désigne le fait d’accéder, sans y être explicitement autorisé, à un système. La Loi française dans l’article 323-1 du code pénal, précise que le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.

Voir STAD.

**Invitation à émettre**

*(Polling)*

En télécommunication, consultation, généralement séquentielle et éventuellement cyclique, des stations d’un réseau de télécommunication par une station centrale, afin que celles qui ont des messages à émettre le fassent immédiatement[[144]](#footnote-145).

**Invitation à recevoir**

*(Selecting)*

Envoi d’ordres, généralement séquentiel et éventuellement cyclique, par une station centrale à des stations d’un ré-

seau de télécommunication, afin que chacune se prépare à recevoir le message qui lui est destiné[[145]](#footnote-146).

**IP V4**

*(Internet Protocol v4)*

IPv4 est un protocole\* réseau, décrit dans la RFC\* 791, qui permet l’interconnexion\* de deux sous-réseaux aux caractéristiques différentes. C’est le protocole fondamental des échanges Internet car il permet le découpage et le transport de l’information (sous forme de datagrammes\*). Il gère l’adressage et le routage\* entre machines, la constitution et le réassemblage des paquets ainsi que leur cheminement dans le réseau. Le protocole IP permet le routage des données par l’ajout de champs qui déterminent l’adresse de destination, l’adresse source et d’autres informations nécessaires au réassemblage des paquets pour retrouver le message d’origine. Une adresse IPv4 est codée sur 4 octets (voir Adresse IP\*), il est donc possible d’allouer 232 adresses (soit un peu plus de 4 milliards). Cette limite a conduit au développement d’IPv6\*.

Voir Adresse IP.

**IP V6**

*(Internet Protocol v6)*

IP V6 est un protocole de réseau de niveau 3 (réseau) du modèle OSI\*, développé dans les années 90 pour succéder à l’IP V4 et faire face à l’épuisement du nombre d’adresses. Avec IP V4 ces dernières sont codées sur 4 octets, ce qui en limitent le nombre. Enfin, IPV4 n’embarque pas de mécanisme de sécurité, cette dernière doit donc être prise en charge par les couches supérieures (SSL\*/TLS), IPSEC\*. Face à la pénurie prévisible, la norme IP V6 devrait être progressivement déployée. Les adresses sont maintenant codées sur 16 octets (ce qui permet d’allouer 2128 adresses, soit environ 3x1038 contre 4,29x109 en IP V4), l’en-tête des datagrammes est plus simple et leur routage en est facilité. Le protocole est décrit complètement dans le RFC 2460. Pour l’heure, la mise en place d’IP V6 est assez lente est représente environ 3 % du trafic mondial en 2014. La notation décimale pointée, utilisée pour les adresses IPv4, est abandonnée et l’on y substitue une écriture hexadécimale. Dans ce cadre, les 8 groupes de 2 octets sont séparés par « : » comme dans l’exemple ci-dessous :

X :X :X :X :X :X :X :X avec X une valeur hexadécimale.

Des simplifications sont possibles (on peut ainsi omettre les zéros non significatifs, ou encore remplacer les groupes consécutifs de 16 bits nuls par « :: » ) et comme pour IPv4 certaines adresses sont réservées.

**IPBX - *Internet Protocol-Private Branch Exchange***

(Autocommutateur privé)

Autocommutateur téléphonique privé, l’IPBX ou PABX IP est utilisé au sein des entreprises pour assurer des services de téléphonie sur IP.

**IPS - *Intrusion Prevention System***

(Système de prévention d’intrusion)

Un IPS est un équipement de sécurité des réseaux qui analyse le trafic et exécute des contre-mesures face aux intrusions. Les mécanismes de détection sont similaires à ceux d’un IDS\* (base de signature et approche comportementale) mais l’IPS ajoute une capacité de réaction associée à la détection (fermeture d’un port\*, reconfiguration de *firewall*\*, génération de paquets pour couper une connexion). Comme l’IDS, l’IPS opère soit au niveau réseau, soit au niveau des hôtes\*, il ne constitue pas une solution parfaite car il peut générer des faux positifs et ainsi couper des flux légitimes.

Voir IDS, *Firewall.*

**IPSEC – *Internet Protocole Security***

(Protocole Internet Sécurisé)

IPSEC est un protocole réseau (couche 3 du modèle OSI\*) défini par l’IETF\* (RFC\* 2401 - 4301) dont l’objectif est de fournir des services de sécurité adaptés aux besoins de confidentialité, de nomadisme et d’accès distant à des ressources internes (extranet\*). La principale fonctionnalité d’IPSEC réside dans son mode *tunneling* qui permet d’établir une communication sécurisée entre deux entités par la création d’un « tunnel » virtuel où les données sont chiffrées. Ces techniques d’encapsulation permettent de créer des réseaux privés virtuels (VPN\*). IPSEC repose sur plusieurs autres protocoles dont *Internet Key Exchange -* IKE (RFC 2409 - 4306) qui permet l’établissement d’un premier tunnel entre deux machines (gestion des clés, données administratives). Pour l’échange de données, IPSEC s’appuie sur deux autres protocoles, *Authentication Header -* AH (RFC 2402 – 4302 - 4305) pour l’authen­tification des deux parties et *Encapsulating Security Payload -* ESP (RFC 2406 – 4303 - 4305) qui chiffre les données.

Outre le mode tunnel, IPSEC implémente deux autres modes :

• mode *transport*: seul les données transportées sont chiffrées, le reste du paquet (donc l’en-tête) n’est pas modifié.

• mode *nesting* (hybride entre transport et tunnel) : dans ce cas, il s’agit d’encapsuler un paquet IPsec dans de l’IPsec.

**IPX – *Internet Packet eXchange***

Protocole de la couche 3 du modèle OSI\* (réseau), il fournit aux serveurs de fichiers et aux stations *Netware* un système d’adressage et de routage inter réseaux. Il s’agit de l’implémentation de IDP – *Internet Datagram Protocol* pour les réseaux locaux *Netware\** de Novell. IPX est utilisé avec SPX – *Sequenced Packet eXchange*, protocole de la couche 4 qui assure les services orientés connexions.

Voir *Netware*.

**IRC – *Internet Relay Chat***

Protocole de communication textuelle en temps réel sur internet par l’intermédiaire d’un client\*. Le client se connecte à un serveur\* lui-même connecté à un ensemble d’autres serveurs. IRC permet de rejoindre des forums (publics ou privés) ou chacun peut dialoguer en utilisant des commandes spécifiques et en respectant des conventions (netiquette\*). Un canal IRC est ainsi un ensemble qui regroupe des utilisateurs autours d’un sujet particulier. Le nom d’un canal est précédé du symbole # qui a, par la suite, était utilisé sur le réseau social Twitter.

**IRTF- *Internet Research Task Force***

L’IRTF est un groupe de travail de l’IAB\* au même titre que l’IETF\*. Ce groupe est plus particulièrement en charge de la recherche et du développement de l’Internet.

Voir IAB.

**IS-95**

Norme américaine de réseau cellulaire de seconde génération. IS-95 est basée sur la méthode d’accès CDMA\*.

**ISDN – *Integrated Service Digital Network***

Voir RNIS - Réseau Numérique à Intégration de Données.

**IS-IS – *Intermediate Sytem to Intermediate System***

A l’instar OSPF\*, IS-IS est un protocole interne de routage\* à état de liens (qui utilise l’algorithme de Dijkstra\*). Typiquement, chaque routeur, pour établir sa table interne et dresser une cartographie de l’état du réseau, transmet vers ses voisins l’état de ses liaisons. IS-IS permet de définir plusieurs domaines, donc des zones de routage, et limite ainsi la taille des tables et les temps de convergence[[146]](#footnote-147). Le routeur IS-IS peut être utilisé en intrazone (pour échanger des messages au sein de la zone où il est défini) ou interzone pour échanger des routes entre plusieurs zones. Le protocole n’utilise pas IP comme protocole réseau (il est indépendant des protocoles qu’il route) il est donc nécessaire de définir un adressage particulier pour chaque routeur. Codée sur 10 octets, l’adresse du routeur (adresse ISO NET) se décompose comme suit : les trois premiers octets sont des identifiants de zone, le six suivants assurent l’identification de l’équipement dans la zone, le dernier octet est positionné à 0x00. Le protocole est normé par l’ISO/CEI 10589 :2002 et spécifié par la RFC 1142.

**ISL – *Inter Switch Link***

Le protocole ISL est un protocole propriétaire CISCO qui permet d’étendre des réseaux virtuels sur plusieurs commutateurs. Ainsi, ISL assure le transfert de trames\* Ethernet\*, avec leurs numéros d’identification de réseau virtuel, entre commutateurs (ou routeurs). Le marquage de la trame (*frame tagging*) est effectué en entrée de l’équipement (commutateur\*) puis la trame est encapsulée. Le mécanisme est indépendant des stations émettrices et réceptrices.

Ce mécanisme est supplanté par le standard IEEE 802.1q qui est un mécanisme d’encapsulation permettant également la propagation de plusieurs VLAN\*\* sur un même lien (physique).

**ISO – *International Standard Organisation***

(Organisation Internationale de normalisation)

L’ISO est une fédération internationale d’organismes de normalisation, il est « le premier producteur mondial de Normes internationales d'application volontaire. Les normes établissent des spécifications de premier ordre pour les produits, les services et les bonnes pratiques dans une optique de qualité, sécurité et efficacité. Élaborées par voie consensuelle à l'échelon mondial, elles aident à supprimer les obstacles au commerce international. Depuis 1947, l'ISO a publié plus de 19 500 normes internationales qui couvrent la quasi-totalité des secteurs de l'industrie – des technologies à la sécurité des denrées alimentaires, et de l'agriculture à la santé[[147]](#footnote-148). »

Les normes concernant les technologies électriques et électrotechniques sont du ressort de la Commission Electrotechnique Internationale\* (CEI)*.*

Le terme ISO est régulièrement confondu avec OSI\* *Open System Interconnect* dont l’acronyme français est Interconnexion des systèmes ouverts (ISO). Par ailleurs, le modèle OSI est lui-même normalisé par l’ISO (ISO 7498)…

Voir modèle OSI\*.

**ISOC – *Internet SOCiety***

Association d’origine américaine, divisée en plusieurs « chapitres » dont un français[[148]](#footnote-149), l’ISOC est un acteur central du développement de l’Internet. L’association se fixe pour mission de :

Promouvoir le *développement, l’évolution, et l’utilisation* de l’Internet au bénéfice de tous les individus à travers le monde.

Pour aider à l’achèvement de cette mission, l’Internet Society :

* Facilite le développement ouvert des normes, des protocoles, de l’administration et de l’infrastructure technique de l’Internet.
* Soutient l'éducation, notamment dans les pays en développement et partout où le besoin existe.
* Favorise le développement professionnel et construit une communauté pour encourager la participation et le *leadership* dans des domaines importants pour l’évolution de l’Internet.
* Fournit des informations fiables sur l’Internet.
* Organise des forums de discussions sur des questions touchant à l’évolution, le développement et l’usage de l’Internet dans les domaines technique, commercial, social et autres.
* Encourage un environnement pour la coopération internationale, la communauté et une culture qui permettent à l’auto-gouvernance de fonctionner.
* Sert de base aux efforts de coopération visant à promouvoir l'Internet comme un outil positif profitant à tous les peuples à travers le monde.
* Gère et coordonne les initiatives stratégiques et les efforts de sensibilisation dans les domaines humanitaire, éducatif, social et autres.[[149]](#footnote-150)

**IT Management**

(Infogérance)

Voir Infogérance.

**ITA – *Information Technology Agreement***

(Accord cadre sur les technologies de l’information)

L’ITA est un accord cadre de l’organisation mondiale du commerce (OMC) conclu par 29 pays lors de la conférence des ministres de Singapour en 1996. Cet accord vise à supprimer les tarifs douaniers pour les produits des technologies de l’information et de la communication (TIC). Le nombre de signataires est progressivement passé à 70 couvrant 97% du marché mondial des produits technologiques.

**ITIL – *Information Technology Infrastructure Library***

(Bibliothèque de l’infrastructure des technologies de l’information)

L’ITIL est un ensemble de références et de guides qui rassemblent les bonnes pratiques en matière de management des services informatiques (IT management). Ce corpus permet aux DSI de disposer de documentations et d’outils afin d’améliorer la qualité de leurs prestations[[150]](#footnote-151).

**Itinérance**

*(Roaming)*

L’itinérance est une fonctionnalité technique qui permet à un usager d’utiliser son téléphone mobile depuis l’étranger (plus précisément hors de portée de son opérateur) via un opérateur qui n’est pas le sien. L’usager bénéficie donc de prestations de la part d’un opérateur « hôte ». Les opérateurs négocient ainsi entre eux des accords d’itinérance qui fixent les prestations qu’ils s’engagent à fournir aux abonnés. Il existe ainsi plusieurs type de *roaming*: régional, national, international en fonction de la zone dans laquelle s’applique le mécanisme d’interconnexion.

***Pour aller plus loin….***

L’itinérance est un processus de mouvement entre deux cellules, gérées par des opérateurs différents, sans clôture de la connexion, exactement comme le mécanisme de « *handover\**» en téléphonie portable mais avec des différences notables dans un environnement « paquets ». Le standard 802.11 ne définit pas à proprement parler le mécanisme de *roaming*, il en fixe quelques règles de base (écoute active, réassociation de station), il a donc été nécessaire de proposer un amendement [802.11r] en 2008 baptisé le *Fast Basic Service Transition.* Ce standard décrit les mécanismes qui permettent à un appareil sans fil en déplacement de rester connecté. La bascule d’un point d’accès à l’autre est plus sûre et plus rapide, elle incorpore aujourd’hui les mécanismes d’authentification (802.1X).

**ITU - *International Telecommunication Union***

Voir UIT - Union Internationale des Télécommunications.

**IXFR – *Incremental Zone Transfer***

(Transfert de zone incrémental)

Le transfert de zone\* incrémental est une technique de transfert de zones DNS normalisée par la RFC 1995. IXFR permet d’envoyer uniquement la liste des changements d’enregistrements à effectuer sur le fichier zone et non une recopie complète de la base.

Voir Transfert de zone.

**IXP – *Internet eXchange Point***

(Point d’échange Internet)

Un IXP est un équipement physique qui permet les échanges de trafic Internet entre opérateurs. Un IXP assure donc l’échange de trafic entre différents systèmes autonomes (AS\*).

# J

**Jabber**

Jabber est un protocole\* de messagerie instantanée basé sur XML\*. Inventé en 1998, Jabber est aujourd’hui devenu le protocole XMPP (*eXtensive Messaging and Presence Protocol*).

**Java**

Le langage de programmation Java est un langage orienté objet\* développé par Sun Microsystems (racheté par Oracle en 2009, qui en assure aujourd’hui le maintien). Java reprend la syntaxe du C++ tout en simplifiant certaines notions (pas d’héritages multiples, pas de gestion de la mémoire). Java a comme principal avantage d’être un langage extrêmement portable, en effet, l’environnement de développement permet de s’assurer que le programme pourra fonctionner sous différents environnements (Linux, Mac Ox, Windows). Il permet de développer de multiples applications et dispose d’environnements spécifiques pour plateformes diverses :

• J2SE (*Java 2 Standard Edition)* pour les applications client lourd ;

• J2EE (*Java 2 Entreprise Edition)* pour les applications Web ;

• J2ME (*Java 2 Micro Edition)* pour les applications sur plateformes mobiles (téléphones, etc.).

Voir Interface, Pointeurs, Programmation par objet.

**JavaScript** - **JS**

JavaScript est un langage de programmation de scripts\*. Langage interprété, il est principalement utilisé pour les pages Web. Dans ce cas, c’est le poste client qui exécute le script (navigateur Web).

**Jeton**

(*Token)*

Dans une topologie\* réseau local « anneau à jeton », le jeton sert dans la méthode d’accès. Le jeton est ainsi une trame\* spéciale de trois octets qui circule (toujours dans le même sens) sur le réseau. Chaque station recueille cette trame et la transmet à la station suivante sur l’anneau. Si une station désire émettre, elle conserve le jeton.

Voir Topologie.

***Jitter***

(Gigue)

En télécommunication, la gigue désigne une variation légère de la phase du signal. Cette variation peut entrainer des erreurs dans la transmission. Dans un réseau, la gigue représente également la variation de la latence\*.

Voir Latence.

**Jonction**

*(Junction)*

Une jonction est une connexion physique (frontière entre deux appareils) définie par un ensemble de caractéristiques mécaniques, électriques et fonctionnelles.

**Journalisation**

La journalisation consiste, pour un serveur ou une application, à consigner dans un fichier ou dans un élément de stockage des données. Les données consignées peuvent être de différentes natures en fonction du type de service ou d’application. Un serveur pourra journaliser les actions des clients venus se connecter sur lui. Elle est un des aspects essentiel dans la gestion et la sécurisation d’un système d’information[[151]](#footnote-152).

Voir *log.*

**JPEG** - ***Joint Picture Expert Group***

Groupe d’experts en charge de l’édition de normes pour la compression des images statiques (photographies). L’u­sage veut que la norme produite par ce groupe soit aujourd’hui reprise par le même acronyme JPEG.

La norme JPEG est normalisée par l’ISO/CEI 10918-, elle décrit l’algorithme de compression, le format d’enre­gis­trement ainsi que le décodage d’une image numérique com­pressée. Ce format est aujourd’hui largement rependu pour les images numériques.

**JSON - *JavaScript Object Notation***

Format\* de données générique qui permet de représenter l’information de façon structurée. JSON est décrit dans la RFC\* 7159. JSON utilise la notation JavaScript\* (dont il tire son nom) mais n’est pas un langage de programmation (un document JSON n’est qu’un objet pour JS). En outre JSON est proche d’XML\* mais plus lisible, et plus facilement interprétable.

# K

1. **Kerberos**
2. Protocole d’authentification\* réseau qui repose sur un système de clés secrètes et d’échange de « tickets ». L’origine du nom vient de la mythologie grecque où Kerberos (Cerbère en français) est le nom du chien à trois têtes gardien des enfers. L’architecture du système s’appuie sur des serveurs d’authentification (*Authentification Server* AS) qui permettent l’authentification des clients, des serveurs de délivrement de tickets de service (*Ticket Granting Service* - TGS) qui permettent d’accéder à des services et un centre de distribution de clés (*Key Distribution Center* - KDC). La version 5 du protocole est décrite dans la RFC\* 4120.
3. ***Kernel***
4. (Noyau)
5. En informatique, le *kernel* ou le noyau (noyau de système d’exploitation) est un programme qui gère les demandes (entrées - sorties) des *softwares* et les traduit en instructions pour le processeur. C’est une partie fondamentale d’un système d’exploitation qui permet la communication entre les processus. Voir Système d’exploitation.
6. ***Keylogger – keystroke loger***
7. (Enregistreur de frappe)
8. Voir Enregistreur de frappe.
9. ***Kill Switch***
10. (Système d’arrêt d’urgence)
11. Le concept du *Kill Switch* repose sur la possibilité d’interrompre, en urgence et à distance, le fonctionnement d’une application ou d’un terminal. Pour limiter les conséquences des vols de téléphones mobiles, les Etats-Unis impose (à partir de 2015) que tous les terminaux vendus sur leur territoire soient équipés d’un tel système. Par ailleurs, le terme a également été utilisé en 2011 pour évoquer la possibilité de « couper » Internet en cas d’attaque majeure contre les infrastructures américaines.
12. ***Killer Services***
13. Un *Killer service* est un service nouveau dont le succès prévisible sera immédiat et pour lequel les utilisateurs sont prêts à payer.

# L

**LA – *Location Area***

(Zone de localisation)

Dans une architecture GSM\*, une aire de service placée sous le contrôle d’un MSC\*/VLR\*, est composée de plusieurs zone de localisation (LA – *Location Area*). Chaque LA est identifiée par une adresse unique la LAI – *Local Area Identification.*

Cette adresse est composée de plusieurs champs :

• MCC\* : *Mobile Country Code.* Désigne le code pays du réseau GSM (ce champ est également présent dans l’IMSI\*) ;

• MNC\* : *Mobile Network Code*. Désigne le code du réseau mobile (ce champ est également présent dans l’IMSI) ;

• LAC\*: *Location Area Code.* Code de la zone de localisation, affecté par l’opérateur.

**Label**

(*Label)*

Un label est un identifiant de longueur fixe qui permet d’identifier un ensemble de paquets\* IP qui doit être traité de façon identique. Utilisé dans le protocole MPLS\* - *MultiProtocol Label Switching*, le label permet d’identifier une classe d’équivalence (FEC – *Forwarding Equivalence Class).* Voir également MPLS.

**LAC** - ***Location Area Code***

(Code de zone de localisation)

Voir LA – Location Area.

**LAI – *Location Area Identification***

(Identifiant de zone de localisation)

Voir LA – *Location Area*.

**LAN** **- *Local Area Network***

(Réseau Local)

Un LAN est un réseau local qui connecte des équipements au sein d’un ensemble géographique limité. Au niveau adressage IP, un LAN correspond en général à un sous-réseau. La norme Ethernet\* est courante dans un réseau local, mais d’autres topologies sont possibles (*Token Ring*). Le LAN est initialement limité par les commutateurs interconnectés. Au sein d’un même réseau physique il est possible, grâce à la virtualisation, de constituer plusieurs LAN comme s’ils étaient physiquement distincts. Les VLAN\* sont donc *logiquement* séparés.

Voir *Intranet,* VLAN.

**LAP**- ***Link Access Protocol***

(Protocole d’accès de lien)

Famille de protocole de niveau 2 du modèle OSI\*, dérivé de HDLC\*, le LAP s’assure que les trames\* arrivent dans l’ordre et sans erreurs. Il existe plusieurs classes de protocole. On utilise fréquemment :

• LAPB - *Link Access Protocol B-channel* : qui est utilisé dans X25 (décrit par la recommandation X.25\* 10/96 de l’ITU\*) ;

• LAPD  - *Link Access Protocol D-channel*: protocole de liaison de données utilisé dans le réseau GSM\*.

**Large bande**

(*Broadband)*

Caractérise les réseaux à haut débit. Ainsi, pour la téléphonie mobile, les fréquences à large bande permettent de transmettre plus de données à plus haut débit.

**Largeur de bande**

*(Bandwidth)*

La largeur de bande représente la différence entre la fréquence la plus haute et la fréquence la plus basse d’une bande de fréquences. On parle également de bande passante\*.

Voir Bande passante.

**LCP – *Link Control Protocol***

(Protocole de contrôle de liens)

LCP est un protocole de contrôle de liens, il est chargé de gérer l’établissement, le maintien et la fermeture d’une liaison physique. LCP est, avec NCP\* *Network Control Protocol,* utilisé par PPP\* *Point to point protocol* comme contrôleur de liens.

Le protocole permet ainsi de vérifier l’identité d’un équipement connecté, de fixer la taille des paquets pour la transmission, de rechercher des erreurs et de terminer une liaison. LCP est décrit dans la RFC\* traitant de PPP, RFC 1661.

**LDAP – *Lightweight Directory Access Protocol***

(Protocole d’accès aux annuaires légers)

Protocole\* qui permet la création et l’interrogation d’annuaires. Initialement utilisé uniquement entre serveurs d’annuaires, LDAP est devenu un service à part entière et permet la communication entre les équipements du réseau et le service d’annuaire. Plus qu’un protocole, LDAP est aujourd’hui également un modèle de données et de nommage.

Couplé à un serveur d’authentification\*, il sert d’infra­structure de gestion d’identité. *Microsoft Active directory* est une interprétation des services d’annuaire LDAP pour les systèmes d’exploitation Microsoft. Modèle léger de DAP - *Directiry Acces Protocol* qui servait pour les interrogations de serveurs X.500\*, LDAP respecte le modèle X.500 normalisé par l’UIT. LDAP est décrit dans de nombreuses RFC\* (4511 à 4519).

**LDAP Injection – *Lightweight Directory Access Protocol Injection***

Technique d’attaque qui permet la compromission d’un site Web qui utilise un serveur LDAP. Ce type d’attaque permet ainsi de saisir le contenu de l’annuaire.

**LDP - *Label Distribution Protocol***

(Protocole de distribution de label)

Dans un réseau MPLS\*, protocole\* qui permet de transmettre aux routeurs (LSR\*) les informations nécessaires pour associer les labels.

Voir MPLS.

***Least Cost Routing***

(Routage à moindre coût)

Type de routage qui permet de choisir, pour un appel, en priorité les routes les moins chères.

**Liaison**

(*Liaison, link)*

Ensemble des ressources nécessaires pour mettre en com­mu­nication deux équipements via un réseau d’inter­con­nexion. Une liaison est donc un moyen de communiquer des caractéristiques spécifiées entre deux points[[152]](#footnote-153).

Il existe plusieurs types de liaison en fonction du sens et du nombre de signaux que le canal véhicule. On parle ainsi de liaison *duplex* lorsque le canal ne supporte qu’un seul signal à la fois et de *simplex* si par ailleurs, il est véhiculé dans une seule direction. Pour que deux équipements communiquent sur un même canal la liaison est dite duplex (elle s’effectue dans les deux sens). Le signal peut alors changer de sens et aller d’un équipement à l’autre et inversement, on parle alors de *half-duplex* ou être transporté simultanément dans les deux sens, on parlera de *full-duplex*.

Voir *Duplex.*

**Liaison commutée**

*(Circuit switched connection)*

Une liaison commutée s’oppose à une liaison permanente car le canal de communication est établi de manière ponctuelle et limitée dans le temps. La commutation consiste donc à établir un canal physique pour une liaison donnée durant un temps donné, puis libérer la ressource.

**Liaison descendante**

*(Downlink)*

Liaison de télécommunication d’une station spatiale vers une station terrienne ou d’une station de base vers une station mobile[[153]](#footnote-154).

**Liaison de données**

*(Data Link)*

Type de liaison particulière affecté à une transmission numérique. Une liaison de données permet l’échange d’informations entre les équipements terminaux. Dans le modèle OSI\* la couche liaison de données (couche 2) gère donc les communications entre équipements directement reliés. Ethernet\*, *Token Ring*\*, X.25\* ou MPLS\* sont des protocoles de niveau 2.

**Liaison montante**

*(Uplink)*

Liaison de télécommunication d’une station terrienne vers une station spatiale ou d’une station mobile vers une station de base[[154]](#footnote-155).

**LIB - *Label Information Base***

Dans la technologie MPLS\*, les routeurs\* LSR\*, *Label Switching Router* constituent une table qui leur permet de savoir comment transmettre les différents paquets en fonction des labels associés. Cette table est la LIB.

**Lien**

*(Link)*

En informatique, un lien est une partie de programme qui transfère la commande et transmet les paramètres entre deux tronçons de programme distincts. Dans un envi­ronnement Web, un lien ou lien hypertexte\* est une référence qui permet de consulter un document lié à la page courante.

Dans un système d’exploitation\* (OS), un lien (ou raccourci) est un fichier qui contient l’adresse d’une ressource (autre fichier par exemple).

**Ligne de défense**

*(Ligne of défense)*

Le concept de défense en profondeur\* d’un système d’information repose sur l’organisation successive de plusieurs lignes de défense. Ces dernières ne sont pas exclusivement des barrières\* physiques mais comme le précise l’ANSSI dans son mémento sur la défense en profondeur :

Une ligne de défense est un ensemble de barrières, par scénario ou famille de scénarii, dont le franchissement provoque un incident dont la gravité\* dépend du nombre de barrières restantes à franchir par la ou les menaces pour atteindre le ou les biens protégés et de la valeur de ces biens (c'est-à-dire qu'à un incident de sécurité donné est associé un niveau de gravité qui indique la ligne de défense abstraite franchie). Toute ligne de défense pour être une ligne et pas seulement un ensemble de moyens de protection, doit être munie des dispositifs et moyens de détection/veille et de notification[[155]](#footnote-156).

**Ligne de transmission**

Une ligne de transmission est une liaison entre deux machines (ETTD\*). Appelé également support physique, elle assure le transport de données entre un émetteur et un récepteur. Les lignes de transmission sont regroupées en trois grandes familles distinctes en fonction des grandeurs physiques qui y circulent :

• Les supports filaires : pour la circulation d’électrons (généralement dans un câble métallique) ;

• Les supports aériens : permettent la propagation d’ondes électromagnétiques ou radio-électriques ;

• Les supports optiques : assurent l’acheminement de signaux optiques à la vitesse de la lumière.

**Liste noire – liste blanche**

(*Black list – White list*)

Utilisé dans tous les systèmes de filtrage, les listes blanche regroupe les éléments autorisés (exemple – liste d’adresses IP) alors que les listes noires regroupent ceux qui seront refusées (filtre anti-spam par exemple).

Voir Filtrage.

**LLC - *Logical Link Control***

(Contrôle de la liaison logique)

Sous-couche supérieure du niveau 2 du modèle OSI\* (liaison de données). Le LLC assure un contrôle d’erreur et un contrôle de flux de la sous-couche MAC\* (elle-même sous-couche inférieure de la couche liaison de données).

**LMI - *Local Management Interface***

(Interface locale de management)

Dans un réseau à relais de trame (*Frame relay*\*), LMI est un protocole local qui contrôle le lien entre un utilisateur et le réseau. Il permet de connaître l’état des circuits virtuels et diffuse des messages de disponibilité des circuits.

Voir *Frame Relay.*

**Log**

*(Log)*

Les logs désignent, dans un système informatique, l’historique des évènements qui affectent les processus (et par extension le fichier dans lequel ils sont stockés). Ils sont un élément essentiel de la sécurité car leur enregistrement chronologique au sein d’un journal (journalisation\*) permet d’analyser pas à pas le comportement d’un système et de détecter des événements suspects ou encore des attaques. Dans son Livre blanc sur les logs, un groupe de travail de l’OSSIR (Observatoire de la sécurité des systèmes d’information et des réseaux) souligne qu’il n’existe pas de définition formelle du terme en droit français. Ainsi, le terme *log* regroupe de nombreuses notions telle que : données relatives au trafic (Code des postes et des communications électroniques), données de connexion à des services de communications électroniques (Loi pour la confiance dans l’économie numérique) ou encore, données de connexion et fichiers de journalisation des connexions. Le groupe de travail estime ainsi que pour une meilleure compréhension il est nécessaire de distinguer les « *logs* » des « traces\* » et propose les définitions suivantes :

*Log* : journalisation de données informatiques résultant de l’utilisation d’une application ;

Trace : donnée informatique témoignant de l’existence d’une opération au sein d’une application. En effet, si toute utilisation d’une application induit directement ou indirectement des « traces », les « logs » eux-mêmes sont le résultat d’un choix volontaire du concepteur ou de l’utilisateur de surveiller une application[[156]](#footnote-157).

Voir Journalisation.

**Logiciel**  
*(Software)*

Un logiciel est un programme informatique constitué d’un ensemble d’instructions et de données pour les exécuter qui est interprétable par une machine. Le logiciel fixe donc les opérations à effectuer, leur ordre d’exécution ainsi que les conditions de cette exécution. Il existe plusieurs typologies de logiciel en fonction de différents critères. Ainsi sur la base de la nature de l’interaction avec une machine on distingue les logiciels systèmes\* des logiciels applicatifs (utilisés pour les applications spécifiques). Une autre distinction s’appuie sur les droits d’exploitation fixés par la licence du logiciel. On parlera alors de logiciels propriétaires et à l’inverse de logiciels libres Voir également *Open source*, *Freeware.*

**Logiciel système**

*(System software)*

Voir Système d’exploitation\*.

**Logiciel espion**

*(Spyware)*

Type de logiciel malveillant spécifique dont l’objectif est de recueillir des informations sur un équipement terminal cible. Le *spyware* utilise plusieurs vecteurs d’infection (*mail*, SMS, site Web) et s’installe sur une machine (il n’a pas vocation à se répliquer et infecter tout un réseau). Il procède alors à l’enregistrement des données qu’il recherche (frappes claviers, modification de fichiers) puis les retransmet vers le commanditaire de l’attaque (en utilisant un canal de communication disponible). Les données exfiltrées peuvent être au préalable chiffrées ou non. L’usage de ces logiciels est assez répandu et s’en procurer est globalement aisé. Certaines entreprises, ou particuliers, ont recours à ces logiciels pour surveiller leurs employés ou dans un usage privé (surveillance de conjoints voire d’enfants).

**Logiciel malveillant**

*(Malware)*

Un logiciel malveillant est un ensemble de programmes conçu par un pirate pour être implanté dans un système afin d’y déclencher une opération non autorisée ou d’en perturber le fonctionnement. On parle également de maliciel. Les virus et les vers sont deux types de logiciel malveillants[[157]](#footnote-158). On peut rajouter à cette liste les chevaux de Troie\* (ou *trojan).* L’histoire des logiciels malveillants est assez récente mais accompagne celle de l’informatique et des réseaux. En effet, dès les années 80, les premiers virus se répandent et commencent à être étudiés. On considère généralement que le premier virus développé pour endommager directement des données a été *Lehigh*, découvert en 1987 par une équipe de l’université de Pennsylvanie. La découverte de nouvelles souches de *malware* est une activité permanente et face à la multiplication des victimes et les gains potentiels générés, elle ne devrait pas décroitre. On estime ainsi à plusieurs millions par an le nombre souches nouvelles (2013 – 10 millions). Enfin, le développement rapide des usages de l’internet mobile favorise la création de nouveaux virus destinés aux téléphones mobiles. Pour l’année 2015, on estime que près de 4 500 virus Android\*[[158]](#footnote-159) sont détectés chaque jour[[159]](#footnote-160).

Voir Cheval de Troie, Virus, Ver.

***Pour aller plus loin***

Les logiciels malveillants sont développés dans le but de nuire à un système d’information, de bloquer ou de modifier des données. Ils s’appuient sur une charge\* virale (*payload*) pour produire un effet sur la cible. Il existe généralement trois types de logiciels malveillants : les chevaux de Troie\* (*trojan*), les vers\* et les virus\*.

**Les chevaux de Troie**

Il s’agit généralement d’un logiciel malveillant qui se dissimule dans une application saine afin de s’introduire dans le système cible. Une fois introduit dans le système, le cheval de Troie va ouvrir un canal de communication vers une plateforme extérieure afin de télécharger d’autres logiciels malveillants. Un cheval de Troie ne dispose pas de routine de propagation, il se diffuse par téléchargement ou par courrier électronique\*. L’entreprise de sécurité G-DATA propose la classification suivante pour les chevaux de Troie[[160]](#footnote-161) :

Les *backdoors*\* ouvrent une porte dérobée sur l'ordinateur infecté ;

Les *adwares\**, ou logiciels publicitaires, enregistrent les activités et les processus d'un ordinateur (habitudes de navigation, par exemple).

Les *spywares*, ou logiciels espions\*, permettent de voler des données utilisateur : mots de passe, documents, clés d'enregistrement de logiciels, adresses électroniques, etc. Les données sont recherchées sur les supports de données ou sont filtrées à partir du trafic réseau.

Les outils de téléchargement et les injecteurs (*Downloader* et *Dropper*) ont pour mission de charger ou de copier un fichier sur l'ordinateur infecté. Pour ce faire, ils tentent régulièrement de modifier ou de compromettre les paramètres de sécurité du système.

Les logiciels de numérotation (*Dialler*) utilisent la connexion par modem bas débit pour réaliser des appels vers des numéros surtaxés. Ces derniers ont disparus avec l’avènement du haut débit.

**Les Virus**

Les virus sont des programmes qui cherchent à se propager par l’intermédiaire d’autres programmes. On en distingue plusieurs types :

Les virus de secteur d’amorçage, virus MBR\* (*Master Boot Record*), s’installent avant le secteur d’amorçage du système, il est donc lu avant le secteur d’amorçage original lors du démarrage.

Les virus de fichiers : catégorie de virus localisés dans les fichiers exécutables. Le code du virus est exécuté lors du lancement du fichier.

Les virus multipartites : virus qui combinent les techniques d’infection du secteur d'amorçage (ou des tables de partitions) à celles utilisées sur les fichiers exécutables.

Les virus compagnon : virus qui ne modifient pas les fichiers exécutables mais utilisent leur exécution pour se lancer.

Les macrovirus : ces derniers utilisent un « langage macro », comme Visual Basic par exemple, ils ont donc besoin d’un interprète pour s’exécuter. Ils sont principalement intégrés dans un fichier bureautique et se répandent par e-mail.

Les virus furtif et *Rootkit*\* : virus dotés de mécanismes de protection spéciaux leur permettant d'échapper à la détection par les antivirus\*. Le but de ce type de virus est de rester indétectable afin de pouvoir utiliser les ressources de l’ordinateur infecté à l’insu de son utilisateur.

Les virus polymorphes\* : virus qui contiennent des mécanismes leur permettant de modifier leur aspect après chaque infection.

**Les vers\***

Catégorie de *malware* qui n’est pas attaché à un fichier exécutable mais qui se transmet par des connexions réseau ou entre ordinateurs. On distingue alors :

Le ver de réseau : qui analyse au sein d’un réseau informatique les ports\* des ordinateurs accessibles. Pour qu’une attaque soit possible, les vers exploitent des failles\* pour se propager. *Blatser (2003)* et *CodeRed* en sont des illustrations. Le ver *Sasser* (2004), comme *Blaster*, exploite une faille de sécurité du système d’exploitation Microsoft Windows et se propage automatiquement.

Le ver de messagerie : qui utilise les programmes de messagerie électronique pour se propager. *Sober* (2003) est un exemple de ver de messagerie qui envoyait une copie de lui-même en pièce jointe de courrier électronique.

Le ver de messagerie instantanée ou IRC\*: qui utilise les programmes de discussions instantanée pour se propager.

Le ver *Peer to peer*: vers qui, stockés sur les zones de partage des logiciels *peer to peer* (*Emule*, *BitTorent*), attendent simplement d’être téléchargés. Ils utilisent généralement des noms de fichiers très recherchés (film récents).

**Loguer**

*(to Log)*

Anglicisme qui désigne l’action d’enregistrer les évènements réseaux (donc de stocker les logs\*).

Voir Journalisation, Log.

**LSR** **– *Label Switching Router***

(Routeur de label)

Dans une architecture MPLS\*, le LSR est un équipement réseau dont la fonction est d’assurer le routage d’un paquet IP.

Voir MPLS.

**LTE – *Long Term Evolution***

LTE est une norme de téléphonie mobile, évolution de l’UMTS\*, elle est d’abord considérée comme appartenant à la troisième génération (3,9G). Spécifiée par le consortium 3GPP dans le *release* 8, elle ne peut prétendre à l’appellation 4G car elle ne remplit pas toutes les spécifications. Pour LTE le débit théorique descendant est d’environ 300 Mbit/s. LTE évolue rapidement et à partir de 2010, la LTE-*advanced* (3GPP *release* 10) est considérée comme une technologie 4G. Avec LTE-*advanced* le débit descendant atteint 1Gb/s théorique.

L’architecture du réseau LTE est divisée en deux parties distinctes :

• la partie accès radio : eUTRAN ;

• la partie cœur de réseau : *Evolved Packet Core EPC.*

# M

**MA – *Mobile Allocation***

(Allocation mobile)

Dans un réseau GSM\*, le *mobile allocation* (MA) correspond à la liste des numéros de fréquences qui sont utilisables pour le saut de fréquence.

**MAC – *Media Access Control***

(Contrôle d’accès au support)

Dans le modèle OSI\*, la couche MAC est la sous-couche basse de la couche 2 (liaison de données). Elle assure le contrôle de l’accès au support physique de communication. L’objectif des protocoles\* de la sous-couche MAC est de réguler les émissions de plusieurs stations sur un même support. Dans ce cadre, les protocoles de la sous-couche MAC doivent pouvoir détecter le début et la fin d’une trame\* (donc les mécanismes de séparation de trames). Plusieurs techniques existent dont notamment le bourrage d’octets et le bourrage de bits qui permettent d’identifier une série de bits spécifique en début et fin de trame.

Voir également Adresse MAC.

***Machine Learning***

(Apprentissage automatique)

Le *machine Learning* ou apprentissage automatique est un domaine d’étude et de recherche qui porte sur le développement de l’intelligence artificielle. Il s’agit de développer des algorithmes d’apprentissage qui permettent aux machines de remplir des tâches plus complexes. Le développement de ce champ de recherche est poussé par l’émergence du *big data\** qui rend possible l’analyse prédictive par l’exploitation d’une quantité suffisante de données.

**MAEC - *Malware Attribute Enumeration and Characterization***

MAEC est un langage standardisé pour la description et l’échange d’information sur les codes malveillants (*malware*). Il permet d’éliminer certaines limites de l’approche par signature uniquement. Projet développé par le MITRE\*, il fait parti des différents projets liés à la cybersécurité.

Voir STIX, CAPEC.

***Mail Harvesting***

(Moisson de courriels)

Action qui consiste à parcourir un grand nombre de ressources publiques (pages internet, groupes de discussion, etc.), afin d’y collecter les adresses électroniques avec des intentions malveillantes[[161]](#footnote-162).

**Maillage**

(*mesh*)

Désigne un modèle d’architecture de réseau qui repose sur la mise en relation des différents nœuds de sorte que chacun puisse accéder à n’importe lequel des autres. Ainsi plusieurs chemins (routes) sont toujours possibles pour relier deux nœuds distincts. Ce modèle d’architecture assure une meilleure sureté de fonctionnement car la transmission ne dépend pas exclusivement d’un lien unique. Il y a par ailleurs la possibilité de répartir la charge et de désengorger certains nœuds par une politique de routage adaptée.

Voir *Mesh Network.*

**MAIO – *Mobile Allocation Index Offset***

Dans un réseau GSM\*, le MAIO est le décalage qui permet à chaque mobile d’utiliser une série de fréquences différentes lors des sauts de fréquence.

***Malware***

(Logiciel malveillant)

Voir Logiciel malveillant.

**MAN - *Metropolitan Area Network***

(Réseau métropolitain)

Un MAN ou réseau métropolitain désigne un réseau de taille intermédiaire et dont la dimension s’étend jusqu’à la taille d’une ville ou d’une région.

***Man in the middle – MITM***

(Homme au milieu)

Catégorie d’attaque où une personne malveillante s’intercale dans un échange de manière transparente pour les utilisateurs ou les systèmes. De façon triviale, dans un échange entre Alice\* et Bob\*, Max\* se fait passer pour Alice auprès de Bob et pour Bob auprès d’Alice.

Remarques : La connexion est maintenue, soit en substituant les éléments transférés, soit en les réinjectant. Une attaque connue dans cette catégorie repose sur une compromission des tables ARP\* (ARP *Poisoning*). Contrer les attaques par le milieu est aussi l’un des objectifs des infrastructures de gestion de clés[[162]](#footnote-163).

***Manager* SNMP**

(Superviseur SNMP)

Logiciel de supervision et d’administration d’un réseau, SNMP permet d’interroger les équipements, de recueillir et de centraliser les informations. Ce logiciel est normalement installé sur une machine dédiée.

Voir SNMP.

**Marqueur (d’attaque)**

*(Indicator Of Compromise - IOC - Pattern)*

Ensemble de caractères de texte constituant la description technique d’une activité malveillante, destiné à la détection de cette dernière par un système de sécurité (IDS, *firewall*, antivirus). On utilise également les termes de marqueur d’activité malveillante ou marqueur de compromission.

***Pour aller plus loin***

Un marqueur s’applique généralement à une communication réseau, à un code binaire d’un exécutable, à une structure de fichiers, à la base de registre Windows, ou encore à un fichier numérique. Pour autant il peut être appliqué, en théorie, à tout ensemble de données numériques manipulées par un ordinateur.

Le marqueur seul est rarement suffisant pour détecter une activité malveillante, il est nécessaire de préciser le contexte d’application (ou le domaine) ainsi que d’autres paramètres (caractère de péremption du marqueur, type de code malveillant associé, etc.). Dans ce cadre, pour utiliser un marqueur en détection, il faut généralement comparer le marqueur à l’ensemble des éléments de son domaine d’application. Le motif est alors comparé à l’ensemble des données considérées. Lorsque le marqueur est trouvé, on parle de détection, de correspondance ou encore de *match* ou *hit*. Lorsque l’activité ainsi détectée ne se révèle pas être malveillante, on parlera de « faux positif ». Ainsi, la détection seule ne suffit pas, il convient de la qualifier (voir Qualification).

Les marqueurs sont, en général, regroupés suivant deux familles distinctes :

• les marqueurs réseau, qui caractérisent une activité réseau (flux, session\*, adresse IP\*, nom de domaine\*) ;

• les marqueurs systèmes, qui caractérisent une activité sur le système d’exploitation\* (chemin de fichier, chaine binaire d’un exécutable, création d’un jeton d’exclusion mutuelle, *hash* de contrôle MD5\* d’un exécutable, etc.).

Enfin, pour représenter les variations d’un marqueur, les motifs comportent régulièrement des caractères génériques de description (utilisant le plus souvant le standard d’écriture des expressions régulières/rationnelles de type POSIX – IEEE 1003.2).

Il existe de nombreuses initiatives de standardisation pour l’écriture des marqueurs au sein d’un système de sécurité donné (RFC\*5070, CyBOX, OpenIOC, etc.) mais aucune n’émerge comme standard commun.

**Matériel**

*(Hardware)*

Ensemble des éléments physiques d'un appareil informatique. On distingue les éléments de l’unité centrale des périphériques qui y sont reliés (clavier, souris, imprimantes). Ces éléments sont généralement des composants électroniques reliés sur des circuits imprimés. Ils présentent, comme les logiciels, des vulnérabilités exploitables par des attaquants et peuvent en outre faire l’objet d’un piégeage « à la source » par le constructeur pour se garantir un accès distant à un équipement.

**Max**

Masculin d’Eve\*.

Voir Bob, Alice.

**MBR – *Master Boot Record***

(Zone d’amorce – secteur d’amorçage)

Dans un disque dur, le MBR, ou secteur d’amorçage est le premier secteur adressable, il contient des informations essentielles pour le démarrage du système. C’est ce secteur que le BIOS\* va lire et exploiter lorsque la machine démarre. Il contient ainsi un programme qui va lire la table de partition du disque et déterminer celle qui est active (donc *bootable*). Le premier secteur de cette partition active va lui lire la première partie du système d’exploitation\* (placé sur la même partition) et le lancer. Le MBR regroupe les informations suivantes :

• Le code de démarrage (*boot code*) : partie qui est lue par le BIOS au démarrage et permet l’interprétation du reste du MBR ;

• Le volume d’octets (*bytes volume*) : il s’agit des quatre octets situés après le code de démarrage qui permettent d’identifier les volumes montables sur le disque ;

• La table de partition (*partition table*) : suite de 64 octets qui définissent au maximum quatre partitions du disque.

**MCC – *Mobile Country Code.***

Voir IMSI.

**MD5 - *Message Digest 5***

MD5 est un algorithme de hachage utilisé pour vérifier l’intégrité des données échangées ainsi que dans les mécanismes d’authentification. La fonction de hachage\* calcule une empreinte de fichier codé sur 128 bits. Le principe repose sur l’impossibilité de générer une collision, soit la certitude que les empreintes de deux fichiers différents seront elles-mêmes distinctes. MD5 est un algorithme créé en 1991 par Ronald Rivest, à partir de 2004, MD5 n’est plus considéré comme un algorithme sûr, il est progressivement remplacé par SHA\*-1. Toutefois, MD5 demeure utile pour vérifier rapidement l’intégrité d’un fichier téléchargé ou encore pour stocker les empreintes de mots de passe plutôt que les mots de passe en clair.

Voir Fonction de hachage, SHA.

***Mesh Network***

(Réseau maillé)

Dans un réseau maillé, tous les hôtes sont reliés aux autres en mode pair à pair\*. Un réseau maillé n’est pas hiérarchisé, chaque hôte dispose des mêmes droits, il reçoit et relaye les données. Ce type de topologie\* est particulièrement flexible (il permet d’accueillir de nouveaux hôtes aisément), résilient car les données peuvent toujours transiter même lorsqu’un lien est rompu. Pour assurer le routage\* au sein d’un réseau maillé, la RFC\* 3626 spécifie le protocole OLSR\* (*Optimized link state routing protocol)*.

Voir OLSR.

**Messagerie multimédia**  
*(Multimedia Messaging Service - MMS)*

Le service de messagerie multimédia est un système qui permet l’émission et la réception de messages multimédia sur un terminal mobile.

**Messagerie texte**

*(Short Message Service - SMS)*

Le service de messagerie SMS permet de transmettre de courts messages sous forme de texte entre terminaux mobiles utilisant la norme GSM\*. Le message est également appelé en France « texto ».

Voir SMS.

**Métadonnée**

*(Métadata)*

Ensemble de données structurées qui caractérise ou qui permet le traitement des données auxquelles elles sont associées.

Ainsi, à une donnée particulière, on peut associer l’horaire de sa création ou de sa modification. En matière de télécommunication, les métadonnées téléphoniques permettent d’associer à une communication, une durée d’appel, le numéro appelé et appelant, le type d’appareil terminal utilisé, etc.

**Metasploit**

Plateforme de tests d’intrusion qui regroupe de nombreuses fonctionnalités. Elle permet, par exemple, d’automatiser l’exploitation de vulnérabilités connues, de développer des exploits\*. Metasploit est le prolongement du projet *Backtrack*, il rassemble sur une base de données près de 300 exploits, 50 modules auxiliaires, 122 *payloads* (charge\*), 17 encodeurs. Le *Framework* Metasploit fait parti des outils utilisés par les auditeurs en sécurité des systèmes d’information, les consultants et les chercheurs.

**MGCF – *Media Gateway Control Function***

Equipement critique d’une architecture IMS\* (*IP Multimedia Subsystem)* le MGCF est une passerelle qui assure la conversion des flux d’origine diverse. Il permet donc d’échanger avec un réseau commuté classique comme avec des réseaux à commutation de paquets (à travers le MGW – *Media Gateway*).

**MIB (SNMP) – *Management Information Base***

Base de données\* contenant les informations nécessaires pour la gestion d’un équipement. MIB est stocké en local par chaque agent, il permet le dialogue SNMP entre l’agent et le manager\* SNMP.

Voir SNMP

**MIC - Modulation par Impulsions Codées**

*(PCM - Pulse Code Modulation)*

La modulation par impulsions codées est une technique de transmission qui permet de transmettre un signal analogique\* sous une forme numérique\*. La technique repose sur un échantillonnage du signal qui permet de le transformer en une suite d’impulsions binaires\*. Cette technique est utilisée en télécommunication pour transmettre des communications vocales en RTC\* ou VoIP\*.

Voir Fréquence, RTC, VoIP.

***Middleware***

(Intergiciel – Logiciel médiateur)

Au sein d’un même ordinateur, un *middleware* est un logiciel qui assure la mise en relation entre plusieurs logiciels de niveau différent. Ainsi, le *middleware* intervient entre les logiciels de haut niveau (applications) et de bas niveau (système d’exploitation). Au sein d’un système d’information plus vaste, ils permettent de lier des applications très diverses en implémentant des mécanismes d’échange de messages et d’appel de procédures à distance par exemple. Le Journal Officiel en donne la définition suivante : logiciel qui permet le fonctionnement de plusieurs ordinateurs en coordination, en attribuant à chacun une tâche spécifique, comme les échanges avec les utilisateurs, l’accès aux bases de données ou aux réseaux[[163]](#footnote-164).

**MIME – *Multipurpose Internet Mail Extensions***

MIME est un protocole\* de transfert de fichiers mis au point, dans un premier temps, pour étendre les possibilités de la messagerie Internet (limitée aux fichiers textes) vers l’usage de pièces jointes aux différents formats. Il est donc une extension de SMTP\*. MIME, standardisé par la RFC\* 1521 propose donc des méthodes de transfert, il structure le corps des messages et liste les différents contenus possibles (types).

**MIMO - *Multiple Input / Multiple Output***

Dans un réseau radio, la technologie MIMO a vu le jour afin d’optimiser les ressources. Avec l’augmentation des besoins de performance des réseaux liés au déploiement de nouvelles normes (UMTS\* – 4G), MIMO permet d’augmenter les débits en utilisant la diversité spatiale ainsi que des systèmes d’antennes multiples. Plusieurs antennes sont alors utilisées en émission sur une même fréquence. Les antennes réceptrices reçoivent, pour leur part, une combinaison de ces flux et les reconstituent (à l’aide de fonctions de traitement du signal).

**Mise à jour**

*(Upgrade)*

Action qui consiste à remplacer du matériel ou un logiciel par une version plus récente. Une mise à jour peut également se matérialiser par l’ajout d’un correctif sur un logiciel existant sans nécessairement le remplacer. On parle également de mise à niveau.

**MISO - *Multiple In / Single Out***.

Technologie dérivée du MIMO\* pour laquelle la station réceptrice ne dispose que d’une seule antenne. Voir MIMO.

**MITRE**

Organisme américaine à but non lucratif, le MITRE est un partenaire du gouvernement des Etats-Unis dans le domaine de la recherche, des nouvelles technologies, et des développements stratégiques. Issu du laboratoire d’informatique du *Massachusetts Institute of Technology* (MIT), le MITRE a été créé au mois de juillet 1958 afin de développer une stratégie gouvernementale dans les domaines technologiques en orientant ses travaux sur le secteur de la défense. Il a ainsi été à l’origine du développement du système de défense anti-aérien SAGE – *Semi Automatic Ground Environment*. L’organisme est aujourd’hui impliqué dans de nombreux programmes gouvernementaux en liens avec la cybersécurité.

**MNC – *Mobile Network Code***

Voir IMSI, GSM.

**MMF – *Multimode Fiber***

*(Fibre Multimode)*

Voir Fibre optique.

**MMS - *Multimedia Messaging Service***

(Service de Messagerie MultiMedia)

Voir Messagerie multimédia.

**MML – *Man Machine Language***

MML est un langage spécifique pour les interfaces\* de management des équipements de télécommunication. Il est standardisé par l’ITU-T Z.301 Z341. Chaque équipementier dispose de commandes spécifiques.

**MOA - Maitrise d'OuvrAge**

Personne morale pour laquelle l’ouvrage est construit. Il est en charge de spécifier le besoin, d’estimer la faisabilité et l’opportunité du projet. Il est donc responsable du contenu « fonctionnel » du projet et pilote sa conduite. La MOA s’appuie par la suite sur le ou les maîtres d’œuvre (MOE\*)

**MOE – Maitrise d’œuvre**

Personne de droit privé qui doit porter les réponses techniques, économiques ou architecturales à un projet.

**Mode connecté**

*(Connection oriented communication)*

Mode de transmission pour lequel, une session\* doit être établie entre le destinataire et l’émetteur. La liaison est libérée à la fin de la transmission. En mode connecté il y a donc un mécanisme spécifique d’ouverture et de fermeture de liaison et parfois un contrôle d’erreur. Le mode connecté s’applique par exemple dans les communications téléphoniques RTC dans un contexte circuit, ou encore pour le protocole TCP\* dans un contexte paquet.

Voir RTC, TCP.

**Mode de transfert asynchrone**

*(Asynchronous Transfer Mode – ATM)*

Protocole réseau de niveau 2 du modèle OSI\*. Il permet de multiplexer plusieurs flots de données sur un même lien. Un mode de transfert est une combinaison des mécanismes de multiplexage\* et de commutation au niveau d’un canal\* de transmission. Dans le cas d’ATM, les horloges de l’émetteur et du récepteur ne sont pas corrélées, les paquets\* accèdent au réseau de façon apériodique. Enfin, ATM est un protocole à commutation de cellule\*. Une cellule est un paquet court de taille fixe de 53 octets.

Voir Cellule.

**Mode de transmission asynchrone**

*(Asynchronus Transmission Mode - ATM)*

Mode de transmission de données dans lequel les horloges du récepteur et de l’émetteur sont indépendantes. Il est donc nécessaire de synchroniser l’horloge de réception au début de chaque transmission.

**Mode de transmission synchrone**

Mode de transmission inverse de l’ATM\* pour lequel l'horloge du récepteur est synchronisée avec celle de l'émetteur. Le mécanisme de synchronisation des horloges est effectué pour chaque bit transmis, il nécessite généralement de disposer d’un canal de synchronisation.

**Mode non connecté**

*(Connection Less Network Service)*

Le mode non connecté (également mode datagramme\*) est un mode de communication qui s’oppose au mode connecté\* (ou orienté connexion, pour lequel, une liaison doit être établie entre le destinataire et l’émetteur). En mode non connecté, les paquets\* circulent indépendamment les uns des autres, ils sont routés suivant une politique locale de routage\*. Le mode non connecté suppose par ailleurs des mécanismes de séquençage afin de pouvoir recombiner les blocs à l’arrivée. Il suppose également que des paquets peuvent être perdus et par conséquent la mise en place de mécanismes d’accusé de réception ou, à minima, de ré-expédition en cas de perte. Enfin il est nécessaire que chaque paquet dispose de l’adresse complète du destinataire. Pour autant, le mode non connecté présente de nombreux avantages, il optimise l’utilisation d’un réseau et permet d’alléger l’intelligence du réseau (qui se limite à transférer des paquets et à commuter). Les équipements terminaux sont alors chargés d’effectuer les contrôles et les réassemblage de message

**Modèle**

*(Template)*

Descriptif des propriétés communes à certains objets informatiques, qui peut servir de cadre de référence pour la création d’objets de même nature, notamment des documents[[164]](#footnote-165). Ainsi, un modèle de données décrit les différents champs et le format des données qui rempliront ces champs.

**Modem – Modulateur / démodulateur**

*(Modem)*

Un modem est un appareil qui assure la conversion des signaux numériques en signaux analogiques et inversement. Les *modem* RTC\* permettent par exemple d’établir une connexion Internet via le réseau téléphonique analogique.

**Modérateur**

*(Moderator)*

Un modérateur est une personne qui veille au respect de l’objet et du règlement des échanges de messages électroniques effectués dans un cadre organisé[[165]](#footnote-166). Le modérateur examine les articles et les échanges (ou commentaires) sur un forum ou un blog, par exemple, et peut interdire une publication ou exclure un membre.

**Modulation**

*(Modulation)*

En théorie du signal, la modulation est l’action qui consiste à modifier les caractéristiques d’une onde porteuse pour transmettre un message. On distingue plusieurs types de modulation :

• la modulation d’amplitude : qui consiste à faire varier l’amplitude de la porteuse ;

• la modulation de fréquence : pour laquelle c’est la fréquence d’oscillation de la porteuse qui variera dans le temps mais pas son amplitude ;

• la modulation de phase : dans ce cadre c’est la périodicité de la porteuse qui évoluera dans le temps.

**Modulation à spectre étalé**

*(Spread Spectrum modulation)*

Technique de transmission dans laquelle la puissance du signal émis est répartie sur une largeur de bande beaucoup plus grande que celle strictement nécessaire à la transmission des informations. La modulation à spectre étalé permet l’accès multiple à une voie de transmission et assure une protection accrue contre le bruit et le brouillage radioélectriques, ainsi que la confidentialité[[166]](#footnote-167).

**Moindre privilège (Principe de)**

Le principe de moindre privilège est un principe de sécurité informatique qui veut que les utilisateurs et les processus doivent accéder aux ressources avec le minimum de privilège qui leur permettent de conduire les actions explicitement autorisées.

Le pendant de ce principe et qu’un attaquant cherchera toujours à augmenter ses privilèges (jusqu’à devenir *root*).

**Moore - Loi de Moore**

La loi de Moore stipule que le nombre de transistors intégrés dans une puce (de même taille), à prix constant, doublera tous les deux ans. Cette affirmation de Gordon Moore date de 1965, elle a été revue (passant d’un doublement tout les deux ans à dix huit mois) et élargie aux ordinateurs. Elle se formule comme suit : la puissance de calcul d’un ordinateur, à prix constant, doublera tous les dix huit mois (augmentera donc de façon exponentielle). Si cette « loi », établie de façon empirique, se révèle globalement vrai, il existe des limites physiques à son développement (notamment la taille de l’atome). Gordon Moore estimait ainsi, en 1997, que cette augmentation s’infléchirait en 2017.

**MOSPF - *Multicast extension Open Shortest Path First***

Extension du Protocole de routage OSPF\*. La spécificité de MOSPF réside dans la diffusion d’information *multicast*\* dans l’annonce de l’état de lien OSPF. S’appuyant sur l’algortithme de Dijkstra\* pour le calcul du plus court chemin, MOSPF effectue un calcul séparé pour les chemins entre la source et les différents groupes identifiés (multicast). MOSPF est essentiel pour router des paquets IP\* multicast (pour le multimédia par exemple), il permet aux routeurs de diffuser les groupes auxquels ils appartiennent. MOSPF est décrit dans la RFC\* 1584 – 1585.

Voir également OSPF.

**Moteur de recherche**

*(Search engine)*

Système d’exploitation de banque de données\* permettant d’accéder à des ressources (pages, sites, etc.) à partir de mots clés. Il existe de nombreux moteurs de recherche, le plus courant demeure Google\* avec plus de 70% de recherches mondiales. Son succès repose sur sa capacité à indexer rapidement des contenus (donc à les rendre accessibles) mais également sur son algorithme de recherche (notamment *Page rank*). Le moteur chinois *Baidu* est également très utilisé (en raison du nombre croissant d’internautes en Chine). Il existe en outre des moteurs de recherche qui insistent sur le respect de la vie privé et la non traçabilité de l’internaute. C’est le cas de *Startpage* par exemple (qui en plus utilise SSL\* par défaut et propose d’utiliser des proxy\* pour consulter les pages) ou encore *DuckDuckgo*. En France, *Qwant* est une initiative récente qui tente de briser le quasi monopole de Google et offre une interface de recherche complète (incluant les réseaux sociaux par exemple).

**Motif**

*(Pattern)*

Voir Marqueur (d’attaque).

**MPLS - *MultiProtocole Label Switching***

MPLS est un protocole qui améliore la gestion du trafic de flux de plusieurs types (dans les infrastructures des opérateurs), il permet ainsi d’assurer la qualité de service\* (QoS) de bout en bout. Il optimise la bande passante\* et permet d’établir des réseaux privés virtuels (VPN\*). MPLS permet d’améliorer la performance des différents équipements de routage sur les grands réseaux sans modification matérielle. Dans l’architecture OSI\*, MPLS est indépendant des protocoles de couche 2 et 3 (il intervient entre les deux), il interagit avec les protocoles de routage existant (OSPF\*, RSVP\*). MPLS supporte les couches de niveau 2 des réseaux IP\*, ATM\* et Frame Relay\*. Le protocole est décrit dans la RFC\* 3031.

Le principe du protocole MPLS est d’établir les conditions d’une commutation orientée connexion\*. Dans ce cadre, le protocole détermine pour un trafic particulier un « label\* », une étiquette pour chaque voie. Chaque paquet\* va donc recevoir un préfixe qui sera interprété par les routeurs du réseau. La transmission de données s’effectue selon des LSP\* (*Label Switched Paths)*  et des FEC *(Forwarding Equivalent Class).* Les données transitent dans les LER (*Label Edge Router)* et les LSR (*Label Switching Router).*

**MSC - *Mobile service Switching Centre***

Le MSC ou Centre de commutation radio mobile est un équipement réseau qui assure l’interface entre le système radio et le réseau téléphonique fixe (RTC\*). Voir GSM.

**MSIN – *Mobile Subscriber Identification Number***

Voir IMSI.

**MSISDN - *Mobile station ISDN number***

*(Numéro ISDN de station mobile)*

Le MSISDN est le numéro de téléphone international d'un abonné mobile.

**MTA - *Message Transfer Agent***

MTA désigne, dans la norme X400 de messagerie électronique, un agent (entité logicielle) en charge de l’acheminement des messages entre les agents utilisateurs.

**MTBF - *Mean Time Between Failure***

(Temps Moyen Entre Panne – TMEP)

Le MTBF d’un équipement est une valeur théorique donnée à titre indicatif par les constructeurs permettant d’estimer le temps moyens entre deux pannes lors d’un fonctionnement de l’équipement dans des conditions optimales.

**MTS - *Message Transfer System***

Le MTS désigne l’ensemble des *Message Transfer Agent (MTA\*)* appartenant à un même domaine.

Voir MTA.

**MTU – *Maximum Transmission Unit***

(Unité de transmission maximale)

La MTU correspond à la taille maximale d’un paquet\* pouvant être acheminé sans être fragmenté (on parle alors de *link MTU)*. Elle est exprimée en octets. La MTU de chemin (*path MTU)* désigne le plus petit MTU de liaison de l’ensemble des MTU composants un chemin entre une source et une destination. Le MTU Ethernet\* est de 1500 octets, il est de 1468 octets sur ADSL\*.

***Multicast***

(Diffusion groupée)

En télécommunication, le *multicast* est un mode de diffusion qui permet d’envoyer les mêmes informations à tous les membres d’un groupe.

Voir *Unicast* et *Broadcast*.

**Multiplex**

*(Multiplex)*

Mode de transmission dans lequel une même voie de communication permet de transmettre des signaux indépendants assemblés (et pouvant être reconstitués) sous la forme d’un seul signal.

**Multiplexage**

*(Multiplexing)*

Action d’assembler des signaux indépendants en un seul signal composite à partir duquel ils peuvent être restitués[[167]](#footnote-168).

**MVNO - *Mobile Virtual Network Operator***

(Opérateur Virtuel Mobile)

Un MVNO est un opérateur mobile qui sous-traite la gestion et le déploiement de son réseau à un autre opérateur. Il peut être limité géographiquement, avoir une offre commerciale distincte ou cibler une catégorie particulière de clients. Généralement un MVNO ne possède qu’une partie des éléments réseau et des infrastructures d’un opérateur classique, il peut parfois limiter son activité à la diffusion de carte SIM\* et entièrement sous-traiter la partie réseau.

**Mystification**  
*(Spoofing)*

Technique qui consiste à modifier les données d'un utilisateur ou d'un programme (le plus souvent, une adresse). On peut ainsi utiliser cette technique pour remplacer l’adresse IP\* de l’expéditeur d’un paquet, cette falsification de la source a été notamment utilisée dans les attaques par déni de service\*. Le *spoofing* d’adresse permet également de bénéficier de la relation de confiance entre deux machines pour prendre la main sur l’une d’entre-elle. La mystification est donc possible à différents niveaux protocolaires (ARP\* *spoofing*, IP *spoofing*, etc.).

# N

1. **NAC - *Network Access Control***
2. Un NAC est un ensemble de méthodes qui contribuent au contrôle d’accès au réseau. Une solution NAC en entreprise repose ainsi sur des outils de sécurité connus (authentification\*, politique de sécurité utilisateur) mais doit apporter une solution de contrôle d’accès distants, imposer des règles de sécurité différenciées selon les réseaux et utilisateurs et enfin mettre à jour les postes clients et éventuellement les nettoyer.
3. La gestion des différents profils s’opère par l’intermédiaire d’un annuaire qui sera interrogé par les différents équipements sollicités dans le cadre du contrôle d’accès (en premier lieu le pare-feux). Il existe plusieurs appellations et solutions en fonction des constructeurs. Voir ainsi *l’United Acces Control* UAC\* de Juniper, le *Network Access Protection* NAP\* de Microsoft et *Secure Network Access* de Nortel.
4. ***Name Service Switch – NSS***
5. En informatique, le mécanisme de *Name Service Switch* permet de gérer l’accès aux bases de données centralisées de configurations. Ainsi, sous Linux, le NSS est configuré sous /etc/nsswitch.conf, fichier qui regroupe les différentes bases de données accessibles (*password*, *netgroup*, *hosts*\*).
6. **NAP – *Network Access Protection***
7. (Protection d’accès réseau)
8. *Network Access Protection* est une solution Microsoft qui assure les fonctions de NAC\*.
9. **Pour aller plus loin…**
10. Le laboratoire de Microsoft présente le NAP comme une technologie permettant de vérifier si les ordinateurs qui se connectent au réseau satisfont aux conditions requises définies par l'administrateur. Si un ordinateur ne remplit pas les conditions, il peut être isolé temporairement dans un réseau, dit de quarantaine.
11. Ce réseau de quarantaine peut contenir les ressources nécessaires pour mettre à jour les ordinateurs, comme, par exemple, des correctifs de sécurité pour Windows XP ou encore des signatures de virus\* pour l'antivirus\*, afin que le client puisse mettre en œuvre les conditions requises pour avoir un accès total au réseau de l'entreprise.
12. La technologie NAP comporte trois aspects :
13. Tout d'abord la validation de la stratégie de réseau. Lorsqu'un ordinateur tente de se connecter au réseau **l'état de l'ordinateur** est vérifié pour savoir s'il est conforme aux stratégies d'accès au réseau définies par l'administrateur. Si un ordinateur n'est pas conforme, il y a deux solutions. Dans un environnement de surveillance, tous les ordinateurs ont accès au réseau même ceux non conformes aux stratégies d'accès, cependant l'état de conformité de chaque ordinateur est inscrite dans un journal. Dans un environnement d'isolement, les ordinateurs conformes ont un accès total au réseau et les autres sont isolés dans un réseau de quarantaine jusqu'à ce qu'ils deviennent conformes aux stratégies d'accès au réseau. L'administrateur peut dans les deux environnements configurer des exceptions au processus de validation.
14. Le deuxième aspect est la **conformité aux stratégies de réseau.** L'administrateur peut mettre à jour automatiquement les ordinateurs qui ne sont pas conformes aux stratégies d'accès au réseau en mettant en place un logiciel d'administration comme par exemple *Microsoft System Management Server* (SMS). Il existe ici aussi deux solutions.
15. Dans un environnement de surveillance les ordinateurs qui ne sont pas conformes aux stratégies d'accès ont tout de même un accès au réseau sans avoir fais les mises à jours et les configurations nécessaires. Dans un environnement d'isolement les ordinateurs qui ne sont pas conformes aux stratégies d'accès au réseau sont isolés dans un réseau de quarantaine qui leur permettra de faire les mises à jour nécessaires pour être conformes. Dans ce deuxième aspect, l'administrateur peut aussi faire des exceptions.
16. Enfin, le dernier aspect est **l'isolement vis à vis du réseau**. Lors d'une connexion, un ordinateur qui n'est pas conformes aux stratégies d'accès réseau peut être isolé dans un réseau de quarantaine. Cet accès permet, selon la configuration de l'administrateur, à l'ordinateur d'être dans un réseau limité pour pouvoir accéder à des ressources. Si l'administrateur ne permet pas à un ordinateur non conforme d'accéder à des ressources, celui-ci restera dans ce réseau isolé pendant toute la durée de la connexion. Cependant s'il permet à l'ordinateur connecté au réseau de quarantaine d'accéder à des ressources de mise à jour, l'ordinateur pourra se connecter au réseau total de l'entreprise[[168]](#footnote-169).
17. **NAS - *Network Access Server***
18. Un *Network Access Server* est un équipement utilisé par les fournisseurs d’accès à Internet (FAI\*) afin de transformer des communications téléphoniques en flux IP en assurant l’interface entre le réseau commuté et le réseau de transport de données[[169]](#footnote-170). Le NAS est composé de différents modem\* analogiques et numériques. Cet équipement assure le maintien de la communication pendant une session\* utilisateur.
19. **NAS - *Network Attached Storage***
20. (Serveur de stockage réseau)
21. Un NAS est un serveur de stockage de fichiers, considéré comme un support de stockage de masse habituel (on parle également de « volume de stockage »), accessible depuis le réseau et disposant souvent d’une importante capacité. Il permet le stockage centralisé pour l’ensemble des clients. Il suffit à l’administrateur de définir des volumes logiques et des autorisations de partage. Le volume est généralement accessible via plusieurs protocoles (SMB\* - *Server Message Block* / CIFS - *Common Internet File System*, AFP - *Apple Filing Protocol* et NFS - *Network File System*). Les OS\* des NAS gèrent des disques RAID, fournissent les systèmes de fichiers réseau adaptés et gèrent l’authentification\* des clients. Les NAS sont très répandus dans les entreprises et se développent chez les particuliers offrant la possibilité de stocker et partager des fichiers multimédias volumineux.
22. **NAT - *Network Address Translation***
23. (Traduction d'adresse réseau)
24. Le NAT est un mécanisme qui consiste à convertir une adresse IP\* d’un espace d’adressage en une autre. Le NAT permet ainsi de fournir à un poste de travail d’un intranet une adresse IP différente sur Internet. Cette « *translation*» d’adresse permet de séparer les adresses privées (sur un intranet – non routables) des adresses publiques. Appliqué par un routeur, le NAT permet un accès internet à plusieurs stations avec un nombre limité d’adresse IP. La plupart des pare-feu et des routeurs permettent à plusieurs machines de partager une seule adresse IP publique. Le NAT permet de diminuer sensiblement le nombre d’adresse IP uniques nécessaires (ce qui est critique pour l’IPv4 avec la pénurie d’adresses) et masque les adresses internes (ce qui améliore la sécurité en rendant moins vulnérables les stations vis à vis d’une attaque directe depuis l’extérieur). L’identification des connexions se fait alors par le biais des ports\* source / destination.
25. **NAT- PT - *Network Address Translation - Protocol Trans­lator***
26. Le NAT-PT est un mécanisme de traduction des adresses IPv6 en adresses IPv4. Ce mécanisme sera nécessaire tant que les deux systèmes d’adressage coexisteront. Toutefois, dans une architecture IPv6, le NAT n’est pas conseillé et d’ailleurs pas utile car le nombre d’adresses disponibles permet de servir chaque équipement connecté.
27. **Navigateur**
28. *(Browser - Web browser)*
29. Le navigateur est une application informatique qui permet la navigation sur le Web, et notamment l’accès à des serveurs HTTP\* Il permet à un utilisateur de disposer d’un affichage graphique des pages et assure la navigation par lien hypertexte\* (clic). On y trouve généralement un système d’onglets, une barre de menus, une barre d’outils et une barre d’adresse. La fonction principale du navigateur est donc d’assurer la consultation de ressources internet, il doit interpréter du code HTML\* *HyperText Markup Language* pour avoir le texte de la page et y associer la feuille de style en cascade (CSS\*) pour la mise en page. Pour visualiser à quoi ressemble une page Web sans un navigateur, effectuer un clic droit sur une page et sélectionner l’option « afficher code source ».
31. **NBMA – *Non Broadcast Multiple Access***
32. NBMA est une famille de réseaux qui n’offrent pas une diffusion au niveau physique (comme sur un réseau Ethernet\* par exemple). On trouve ainsi dans la famille NBMA les réseaux ATM\*, *Frame Relay*\*, GPRS, X.25\*…
33. **Netbios - *Network Basic Input Output System***
34. Netbios est un progiciel développé par IBM et utilisé par Microsoft. Il permet l’interface entre des systèmes d’exploitation MS-DOS et les applications de gestion des échanges entre plusieurs clients en réseau local. C’est donc un système de nommage qui permet l’établissement de sessions\*. Une méthode d’encapsulation Netbios dans des paquets TCP\* et UDP est décrite par les RFC 1001 et 1002, certains ports\* sont alors réservés à des services *Netbios over TCP/IP*.
35. On retrouve ainsi :
36. • Sur le port\* 135, service de localisation utilisé pour les appels de procédure à distance (RPC – *Remote Procedure Call*);
37. • Port 137, le *Netbios Name Service* (ns), service d’association d’un nom d’ordinateur à une adresse IP ;
38. • Port 138, le *Netbios datagram service* (dgm), permet l’échange de message en mode non connecté ;
39. • Port 139, le *Netbios Session* *Service* (ssn), permet l’échange de message en mode connecté.
40. **Nétiquette**
41. La nétiquette ou étiquette du net est un ensemble informel de règles de bonne conduite sur Internet. Sans formalisme, ces « règles » relèvent plus du bon usage et constituent un véritable marqueur social. Le respect, ou pas, de ces règles non écrites permet à ceux qui en connaissent les clés de lecture de reconnaître les membres d’un groupe particulier. Il est à noter qu’une RFC a tenté une spécification (RFC 1855) et propose par exemple des règles comme ne pas propager de *hoax*\* ou ne pas utiliser les *smiley* dans les mails…
42. ***Netware***
43. Système d’exploitation\* développé par Novell et dédié aux serveurs PC. Il a été supplanté par son conçurent Windows NT. L'administration des ressources comme les imprimantes, les fichiers et les utilisateurs, est alors possible depuis un client avec les privilèges administrateur. A partir de la version 6, NetWare 6, il n'est plus nécessaire de disposer d'un client, et la configuration peut alors être effectuée depuis le serveur[[170]](#footnote-171).
44. Le système n’est plus soutenu depuis 2010. Netware repose sur une pile protocolaire propriétaire (Novell) qui regroupe :
45. • RIP\* – *Routing Information Protocol*, qui assure l’échange des information de routage ;
46. • IPX\* – *Internetwork Packet eXchange*, protocole de la couche 3 du modèle OSI\* ;
47. • SPX – *Sequenced Packet eXchnage*, protocole de la couche 4 (orienté connexion) ;
48. • SAP – *Service Advertising Protocol*.
49. Voir RIP, IPX.
50. **NFC - *Near Field Communication***
51. (Communication dans un champ proche)
52. Technologie radio qui permet l’échange de données à très courte distance (quelques centimètres). Le NFC permet la communication entre un émetteur et une cible « passive », c’est à dire n’assurant pas elle-même son alimentation électrique. Il existe de nombreuses applications de la technologie NFC comme le paiement sans contact (carte bancaire NFC), ou encore les cartes d’accès sans contact et autre *pass* de transport.
53. **NFS - *Network File System***
54. Protocole permettant l’utilisation de ressources partagées sur un réseau de stations de travail qui utilisent le système d’exploitation UNIX et Linux. Développé en 1984 par *Sun Microsystems*, NFC est aujourd’hui largement utilisé et s’impose comme un standard. Le système de fichiers permet ainsi l’échange et le partage sur la plupart des systèmes d’exploitation\* (OS). La version 4 du protocole fait l’objet de la RFC\* 3530. Elle marque une rupture car elle est développée spécifiquement pour les usages Internet. NFSv4 intègre, par exemple, la négociation des paramètres de sécurité entre client et serveur, la possibilité de chiffrer les communications, une maintenance simplifiée, des mécanismes de reprise d’incidents et supporte plusieurs protocoles de transport.
55. **NIC - *Network Information Center***
56. Historiquement, organismes responsables du maintien de la « racine » d’Internet. Les NIC administraient les DNS\* racine et également les domaines de premier niveau, *Top Level Domain* TLD. Aujourd’hui cette fonction dépend de l’IANA\* et des registres de noms de domaine comme l’AFNIC\*.
57. Voir Registre Internet Régionaux - RIR
58. **NIC – *Network Interface card***
59. Voir Carte réseau.
60. **NIS - *Network Information Services***
61. Protocole\* réseau développé pour centraliser l’administration des systèmes UNIX. NIS est ainsi un système client\* - serveur\* qui permet à un groupe de machines (d’un même domaine\* NIS) de partager des fichiers de configuration. L’information est distribuée, et l’architecture repose sur le protocole *Remote Procedure Call* (RPC) pour transmettre les fichiers de configuration vers les machines hôtes. Le NIS utilise un système de nom de domaine\* (géré par un serveur primaire).
62. **NIST - *National Institute of Standards and Technology***
63. Agence gouvernementale américaine, qui dépend du département du commerce - DoC, en charge de l’établissement des normes techniques à l'échelle nationale. Plusieurs normes du NIST ont été largement adoptées à l’échelle mondiale.
64. **NMS - *Network Management System***
65. (Système de gestion de réseau)
66. Un NMS, comme son nom l’indique, est un système qui permet de contrôler le fonctionnement courant d’un réseau. Il assure le suivi des utilisations système, des configurations et la sécurité (par la détection d’erreurs par exemple). Un NMS est donc un ensemble logiciel et matériel qui concourt à la supervision d’un ensemble de composants individuels d’un réseau donné.
67. **NNI - *Network to Network Interface***
68. (Interface réseau à réseau)
69. Le NNI est une interface\* physique entre (au moins) deux réseaux qui définit le processus de gestion de la signalisation\*. Ainsi, un circuit NNI sera utilisé pour interconnecter la signalisation\* (exemple SS7\*) entre réseaux distincts. Dans une architecture MPLS\*, le NNI est utilisé pour interconnecter les routeurs de cœur de réseau d’opérateurs.
70. Voir UNI - *User to Network Interface*, MPLS.
71. **NNTP - *Network News Transfert Protocol***
72. Protocole\* réseau de gestion des transferts de messages des groupes de discussion USENET. NNTP, spécifié par la RFC\* 3977, est un protocole simple créé en 1986 (donc avant le Web) pour gérer la distribution des messages d’un *newsgroup*. Il assure le dialogue entre les serveurs et les outils de lecture de *newsgroup* et fonctionne généralement en écoute sur le port\* 119 ou 563.
73. **Noeud**
74. *(Node)*
75. Un nœud dans un réseau est un lieu où convergent des voies de transmission. Ce point particulier est en charge de commuter les voies pour assurer la transmission de messages. Cette fonction est généralement effectuée par un équipement physique (routeur\*, commutateur).
76. **Nœud de raccordement d’abonnés – NRA**
77. Voir NRA.
78. **Nœud de Transit International - NTI**
79. Commutateur qui permettait la connexion du réseau national Transpac\* aux réseaux étrangers de transmission par paquets\* conformes à la norme X 25\*. X.25 a été progressivement abandonné au profit de protocoles supportant des vitesses de transfert plus importantes. L’arrivée de l’IP a marqué la fin de ce protocole.
80. Voir Transpac et X.25
81. **Nom de domaine**
82. *(Domain name)*
83. Dans le système DNS\*, un nom de domaine est l’identifiant d’un domaine particulier. Un domaine appartient à une personne physique ou une organisation, le nom de domaine est alors une suite alphanumérique qui se termine par le suffixe indiquant le domaine de premier niveau (TLD\*).
84. On parle alors de *Fully Qualified Domain Name –* FQDN.
85. Voir DNS, TLD.
86. **Nommage**
87. *(Naming)*
88. Attribution de noms identifiant des éléments d’un réseau ou des utilisateurs. Dans l’internet, l’attribution d’un nom de domaine à un organisme utilisateur est une opération de nommage.
89. Voir ICANN, DNS.
90. **Non-répudiation**
91. *(Non-repudiation)*
92. En France, selon l’Instruction Générale Interministérielle 1300, la non-répudiation consiste en l’impossibilité de nier la participation au traitement d’une information. Cette caractéristique (en général cryptographique) permet, par exemple, d’empêcher qu’un expéditeur puisse ultérieurement nier avoir envoyé un message.
93. **Normalisation**
94. Activité qui vise à produire des normes\*. En France, c’est l’AFNOR\*, Association française de normalisation, qui produit des normes, le CEN, Comité Européen de Normalisation, au niveau européen et l’ISO\* sur le plan international.
95. **Norme**
96. Document qui définit des exigences, des spécifications, des lignes directrices ou des caractéristiques à utiliser systématiquement pour assurer l’aptitude à l’emploi des matériaux, produits, processus et services.
97. **NRA - Nœud de Raccordement d’Abonné**
98. Le NRA est un central téléphonique proche du central qui dessert les lignes d’abonnés d’un périmètre défini. Dans un NRA on trouve un répartiteur qui permet de trier les lignes d’abonnés pour les envoyer ensuite vers les DSLAM\* (*Digital Subscriber Line Multiplexer)* des FAI\*[[171]](#footnote-172).
99. **NRO - Nœud de Raccordement Optique**
100. Dans un réseau fibre optique pour particulier de type FTTH - *Fiber To The Home*, le nœud de raccordement optique désigne le local où convergent les arrivées de fibres optiques des abonnés. C’est l’équivalent pour la fibre du NRA\*.
101. Voir NRA.
102. **NSA - *National Security Agency***
103. Agence gouvernementale américaine chargée du renseignement d’origine technique. Elle est responsable du renseignement d’origine électromagnétique (ROEM), de sa collecte et de son traitement mais également de la sécurité des systèmes d’information gouvernementaux (*Information Assurance*). Créée en 1952, l’agence est demeurée extrêmement discrète et son existence a été dévoilée tardivement (1957). L’importance du secret trouve son origine dans « la guerre des codes » de la seconde guerre mondiale où les états-majors ont parfaitement intégré l’intérêt de percer à jour les codes adverses tout en s’appuyant sur de la cryptographie robuste. Les effectifs de l’agence seraient d’environ 40 000 employés. Depuis les révélations d’Edward Snowden (2013), ancien consultant de la NSA, sur les programmes de surveillance de masse de l’Internet, l’agence est au cœur de nombreuses polémiques.
104. **NSAP - *Network Service Access Point***
105. Dans les réseaux ATM\*, le NSAP est l’équivalent de l’adresse IP\* utilisée par le protocole Internet. Le NSAP est défini par le standard ISO/IEC 8348 comme une adresse de 20 octets. Outre ATM, on retrouve le NSAP dans les technologies X.25\*, *Frame* *Relay*\*, IS-IS\*.
106. **NSS - *Network Sub System***
107. Dans un réseau GSM\*, le NSS est le sous-système d’acheminement des données. Il est composé des HLR\*, MSC\* et VLR\*.
108. Voir GSM.
109. **NSS – *Network Security Services***
110. Ensemble de librairies conçues pour le développement multi- plateformes d’applications s’appuyant sur des mécanismes cryptographiques. Les applications construites avec NSS peuvent supporter SSL\* v2 et v3, TLS\*, PKCS\* #5, PKCS #7, PKCS #11, PKCS #12, S/MIME\*, les certificats X.509 v3, et d'autres standards de sécurité[[172]](#footnote-173) (signature, chiffrement, authentification).
111. **NTP – *Network Time Protocol***
112. Protocole\* qui permet la distribution de l’heure sur un réseau. Il fonctionne suivant un mode client\*–serveur\*, chaque équipement réseau doit alors interroger un serveur NTP afin d’obtenir l’heure et mettre à jour son horloge. La version 3 du protocole est décrite dans la RFC\* 1305. NTP repose sur une « architecture » de serveurs hiérarchisés comprenant des serveurs primaires (strate 1) et des serveurs secondaires (strate 2). Cette organisation permet la diffusion de l’heure de façon verticale (de strate 1 vers strate 2 et postes clients) mais également de proche en proche (au sein d’une même strate). Des messages NTP sont donc échangés régulièrement sur un réseau, ils utilisent le protocole de transport UDP sur le port\*123.
113. **Numérique**
114. *(Digital)*
115. Le mot numérique désigne un nombre croissant de phénomènes associés aux technologies de l’information et de la communication (révolution numérique, entreprise numérique, etc.). En France le terme *digital* est régulièrement employé mais il s’agit d’un anglicisme impropre à proscrire. En télécommunications, un signal numérique est un signal qui n’est décrit que par une succession limitée de valeurs, choisies dans un ensemble fini (on parle de parle de signal discret, par opposition à un signal continu, qui lui est décrit par une succession infinie de valeurs). On parle de signal binaire\*, lorsque le signal numérique ne peut prendre que deux valeurs. La représentation de phénomènes physiques par un signal numérique a été rendue nécessaire par l’informatique, qui *in fine*, ne manipule que des états binaires. Un signal numérique s’oppose à un signal analogique\*, qui lui est un signal continu. La transformation d’un signal analogique en signal numérique (numérisation\*) nécessite un échantillonnage\*, car afin de transformer un signal continu en signal discret, il faut choisir un nombre limité de valeurs parmi l’infinité de valeurs du signal continu.
116. Voir Analogique, Shannon (Théorème), Échantillonnage, Numérisation.
117. **Numérisation**
118. *(Digitizing)*
119. Action qui consiste à convertir un signal analogique\* en un signal numérique\*. Pour ce faire deux actions sont nécessaires, il faut dans un premier temps échantillonner\* le signal (action qui consiste à prélever de façon périodique un échantillon du signal analogique source) puis, dans un deuxième temps de quantifier\* les échantillons (action qui consiste à affecter une valeur numérique aux échantillons prélevés).
120. De façon plus classique, le terme est utilisé pour désigner toutes les transformations organisationnelles et fonctionnelles liées au déploiement des nouvelles technologies de l’information et de la communication.
121. Voir Echantillonnage, Quantification.
122. **Numérisation de l’espace de bataille - NEB**
123. La NEB regroupe, dans les armées françaises, un ensemble de mesures techniques et organisationnelles visant à utiliser au mieux les capacités des nouvelles technologies dans la conduite du combat. L’objectif est de relier les acteurs tactiques et les systèmes de commandement au sein d’un système d’information commun permettant l’échange rapide d’information, d’ordres etc.

# O

**Obfuscation**

*(Obfuscation)*

Technique de programmation qui vise à rendre le code\* difficilement compréhensible par un opérateur humain mais qui demeure compilable. Cette technique permet de protéger un code des tentatives de rétro ingénierie\*. Elle permet d’améliorer la sécurité et contribue à garantir la propriété intellectuelle des développeurs.

Voir Rétro ingénierie.

**Objectif de sécurité**

Un objectif de sécurité formalise, dans le cadre de la méthode EBIOS\* (Expression des besoins et identification des objectifs de sécurité), la décision de traiter un risque selon des modalités prescrites.

Voir également EBIOS (méthode).

**OBL - Opérateur de Boucle Locale**

Opérateur\* de télécommunication qui déploie les infrastructures qui assurent le raccordement d’un abonné à la boucle locale\*. Cette activité regroupe ainsi les lignes d’abonnés et les équipements de commutation.

**Octet**  
*(Byte)*

En informatique, l’octet est une unité de mesure de l’information numérique. Un octet est un ensemble organisé de huit éléments binaires (bits).

**OFDM - *Orthogonal Frequency Division Multiplexing***

(Multiplexage par répartition autonome de fréquence)

Technologie de multiplexage\* qui consiste à transmettre les données de manière simultanées sur plusieurs porteuses modulées. Cette technologie de modulation permet d’augmenter le débit, elle est donc utilisée largement dans les technologies « haut débit ».

Voir Multiplexage.

***Off-line***

(Hors ligne)

Le mode *off-line* désigne un mode de fonctionnement autonome d’un équipement sans être relié au réseau. Il s’oppose au mode *on-line* qui en outre qualifie le fait d’être présent sur le réseau c’est à dire identifié et connecté.

**OIV – Opérateur d’importance vitale**

*(Critical infrastructure)*

La notion d’opérateur d’importance vitale est une notion de droit français qui précise les opérateurs publics ou privés dont l’activité contribue directement au potentiel de la Nation. L’article R. 1332-1 du code de la défense précise que les opérateurs d’importance vitale sont désignés parmi les opérateurs publics ou privés mentionnés à l’article L. 1332-1 du même code, ou parmi les gestionnaires d’établissements mentionnés à l’article L. 1332-2. Le terme est souvent traduit par *critical infrastructure* mais celui-ci s’avère beaucoup moins précis et semble avoir un périmètre assez variable. Le glossaire de l’ANSSI présente alors un OIV comme, un opérateur qui exerce des activités mentionnées à l’article R. 1332-2 et comprises dans un secteur d’activités d’importance vitale ; gère ou utilise au titre de cette activité un ou des établissements ou ouvrages, une ou des installations dont le dommage ou l’indisponibilité ou la destruction par suite d’un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement d’obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou de mettre gravement en cause la santé ou la vie de la population.

**OLSR - *Optimized Link State Routing Protocol***

Protocole de routage\* spécifique des réseaux maillés\*. Il est décrit dans la RFC 3626. Comme son nom l’indique il s’agit d’un protocole à « état de liens » (Voir Algorithme de routage à état de liaison). Ainsi, chaque nœud diffuse un message spécifique (type *Hello*) dans lequel figure les informations sur son voisinage et l’état des liaisons. Une des spécificités de OLSR repose sur l’introduction du concept de relai multipoints (MPR – *MultiPoint Relay*) afin d’éviter les phénomènes d’inondations (saturation des nœuds par les messages de tous le réseau). Chaque nœud choisit dans son voisinage un ensemble de nœuds vers qui il retransmet les messages. Ce mécanisme permet donc d’éviter la double retransmission vers un même nœud.

Voir Routage.

**OMG - *Object Management Group***

L’*Object Management Group* est une association internationale (de droit américain) dont l’objectif est de faire émerger des standards\* afin de favoriser l’interopérabilité entre des applications orientées objets développés indépendamment. Elle regroupe plus de 800 membres, utilisateurs, concepteurs, producteurs de logiciels, institutionnels etc. L’OMG est, par exemple, à l’origine du standard UML\* - *Unified Modeling Language*.

***Open source***

Les systèmes dit « *open source*» sont des applications pour lesquelles les licences respectent les critères de *l’open source initiative* (libre redistribution et accès au code source). Ils diffèrent des « *freewares*» ou logiciels libres pour qui le code source est libre d’accès, de distribution et de modification.

**Opérande**

Voir Opérateur (informatique).

**Opérateur**

*(Operator)*

En France le Code des postes et des télécommunications désigne par le terme « opérateur », toute personne physique ou morale qui exploite un réseau de communications électroniques ouvert au public ou qui fournit au public un service de communication électronique.

En programmation informatique, l’opérateur est un des deux éléments essentiels d’une instruction (action de spécifier au processeur l’action à réaliser). Une instruction est composée d’un opérateur (action à effectuer) et une ou des opérandes (les données sur lesquelles s’applique l’opérateur). Il existe plusieurs types d’opérateurs :

• Opérateurs arithmétiques : addition, soustraction ;

• Opérateurs de comparaison : supérieur à, inférieur à, égal à ;

• Opérateurs logiques : vrai, faux, et, ou ;

• Opérateurs conditionnels : si, sinon…

**Opération d’information**

Les opérations d’information sont constituées par l’ensemble des actions menées par les forces armées, dirigées et coordonnées au plus haut niveau, visant à utiliser ou à défendre l’information, les systèmes d’information et les processus décisionnels, pour appuyer une stratégie d’influence et contribuer, dans le cadre des opérations, à l’atteinte de l’état final recherché, en respectant les valeurs défendues[[173]](#footnote-174).

**Opération militaire d’influence**

Les opérations militaires d’influence (OMI) regroupent l’ensemble des activités dont l’objet est d’obtenir un effet sur les comportements d’individus, de groupes ou d’organisations (info cibles) afin de contribuer à l’atteinte des objectifs politiques et militaires. Elles se caractérisent par la volonté de l’action efficace sur autrui par des moyens qui ne font pas nécessairement appel à l’usage de la force ou à l’exercice de l’autorité. Fonction coordonnée par les Opérations d’Information (O.I.), les OMI mettent en œuvre des médias spécifiques ou non aux forces armées. Elles réalisent des actions conçues principalement aux niveaux stratégique ou opératif. Elles sont conduites le plus souvent au niveau tactique. Elles s’inscrivent dans la durée. Elles délivrent des messages ou des signaux crédibles, adaptés aux spécificités culturelles et linguistiques des info cibles. (DIA 3.10)

**Ordinateur quantique**

*(Quantum processing)*

Les ordinateurs actuels fonctionnent à l’aide de processeurs qui utilisent des transistors qui ne gèrent que deux états (0 ou 1). Le principe de l’ordinateur quantique est d’utiliser une des propriétés de la matière subatomique révélée par la physique quantique : l’intrication. Ce phénomène, que nous ne détaillerons pas ici, permet de « lier » des particules distantes dans des états quantiques identiques. Appliqués à l’informatique les propriétés des particules permettent ainsi de ne plus se limiter à la gestion de deux états mais plusieurs. En informatique classique l’information est stockée dans un bit (qui n’a que deux états 0 ou 1), en informatique quantique on fait appel au qubit ou Qbit qui est en fait une superposition d’états (0 et 1). Le Qbit peut donc prendre « plusieurs » valeurs, 0, 1 ou une superposition des deux… (il est ici utile de rappeler que l’un des pères de la physique quantique, Niels Bohr, disait : « Quiconque n'est pas choqué par la théorie quantique ne la comprend pas. »).

Cette particularité s’avère très utile en informatique et permettrait d’augmenter très significativement les capacités de calcul de nos ordinateurs. Ce point est essentiel notamment pour la cryptanalyse. Si le modèle théorique permet d’envisager l’ordinateur quantique, la réalité se heurte encore aux difficultés de réalisation. Des expériences concluantes ont pu avoir lieu et ce segment de recherche est aujourd’hui très développé.

L’ordinateur quantique promet de révolutionner en profondeur de nombreux pans de l’informatique, que ce soit en termes d’algorithmique, ou de protection de l’information.

**OSI (modèle) – *Open System Interconnexion***

Le modèle OSI (*Open System Interconnexion*) est une représentation fonctionnelle des niveaux de communication entre ordinateurs (équipement réseau). Il décrit donc les fonctionnalités et l’organisation nécessaires à l’établissement d’une communication distante. La norme est référencée dans l’ISO 7498 « Modèle basique de référence pour l’interconnexion des systèmes ouverts ». L’architecture proposée se décline suivant sept couches fonctionnelles différentes présentées dans le tableau ci-dessous.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Couche** | **Fonction** | **Protocoles** | **Type de données** | **Commentaire** |
| Application  7 | Accès aux services réseaux | SSH-FTP-SNMP-HTTP | données | Couches hautes |
| Présentation  6 | Conversion des données machine en données exploitables | SMB-ASCII-SSP |
| Session  5 | Gère les sessions entre différentes applications | NetBIOS AppleTalk |
| Transport  4 | Connexion de bout en bout, contrôle de flux | TCP-UDP-SCTP-DCCP-SPX | Segments |
| Réseau  3 | Détermination du cheminement des données, adressage logique | IP-OSPF-BGP | Paquets ou datagrammes | Couches basses |
| Liaison de données  2 | Adressage physique (MAC) | Ethernet-X25-HDLC-ATM | Trames |
| Physique  1 | Transmission du signal (binaire) | Wifi | Bits |

Le modèle OSI qui date de 1984 est pourtant plus récent que celui que l’on rencontre massivement aujourd’hui et communément appelé modèle Internet (en fait modèle TCP/IP\*) qui lui ne regroupe que quatre couches :

Physique ;

Réseau ;

Transport ;

Services.

Voir TCP/IP.

**OSI – *Open Source Initiative***

L’*Open Source Initiative* est une association dont l’objectif est la défense et la promotion des logiciels *open source\**.

Voir *Open source.*

**OSPF – *Open Shortest Path First***

Protocole de routage\* à état de liens\*, décrit par la RFC\* 2328, OSPF est adapté au réseau de grande taille, il utilise l’algorithme *Shortest Path First, SPF.* Chaque routeur calcule ainsi de façon autonome les informations de routage. Développé au début des années 90, OSPF est un protocole de la famille IGP\* - *Interior Gateway Protocol* interopérable. En outre, OSPF utilise un système *d’area* ou de *zone* qui permet de regrouper les routeurs au sein de mêmes entités logiques. Il succède au protocole RIP\* qui avait atteint ses limites en raison de l’expansion des réseaux :

• RIP est limité à 15 sauts ;

• RIP ne supporte pas les masques à longueur variables (VLSM\* – *Variable Length Subnet Mask)*;

• L’envoi régulier des tables de routage entières consomme une grande quantité de bande passante ;

• RIP converge plus lentement qu’OSPF ;

• RIP ne prend pas en compte les paramètres de délai et de coût (le routage est basé sur le nombre de sauts) ;

• Les réseaux RIP sont des réseaux plats (pas de concepts de zones ou *area)*.

Caractéristiques du protocole :

• Les routeurs OSPF entretiennent une relation orientée connexion avec les routeurs d’un même segment physique (on parle d’adjacence *- adjency* ou de contiguïté) ;

• Lors d’un changement de topologie\* réseau, OSPF n’envoie qu’une mise à jour incrémentielle ;

• OSPF n’est pas limité par une segmentation dépendante de l’adressage IP\* ou des sous-réseaux, il utilise la notion d’*area* pour désigner un groupe de routeurs ;

• OSPF supporte le VLSM - *Variable-Length Subnet Mask*, et la *summarization* manuelle des routes ;

• La communication inter-routeurs est efficace (possibilité de donner des rôles particuliers) ;

• OSPF permet une communication *inter-area* mais il demeure un protocole de routage intérieur (IGP)[[174]](#footnote-175).

Le protocole a été adapté pour effectuer de la multi diffusion. MOSPF - *Multicast Open Shortest Path First* est spécifié dans la RFC 1585.

**OSS - *Operating System and Service***

(Sous système d’exploitation et de maintenance)

Dans un réseau mobile GSM\* on retrouve trois sous systèmes : Le sous système radio *Base Station Sub system - BSS*\* ;

Le sous système réseau *Network Switching Sub system - NSS\* ;*

Le sous système d’exploitation *Operating System and Service* ou *Operation Support Sub system.*

L’OSS assure la gestion et la supervision du réseau afin de maintenir le niveau de service spécifié. La norme GSM définit les fonctions d’administration suivantes :

• Administration commerciale (déclaration des abonnés, mobiles, facturation) ;

• Gestion de la sécurité ;

• Gestion de la charge du réseau ;

• Contrôle de configuration du système (mises à jour) ;

• Maintenance.

**OTP – *One Time Pad***

(Masque jetable)

Algorithme de chiffrement théoriquement impossible à casser. Le principe est extrêmement simple, il consiste généralement à effectuer un XOR\* entre le message à chiffrer et un masque aléatoire de même longueur. Cette technique demeure toutefois difficile à implémenter car, le masque doit être réellement aléatoire (ce qui n’est pas le cas s’il est créé par un logiciel), le masque ne peut servir qu’une seule fois, il doit être de la même longueur que le message (ce qui peut être assez long). Enfin, cette technique, comme le chiffrement symétrique\*, nécessite que le destinataire du message dispose également du masque pour pouvoir le déchiffrer.

Voir Chiffrement, Cryptographie, XOR.

# P

**PABX - *Private Automatic Branch Exchange***

(Autocommutateur téléphonique privé)

Un autocommutateur privé est utilisé pour effectuer la gestion des communications téléphoniques au sein d’une structure en liaison avec le réseau public. Il est communément appelé le « standard » ou « central téléphonique ». Il assure de façon automatique la gestion des appels. Avec le déploiement de la téléphonie IP, les PABX sont remplacés par des IPBX\* ou PCBX. Par simplification l’usage veut que l’on parle aujourd’hui de PBX.

**Page d'accueil**

*(Home page)*

La page d'accueil d’un site Web est la page qui sera affichée par défaut lors de l’accès au site. Elle correspond à la vitrine principale du site et offre des options de navigation à l’internaute.

**Pair à pair**

*(Peer to peer – P2P)*

Un réseau P2P est un modèle d’architecture où chaque machine est à la fois serveur\* et client\*. Cette facilité permet ainsi l’échange de fichiers entre ordinateurs membres du réseau en évitant la surcharge d’un seul serveur et en optimisant la bande passante\* disponible. La participation à un réseau P2P nécessite d’installer sur la machine un logiciel dédié (ex emule, bitTorrent, µ-torrent etc.). Ces réseaux sont largement critiqués car ils ont été utilisés pour l’échange de fichiers (audio – vidéo) soumis au droit d’auteur. Pour autant, les échanges de pair à pair sont essentiels pour le partage libre de logiciels ou de productions spécifiques. La terminologie française retient également le terme : poste à poste.

**PAN – *Personal Area Network***

Catégorie de réseau centrée sur un individu et permettant l’interconnexion de ses équipements personnels (ordinateur, tablette, voiture, etc.). Un PAN a une portée inférieure à 10 mètres. Les PAN répondent au standard de la famille IEEE 802.15. Lorsqu’il est sans fil, le PAN est désigné WPAN *- Wireless Personal Network*.

Voir *Body Area Network*, *Bluetooth*.

**PAP - *Password Authentication Protocol***

(Protocole d’authentification par mot de passe)

PAP est un protocole\* d’authentification\* par mot de passe extrêmement simple à implémenter. Le principe repose sur l’échange du couple identifiant – mot de passe. En revanche, PAP ne chiffre pas les échanges (identifiant et mot de passe circulent en clair sur le réseau) il doit donc être réservé à un usage sur un réseau sécurisé. PAP a été initialement développé comme système d’authentification dans PPP\* *Point to Point Protocol* présenté dans la RFC\* 1334 puis sa dernière version 1661.

**Paquet**

*(Packet)*

Un paquet est un ensemble d’information véhiculé dans un réseau. Il comporte des données à transmettre ainsi que des informations permettant son traitement (adresses source et destination). En règle générale un paquet est de longueur fixe et représente l’unité de base sur la couche réseau du modèle OSI\*.

Voir Routage, modèle OSI, TCP.

**Pare-feu**

*(Firewall)*

Voir *Firewall*.

**Parité**

Dans les systèmes de transmission binaires, le signal peut être dégradé et subir des erreurs. Il est donc nécessaire de contrôler la validité d’un message reçu. La parité est un des systèmes le plus simple de contrôle d’erreurs, appelé également contrôle de parité ou *Vertical Redundancy Check VRC,* il consiste à ajouter un bit supplémentaire à un nombre de bits de données (appelé mot de code). De façon classique, le mot de code est à sept bits ce qui permet d’atteindre une taille d’un octet avec le bit de parité. La technique consiste à ajouter un bit à 1 si le nombre de bits du mot de code est impair et un bit à 0 si pair.

**Passerelle**

*(Gateway)*

Voir *Gateway.*

***Payload***

(Charge utile – Charge active)

Expression issue du vocabulaire militaire, une charge désigne la partie active d’une arme ou d’un explosif. Par analogie, le *payload* d’un logiciel malveillant\* (*malware*)représente la partie active du code qui sera utilisée par l’attaquant pour produire un effet sur sa cible. Dans le contexte du *Framework\* Metasploit\**, par exemple, un *payload* est un code que l’attaquant veut faire exécuter par le système et qui sera sélectionné et délivré par le *Framework*. Par exemple, un *reverse shell* est un *payload* qui créé une connexion depuis la machine cible vers l’attaquant[[175]](#footnote-176).

Dans un message, véhiculé par un réseau, il représente les données à transporter, indépendamment des informations liées à son transport.

Voir Logiciel malveillant.

**PBX - *Private Branch Exchange***

Voir PABX.

**P-CSCF - *Proxy Call Session Control Fonction***

Dans une architecture IMS\*, le P-CSCF est un serveur qui permet d’identifier les types d’appel entrants, il est en charge de la facturation. Le P-CSCF est le premier point de contact entre un terminal et le réseau, il valide et transmet les requêtes des usagers.

Voir IMS.

**PDN - *Public Data Network***

(Réseau public de transmission de données)

Un PDN est un réseau public pour la transmission de données, il peut être orienté circuit ou à commutation de paquets\*. Le PDN garantit en général une bande passante\* aux usagers.

***Peering***

(Appairage)

Voir Appairage.

**Périmètre d’audit**

Environnement physique, logique et organisationnel dans lequel se trouve le système d’information ou la portion du système d’information, sur lequel l’audit est effectué[[176]](#footnote-177).

Voir Audit, Preuve d’audit, Prestataire d’audit.

**Permutation**

*(Swap)*

Processus qui consiste à échanger le contenu d’une zone de mémoire principale avec le contenu d’une zone de mémoire auxiliaire[[177]](#footnote-178).

**PGP - *Pretty Good Privacy***

Système de chiffrement permettant d’utiliser le RSA\* sur des ordinateurs particuliers. Développé par Philip Zimerman à partir de 1984, PGP s’est imposé progressivement et a donné lieu à de nombreuses variantes (Open PGP, GnuPG). PGP garantit la confidentialité des échanges (chiffrement) ainsi que l’authentification\* (certificat et signature).

**PHP – *Hypertext Preprocessor***

Langage de programmation orienté objet\*, avec un syntaxe proche du langage C, PHP est principalement utilisé pour générer des pages Web dynamiques (pages Web générée à la demande). Il est donc le plus souvent utilisé côté serveur, sur un serveur HTTP\*. Ce dernier interprète le code PHP pour générer du code HTML\* de la page Web demandée.

***Phreaker***

Terme anglais composé par l’apposition des mots *phone* (téléphone) et *freak* (bête curieuse, marginal – terme lié à la contre culture américaine) pour désigner les personnes cherchant à pirater les réseaux téléphoniques RTC\*. Le but est de pouvoir téléphoner à moindre frais (communications internationales facturées en local, communications non facturées…). Avec le développement des réseaux mobiles et de la téléphonie sur IP, l’intérêt décroît et le terme est moins utilisé.

**Phénomène viral**

*(Going viral)*

Voir *Buzz*. Un phénomène viral est un contenu Internet qui se propage rapidement par l’intermédiaire des réseaux sociaux, *microbloging*, site d’échange et messagerie électronique.

***Phishing***

(Hameçonnage)

Voir Hameçonnage.

**Physique (couche)**

*(Physical layer)*

Voir Couche physique.

**Picoréseau**

*(Piconet)*

Mini-réseau qui se créé de façon automatique lorsque plusieurs périphériques *Bluetooth\** sont dans un même rayon de portée radio. Le picoréseau est organisé suivant une topologie\* en étoile dans le modèle maître – esclave.

Voir Topologie.

**Pièce jointe**

*(Attachment)*

Document ou fichier annexé au corps d’un message électronique[[178]](#footnote-179).

***Piggyback***

Technique d’acquittement\* de message dans laquelle l’acquittement d’un bloc de données est transmis en même temps que le bloc de données suivant. Cette technique permet d’optimiser le nombre de messages transmis et donc le débit.

**Pilote de périphérique**

*(Driver)*

Un pilote de périphérique (*driver*) est un logiciel\* qui permet la gestion des échanges entre un ordinateur et un périphérique (imprimante, appareil photo, etc.).

**PIN - *Personnal Identification Number***

Code de 4 à 8 chiffres qui verrouille l’utilisation d’un téléphone mobile. Le code PIN est associé à une carte SIM\*.

**Ping**

En informatique, *ping* est une commande qui permet de tester l’accessibilité d’une machine sur le réseau (en spécifiant son adresse IP\*). Si la machine cible est accessible, la commande renvoi en retour la durée de trajet entre les deux machines. Cette durée est également appelée *Round Trip Time (RTT\*).*

**Exemple** de retour de commande *ping* sur l’adresse IP\* de *google* 74.125.133.94 (trois premières séquences).

PING 74.125.133.94 (74.125.133.94): 56 data bytes

64 bytes from 74.125.133.94: icmp\_seq=0 ttl=45 time=113.607 ms

64 bytes from 74.125.133.94: icmp\_seq=1 ttl=45 time=62.358 ms

64 bytes from 74.125.133.94: icmp\_seq=2 ttl=45 time=47.420 ms

***Ping of Death***

(Ping de la mort)

Le *ping of death* est un type d’attaque informatique qui consiste à envoyer un paquet\* *ping* particulier vers une cible. Cette attaque est une des premières attaques réseau connue et exploite une vulnérabilité aujourd’hui corrigée sur la pile TCP/IP\* sous licence BSD, présente sur la plupart des OS. Elle consiste à envoyer un paquet\* IP dont la taille excède la taille autorisée (65536 octets) et provoque ainsi un plantage de la machine cible.

**Piratage**

*(Piracy)*

Terme impropre qui peut désigner toute forme d’attaque de système d’information. Pour autant, l’usage du terme s’est développé pour définir les atteintes aux droits de propriété intellectuelle et aux droits d’auteurs. Ainsi, on parlera d’un film « piraté » pour souligner le fait qu’il s’agit d’une copie illégale d’une œuvre protégée. Pirater, c’est alors copier ou échanger des fichiers normalement protégés par des droits particuliers. Cela n’a rien à voir avec du *hacking*.

Voir *Hack, Hacker.*

**Pirate informatique**

*(Hacker)*

Voir Hacker.

**PKI - *Public Key Infrastructure***

(Infrastructure à clés publique - ICP)

Dans un système d’information, une PKI ou ICP est une architecture globale qui permet de gérer les technologies de chiffrement et de signature électronique\*.

Une ICP permet ainsi, l’émission de certificats\* numériques, la création et la distribution de paires de clés publiques et privés. L’architecture comprend :

• Une autorité de certification\* (CA) ;

• Une autorité d’enregistrement (RA) : pour la création des certificats et la vérification d’identité des utilisateurs ;

• Une autorité de dépôt (*Repository)* pour le stockage des certificats ;

• Une entité qui génère les clefs (sur un site sécurisé ou le poste client);

• L’entité finale *(End Entity)* qui est l’utilisateur du service.

Il peut exister également une entité de séquestre qui stocke une copie des clés privées afin de permettre le déchiffrement des communications dans certaines conditions (fixées par la Loi).

**PKCS - *Public Key Cryptography Standard***

(Standards de cryptographie à clé publique)

Les PKCS sont un ensemble de standards développés par la société RSA\*. Leader dans le domaine de la cryptographie à clé publique, à l’origine de plusieurs algorithmes, RSA a développé un corpus définissant les différentes méthodes de chiffrement\* et de signature\*, l’échange de clés Diffie-Hellman\* [PKCS #3], les formats de requêtes pour l’obtention d’un certificat vers une autorité de certification [PKCS #10], etc. Plusieurs documents font l’objet de RFC\* pour leur usage Internet.

**Plan de continuité d’activité – PCA**

Ensemble de mesures visant à assurer, selon divers scénarios de crises, y compris face à des chocs extrêmes, le maintien, le cas échéant de façon temporaire selon un mode dégradé, des prestations de services essentielles de l’entreprise, puis la reprise planifiée de ses activités[[179]](#footnote-180).

Voir Plan de Reprise d’Activité – PRA.

**Plan de numérotation**

*(Numbering Plan)*

Ensemble de règles qui permettent d'attribuer à chaque abonné d'un réseau un numéro d'appel unique.

**Plan de reprise d’activité – PRA**

Le PRA est un ensemble de mesures qui permet la reprise d’activité totale ou en mode dégradé après une interruption. Il se distingue du plan de continuité d’activité\* PCA car ce dernier ne supporte pas d’interruption.

**PLMN - *Public Land Mobile Network***

(Réseau Mobile Terrestre Public)

Réseau qui permet d’accéder à des services de communication en situation de mobilité. Un PLMN est exploité par un opérateur de téléphonie mobile.

**PMR - *Professional Mobile Radio***

(Réseaux radio mobiles professionnels)

Un PMR est un réseau radio mobile à usage professionnel, il est donc indépendant et fonctionne sur des bandes de fréquence du service mobile. Il est distinct des réseaux mobiles ouverts au public. En 2013, l’ANFR\* gérait 25793 réseaux PMR[[180]](#footnote-181). La même agence souligne de nombreuses utilisations correspondant à des flottes de terminaux de type talkie-walkie en communication directe ou avec une infrastructure locale limitée.

* Installations mises en œuvre par exemple par de petites entreprises.
* Fourniture essentiellement de services de voix.

Quelques réseaux d’ampleur régionale, parfois nationale, avec une architecture s’appuyant sur un  nombre significatif de stations de base.

* Technologies numériques de type TETRA, TETRAPOL ou GSM-R.
* Fourniture de services de voix et d’échange de données.

**PNNI - *Private Network Network Interface* (ATM)**

Protocole de routage\* à état de lien utilisé dans les réseaux ATM\*. Il définit les mécanismes de routage et de signalisation\* entre les nœuds du réseau.

**Point d'accès**

*(Access Point)*

Un point d’accès est un équipement réseau qui assure la connexion physique avec l’équipement terminal. Ce lien physique peut être filaire ou non. Ainsi, un *hub* (concentrateur), un *Switch* (commutateur) et une borne Wi-Fi sont des points d’accès. En outre, le point d’accès peut également effectuer des opérations de routage (il fournit en général une adresse IP\* à l’équipement terminal). Enfin, le point d’accès peut partager les adresses IP entre plusieurs équipements :

* soit séquentiellement en effectuant des allocations dynamiques d'adresses IP aux machines lorsqu'elles se connectent effectivement (cas des serveurs de modem) ;
* soit simultanément en réalisant de la traduction (NAT\*) d'adresse IP (cas des routeurs Wi-Fi)[[181]](#footnote-182).

**Point à point**

*(Point to point)*

Une liaison point à point désigne une liaison connectant uniquement deux équipements distincts.

Voir PPP – Point to Point Protocol.

**Point de code**

(*Code point*)

Voir UTF, Unicode.

**Pointeur**

*(Pointer)*

En informatique, un pointeur est une donnée qui permet de retrouver l’adressage d’un groupe de données[[182]](#footnote-183). Dans un langage de programmation, le pointeur est une variable qui contient une adresse mémoire.

**Politique de sécurité de système d’information - PSSI**

*(Security Policy)*

Ensemble formalisé des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection du (des) système(s) d’information de l’organisme[[183]](#footnote-184).

**Politique en matière de protection des renseignements personnels**

*(Privacy Policy)*

Énoncé lié à la collecte, le stockage ou l'utilisation de renseignements personnels.

**Polymorphe**

*(Polymorphic)*

Se dit d’un ver ou d’un virus dont le code est chiffré, changeant le code de déchiffrement d’une infection à l’autre, et donc l’apparence et/ou la signature[[184]](#footnote-185).

Voir Virus polymorphe, Logiciel malveillant.

***Polling***

(Scrutation)

Méthode de transmission dans laquelle un équipement de contrôle assure la gestion des émissions par des « invitation à émettre ». L’équipement scrute l’état du réseau et procède à ces invitations.

Voir Invitation à émettre.

**Pont**

*(Bridge)*

Un pont est un dispositif d’interconnexion entre réseau dont l’unique fonction est d’assurer le transit des trames\*. Le pont intervient au niveau 2 du modèle OSI\*, il peut interconnecter des réseaux très hétérogènes et assurer le filtre d’adresses, ne laissant passer que les trames adressées aux dispositifs distants.

**PoP - *Point of Presence***

(Point de Présence)

Un point de présence (IP) est une infrastructure technique du réseau d’un opérateur qui abrite les équipements nécessaires à l’interconnexion des réseaux locaux à l’Internet.

**POP3 - *Post Office Protocol* 3**

POP est un protocole de gestion du courrier électronique décrit dans la RFC\* 1939. Il assure la récupération du courrier sur le serveur de messagerie et son rapatriement vers le poste client. POP3\* utilise une connexion TCP\* sur le port\* 110.

Voir Courrier électronique\*.

**Port**

*(Port)*

Dans une architecture TCP/IP\*, un port est une adresse codée sur 16 bits qui est allouée à une application particulière sur une machine. En effet, l’ordinateur doit pouvoir identifier les différentes sources de données entrantes lorsque sont effectuées plusieurs tâches en parallèle (relève du courrier, navigation, connexion FTP\*). Ainsi, sur une machine il existe plusieurs milliers de ports (65536) dont certains sont attribués à des applications spécifiques.

Les *well known ports* (ports reconnus) de 0 à 1023, réservés aux processus système ou aux programmes exécutés par des utilisateurs privilégiés. De 1024 à 49151 les *registered ports* puis de 49152 à 65535 des ports dynamiques ou privés.

|  |  |
| --- | --- |
| **Port** | **Service** |
| 20 – 21 | FTP |
| 22 | SSH Secure Shell |
| 23 | Telnet |
| 25 | SMTP |
| 53 | Domain Name System |
| 88 | Kerberos |
| 110 | POP 3 |
| 137 | Netbios-ns |
| 161 | SNMP |
| 194 | IRC |
| 443 | HTTPS |
| 995 | POP 3 sécurisé |
| 2164 | Dynamic DNS |

La combinaison d’une adresse IP\* et d’un numéro de port est appelé *socket*.

Sur le plan physique, un port (d’ordinateur par exemple) est un accès qui permet la connexion d’un périphérique (imprimante, micro, disque dur externe). On rencontre ainsi des ports USB\*, *firewire*, HDMI, Ethernet\*…

**Portabilité**

Pour un logiciel, un système ou un langage de programmation, la portabilité désigne la possibilité de pouvoir fonctionner sur des architectures différentes.

En téléphonie, la portabilité (d’un numéro de téléphone) désigne la possibilité pour l’abonné de conserver son numéro lorsqu’il change d’opérateur.

**Porte dérobée**

*(Backdoor)*

Voir *Backdoor.*

**Porteuse**

*(Carrier)*

Oscillation périodique dont on fait varier une grandeur caractéristique suivant les informations à transmettre. En général l’amplitude, la phase ou la fréquence sont les grandeurs utilisées.

**Pourriel**

*(Spam)*

Message électronique non sollicité généralement publicitaire. Le pourriel est l’équivalent numérique du prospectus glissé dans une boîte aux lettres.

**PPP - *Point to Point Protocol***

PPP est un protocole standardisé par la RFC\* 1661 qui assure le transport de datagrammes\* multi-protocoles sur une liaison point à point\*. PPP définit également un protocole de commande de liaison (LCP – *Link Control Protocol*) qui permet l’établissement, la configuration et la vérification de la liaison de données ainsi qu’une famille de protocole de commande réseau (NCP - *Network Control Protocol*) pour l’établissement et la configuration des différents protocoles de la couche 3 (couche réseau du modèle OSI\*). Le protocole a été conçu pour les liaisons simples qui transportent des paquets\* entre deux homologues. Ces liaisons permettent un fonctionnement bidirectionnel simultané, et sont supposées livrer les paquets dans l’ordre. L’intention est que PPP fournisse une solution commune pour la connexion facile d’hôtes, ponts et routeurs très divers [RFC1547][[185]](#footnote-186). PPP est utilisé comme protocole d’accès distant entre deux machines pour l’établissement de liaisons sécurisées.

Voir PPTP.

**PPTP - *Point-to-Point Tunneling Protocol***

PPTP est un protocole\* de liaison point à point par établissement d’un tunnel. Utilisant l’encapsulation PPP sur IP, il a été développé et soutenu par *Microsoft* pour la mise en œuvre de VPN\* à partir de machine sous un système d’exploitation *Windows*. PPTP est un protocole de niveau 2 (couche liaison du modèle OSI) qui encapsule des trames PPP\* (le protocole permet le chiffrement des données et la compression). *Microsoft* présente le fonctionnement de PPTP comme suit :

La plupart des sessions\* PPTP sont démarrées par un client\* appelant le serveur d'accès réseau d'un ISP. Le protocole PPP est utilisé pour créer la connexion *dial-up* entre le client et le serveur d'accès réseau et accomplit les fonctions suivantes :

* Etablir et terminer la connexion physique

Le protocole PPP utilise une séquence définie par la RFC\* 1661 pour établir et maintenir des connexions entre des ordinateurs distants.

* Authentifier des utilisateurs.

Les clients PPTP sont authentifiés en utilisant le protocole PPP.

* Créer des datagrammes PPP qui contiennent des paquets « cryptés » IPX, NetBEUI ou TCP/IP.

PPP créé des datagrammes qui contiennent un ou plus paquets de données « cryptés » TCP/IP, IPX ou NetBEUI.[[186]](#footnote-187).

**Prestataire d’audit**

Organisme réalisant des prestations d’audit de la sécurité des systèmes d’information[[187]](#footnote-188).

Voir Audit, Critère d’audit.

**Preuves d’audit**

Enregistrements, énoncés de faits ou autres informations qui se rapportent aux critères d’audit\* et sont vérifiables[[188]](#footnote-189).

**Preuve numérique**

*(Digital proof)*

Avec la dématérialisation de nombreux actes, la question de la preuve numérique a rapidement émergé. En France, le Code civil précise dans l’article 1316-1 que l’écrit sous forme électronique ne vaut preuve qu’à la double condition que son auteur puisse être dûment identifié et qu’il soit établi et conservé dans des conditions de nature à en garantir l’intégrité. Reste encore à garantir l’intégrité…

Ainsi, un jugement du Tribunal de Grande Instance de Paris (TGI) du 10 avril 2013, démontre, par exemple, que l’impression d’une capture d’écran ne constitue pas une preuve suffisante pour établir la réalité d’une publication dans une affaire de diffamation en ligne.

**PRI - *Primary Rate Interface***

Le PRI est l’interface de raccordement au réseau numérique (RNIS\*) d’une capacité de 30 canaux B à 64 Kbits/s, un canal de signalisation et un canal D à 64 Kbits/s également.

Voir Accès primaire.

**Principe de sécurité**

Les principes de sécurité sont l’expression des orientations de sécurité nécessaires et des caractéristiques importantes de la SSI en vue de l’élaboration d’une PSSI[[189]](#footnote-190).

**Procédure**

Dans le cadre de la sécurité des réseaux, les procédures sont des documents à caractère opérationnel et technique, qui décrivent de manière claire et précise les étapes à suivre pour atteindre un objectif de sécurité\* donné.

**Processeur**

*(Processor – Central Processing Unit - CPU)*

Dans un ordinateur, le processeur est la partie qui interprète et exécute les instructions. En 1971, les premiers microprocesseurs voient le jour. Leur taille réduite permet aujourd’hui de les implémenter sur une puce électronique. On trouve ainsi des microprocesseurs multi-cœur (*multi-core)* qui, sur une même puce, permettent le fonctionnement de plusieurs ensembles de circuits qui exécutent des instructions autonomes.

**Produit de sécurité**

Tout dispositif, matériel ou logiciel, mettant en œuvre des fonctions qui contribuent à la sécurité des informations échangées par voie électronique[[190]](#footnote-191).

**Progiciel**

*(Package)*

Ensemble complet et documenté de programmes conçu pour être fourni à plusieurs utilisateurs, en vue d’une même application ou d’une même fonction[[191]](#footnote-192).

**Programmation objet - Programmation orientée objet**

*(Objet-oriented programming)*

Mode de programmation dans lequel les données et les procédures qui s’appliquent sont regroupées en entités appelées « objet ». On entend par objet une entité constituée d’un ensemble d’informations et de lois de comportement[[192]](#footnote-193). On parle improprement de programmation orientée objet pour décrire les langages de programmation qui utilisent ces notions. Java, Python, C++, Ruby ou encore C# sont des langages de programmation par objet. La raison de la grande popularité des langages orientés objets tient dans le mécanisme d’*héritage*. Ce dernier permet de créer des nouveaux objets simplement en les appelant et en remplaçant certains de leurs attributs. Cela permet au programmeur de manipuler des objets complexes en réutilisant des portions utiles et en surchargeant les fonctions à ajouter. Cela permet ainsi de développer simplement des applications graphiques alors que la gestion graphique est intrinsèquement complexe.

**Protocole**

*(Protocol)*

Description formelle de règles et de conventions régissant la manière dont les stations d’un réseau échangent des informations[[193]](#footnote-194). Plus largement, un protocole peut regrouper les conventions pour la coopération d’entités distantes. Ces entités peuvent être réelles ou virtuelles, des matériels ou des logiciels.

**Protocole de routage**

*(Routing protocol)*

Protocole\* qui décrit la manière dont s’opère le routage\* au sein d’un réseau. Il existe deux familles de protocole de routage, ceux pour échanger des informations de routage entre systèmes autonomes (routage externe – BGP\*) et ceux qui échangent des informations à l’intérieur d’un système (routage interne – IGP\*).

Pour le routage interne, il existe plusieurs techniques :

* A état de lien : dans ce cas toutes les informations de routage sont transmises à tous les routeurs qui établissent leurs tables de routage\* avec leurs voisins directs (exemple OSPF) ;
* Vecteur de distance : seuls les meilleures routes sont diffusées (exemple RIP)

Pour le routage externe, voir BGP.

Voir Routage, Protocole, BGP.

**Propriété intellectuelle**

*(Intellectual property)*

La propriété intellectuelle est une notion de droit qui fait en France l’objet d’une définition spécifique dans le Code de la propriété intellectuelle. La propriété intellectuelle regroupe la propriété industrielle et la propriété littéraire et artistique. La propriété industrielle a pour objet la protection et la valorisation des inventions, des innovations et des créations. Les droits de propriété industrielle s'acquièrent en principe par un dépôt (dépôt d'un brevet, d'un dessin ou modèle ou d'une marque). Les droits de propriété industrielle donnent un monopole d'exploitation (sanctionné par l'action en contrefaçon) et constituent à la fois une « arme » défensive et offensive pour les entreprises détentrices de ces droits. Il existe plusieurs voies possibles de protection pour ces droits de propriété industrielle.

La propriété littéraire et artistique s'attache avec le droit d'auteur à protéger les œuvres littéraires, créations musicales, graphiques, plastiques, créations de mode, etc. et les logiciels, ainsi qu'un certain nombre de « droits voisins » (concernant les artistes-interprètes, les entreprises de communication audiovisuelle, par exemple). Le droit d'auteur ne protège pas les idées ou les concepts. Le droit d'auteur s'acquiert sans formalités, du fait même de la création de l'œuvre[[194]](#footnote-195).

***Proxy server***

(Serveur mandataire)

Un serveur proxy (ou serveur mandataire) est un équipement informatique qui sert de relai entre deux ordinateurs. Il assure la double fonction de client\* et de serveur\*, ainsi un proxy cache permet par exemple d’accélérer la navigation. Exécutant les requêtes pour le compte des machines servies, il permet également de cacher la topologie\* d’un réseau ainsi que les clients desservis et par conséquent contribue à la sécurité.

***Proxy***

De façon générale, le terme *proxy* est utilisé pour désigner tout système qui se substitue à un autre pour effectuer une tâche.

**PSTN - *Public Switched Telephone Network***

(Réseau téléphonique commuté -- RTC)

Le PSTN correspond à un réseau public de téléphonie. En France on utilise généralement l’acronyme RTC (Réseau téléphonique commuté). Dans ce réseau un abonné est raccordé à un commutateur par un lien filaire. Le réseau public historique de France Télécom était un PSTN.

Voir RTC.

**Publication**

*(Post)*

Une publication est une contribution, publique ou restreinte, d’un usager sur son profil personnel d’un réseau social, d’un blog, ou d’un chat.

**Puce**

*(Chip - Die)*

Composant électronique monolithique non encapsulé[[195]](#footnote-196).

**PUK – *PIN Unblocking Key***

Le code PUK est le code nécessaire au déverrouillage d’une carte SIM\*.

Voir SIM, GSM.

# Q

**Qualification**

Processus qui consiste à garantir la conformité du produit à ses spécifications.

Dans le cadre de l’analyse d’un incident de sécurité, la qualification consiste à déterminer la nature et la gravité\* de l’incident.

Voir Qualification de produits de sécurité.

***Pour aller plus loin***

L’objectif de la qualification est de s’assurer qu’un produit de sécurité (matériel ou logiciel) ou qu’un prestataire de services de confiance répond aux besoins de l’administration. Le cadre réglementaire (décret no 2010-112 du 2 février 2010) prévoit que le recours à des produits de sécurité et à des prestataires de services de confiance et qualifiés soit la règle générale pour les administrations, les exceptions devant être justifiées. Pour les produits de sécurité, cette qualification est directement délivrée par l’ANSSI, sur la base d’une certification. On distingue trois niveaux de qualification : élémentaire, standard et renforcé permettant de résister à des attaques de niveau croissant. Pour les prestataires, cette qualification est délivrée par un organisme de qualification accrédité par le COFRAC (Comité Français d’Accréditation) et habilité par l’ANSSI. Les familles de prestataires de services de confiance actuellement qualifiées ou en cours de qualification sont : les prestataires de services de certification électronique, les prestataires d’audit SSI, les prestataires d’informatique en nuage (en cours), les prestataires de détection des incidents de sécurité (en cours) et les prestataires de réponse aux incidents de sécurité (en cours). Le catalogue des produits de sécurité et des prestataires de service qualifiés est publié sur le site Web de l’Agence. Au sein de l’ANSSI, c’est le Bureau Qualifications et Agréments de la Sous-direction Expertise qui remplit ces missions[[196]](#footnote-197).

**Qualification de produits de sécurité**

Dans le cadre de ses missions, l’Agence Nationale de la Sécurité des Systèmes d’Information procède à la qualification de produits de sécurité. Il s’agit de conduire un processus pour garantir la conformité du produit par rapport à ses spécifications de sécurité. La démarche permet de recenser les vulnérabilités d’un produit et de tester les contournements possibles des fonctions de sécurité. L’ANSSI présente le processus comme suit : La qualification de produits de sécurité fait l’objet du chapitre III du décret n° 2010-112 du 2 février 2010 pris pour l’application des articles 9, 10 et 12 de l’ordonnance n° 20005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les autorités administratives et les usagers. Elle permet d’attester de la conformité d’un produit de sécurité au RGS (dont la première version en entrée en vigueur le 6 mai 2010 par arrêté du Premier ministre).

Elle prévoit trois niveaux de qualification, un niveau élémentaire, un niveau standard et un niveau renforcé[[197]](#footnote-198).

**Qualité de service**

*(Quality of service – QOS)*

En matière de télécommunications, la qualité de service désigne la capacité à fournir un service conforme aux exigences techniques du dit service (il peut ainsi s’agir de la mesure du temps de réponse et de la bande passante\* notamment). Sur un plan technique les principaux critères de QoS sont le débit, la gigue\*, la perte de paquet, et le déséquencement. La notion de qualité de service est parfois peu précise lorsqu’elle est utilisée dans un contexte *marketing* qui fait référence à « l’expérience utilisateur » et sa perception du service rendu (ex : le service client, la réponse aux incidents etc.). L’usage est rendu encore plus complexe par l’apparition de l’expression anglaise *quality of expérience* qui recouvre les aspects techniques du service. La qualité de service dans un réseau permet de classer les différents types de trafic (on parle alors de classes de services – *Class of Service -* CoS) et permet de garantir un service. Les trois principaux niveaux de QoS sont ainsi :

* *best effort* (meilleur effort), ce niveau ne fournit aucune garantie, il n’y a pas de différenciation des flux réseaux ; on parle également de *lack of QoS ;*
* *differenciated service* (service différencié) qui permet de prioriser les différents flux (sans stricte garantie). Ainsi il est possible de privilégier un flux voix par rapport à un flux donnée (*data*). On parle également de *soft QoS ;*
* *guarented service* (service garanti) dans lequel les flux sont priorisés et des ressources sont réservées pour garantir un niveau de service ; on parle également de *hard QoS*.

En France, une décision de l’ARCEP[[198]](#footnote-199), en application d’une directive européenne antérieure[[199]](#footnote-200), impose aux opérateurs\* (de plus de 100 000 abonnés) au service fixe de mettre à disposition du public les résultats des mesures de qualité de service de leur réseau (ainsi que les indicateurs utilisés et une synthèse des systèmes de mesure utilisés). Ces derniers peuvent être consultés sur le site Internet de l’ARCEP.

**Quantification**

*(Quantizing)*

Action qui consiste à transformer la valeur instantanée d’un signal analogique par une valeur transformée fixe proche de la valeur instantanée. Dans le traitement d’un signal, et typiquement pour la conversion d’un signal analogique\* en un signal numérique\*, il s’agit de remplacer la suite de valeurs instantanées dans un intervalle continu par une suite de valeur discrètes approchante. La quantification est nécessaire pour la conversion analogique – numérique (numérisation\*) mais également pour tous les systèmes de compression d’image ou de signaux audios. Cette opération s’accompagne nécessairement d’une perte d’information, le signal quantifié étant « proche » du signal source mais néanmoins différent. Cette erreur induite par la quantification est appelée distorsion.

Voir Numérisation, Shannon (Théorème).

# R

***Rabbit***

En sécurité informatique, un *rabbit* est un virus ou ver qui se reproduit localement sans limite afin d’épuiser les ressources.

Voir Logiciel malveillant, Virus, Ver.

***Rack***

(Baie)

Une baie (*rack*)est un cadre servant à accueillir des équipements informatiques et réseau. Les baies sont en général de taille normalisée elles peuvent être équipées de portes et intégrer un système de climatisation. Ce système permet de rentabiliser l’espace au sol, la gestion du câblage et de la climatisation.

**Radius – *Remote Authentification Dial In Users Services***

Protocole d’authentification\* et de gestion de serveur\* des accès sur le mode client-serveur. Ce protocole assure les fonctions « triple A », pour Authentification (vérification de l’identité du client), Autorisation (quels sont les droits associés à cette identité), *Accounting* (que fait le client). Le protocole RADIUS est standardisé par une série de RFC\* [2138, 2865, 2866]. Pour assurer la fonction de vérification d’identité des utilisateurs, le service s’appuie sur une architecture ou l’on retrouve :

* Le poste client (celui qui veut se connecter au réseau) ;
* Un client RADIUS – qui est un NAS\* *Network Access Server* – faisant office d’intermédiaire entre le poste client et le serveur RADIUS ;
* Le serveur RADIUS et une base d’identification (annuaire LDAP\* en général ou base de données SQL\*) ;

Lors d’une tentative d’accès, le client RADIUS envoie, sous la forme d’un message spécifique, les informations d’identification d’utilisateur et les paramètres de connexion vers le serveur RADIUS. Celui-ci interroge la base d’identification et autorise (ou pas) la demande du client. Les messages RADIUS utilisent le protocole de transport UDP\* (*User Datagram Protocol*) sur le port\* 1812 pour l’authentification et 1813 pour la gestion des comptes[[200]](#footnote-201). Il existe ainsi une série de messages RADIUS définis dans les RFC, on trouve par exemple[[201]](#footnote-202) :

* Requête d'accès : envoyé par un client RADIUS pour demander l'authentification et l'autorisation d'une tentative de connexion.
* Acceptation d'accès : envoyé par un serveur RADIUS en réponse à un message de requête d'accès. Ce message signale au client RADIUS que la tentative de connexion a été authentifiée et autorisée.
* Rejet d'accès : envoyé par un serveur RADIUS en réponse à un message de requête d'accès. Ce message signale au client RADIUS que la tentative de connexion est rejetée. Un serveur RADIUS envoie ce message si les informations d'identification ne sont pas authentiques ou si la tentative de connexion n'est pas autorisée.
* Challenge d'accès : envoyé par un serveur RADIUS en réponse à un message de requête d'accès. Ce message est un challenge au client RADIUS qui exige une réponse destinée à prouver l’identité du client (authentification).
* Demande de compte : envoyé par un client RADIUS pour spécifier les informations de gestion de compte d'une connexion acceptée.
* Réponse de compte : envoyé par le serveur RADIUS en réponse à un message de demande de compte. Ce message accuse la réception et le traitement du message de demande de compte.

***Rainbow tables***

(Table arc-en-ciel)

Les *rainbow tables* sont des tables de correspondance utilisées en cryptanalyse\* afin de retrouver un mot de passe à partir de son empreinte par une fonction de hachage\*. De nombreuses tables sont disponibles en ligne et peuvent être utilisées par des attaquants.

**RAM - *Random Access Memory***

En informatique, la RAM désigne la mémoire vive de l’ordinateur. Celle-ci n’est utilisée que lorsque le système est allumé, et permet le stockage des données lors de leur traitement. La RAM se caractérise par sa rapidité d’accès et sa volatilité, critères significatifs de performances d’un ordinateur. La RAM est à distinguer de la ROM (*Read Only Memory*), ou mémoire morte, qui constitue la mémoire permanente permettant le fonctionnement de l’ordinateur.

Voir ROM.

**Rançongiciel**

*(Ransomware)*

Logiciel malveillant qui bloque totalement l'accès aux données d’un utilisateur et qui réclame une contrepartie financière pour les rendre de nouveau disponibles. Certains logiciels se contentent de « bloquer » le bureau de l’utilisateur, d’autres chiffrent entièrement le disque dur (*cryptolocker*). Ainsi, *Cryptolocker* est une forme de *ransomware* infectant les postes de travail *Windows* à l’aide d’une pièce jointe piégée d’un message électronique (en général, fichier PDF de facture UPS ou autre). Depuis sa découverte en fin d’année 2013, *Cryptolocker* et ses variantes auraient infecté près de 40 000 machines.

**Rapport signal / bruit**

Le rapport signal sur bruit compare la valeur d’un signal aux perturbations qui l’altèrent. Cette valeur permet de qualifier la qualité d’une transmission, elle est exprimée en décibels.

**RARP - *Reverse Address Resolution Protocol***

RARP est un protocole\* réseau standardisé par la RFC\* 903 permettant à une station d’obtenir une adresse IP\* à partir de son adresse MAC\*. La station interroge une table de correspondance entre adresses MAC\* (adresse physique) et adresses IP situées sur le même réseau local (LAN\*). Cette table est localisée sur la passerelle (routeur). Ce protocole est le mécanisme inverse d’ARP\*.

Voir ARP.

**RAT – *Remote Administration Tool***

(Outil d’administration à distance)

Un RAT est un outil logiciel permettant l’administration à distance d’un système. Il se compose de deux parties distinctes, le client, installé sur l’ordinateur à contrôler, et le serveur, qui prend le contrôle du client sur un poste distant.

On peut rencontrer également l’expression *Remote Access Trojan* qui désigne un ensemble réunissant un cheval de Troie\* (de type *backdoor* par exemple), pour les fonctions d’accès à la machine cible, auquel on adjoint un outil d’administration à distance (pour prendre le contrôle du système cible).

Voir Cheval de Troie, Logiciel malveillant.

**RBL - *Realtime Blackhole List***

Dans le cadre de la lutte *anti-spam* (anti pourriels), les RBL sont des listes de serveurs, d’adresses IP\*, de domaines (URIBL), connus pour héberger, produire ou faciliter les *spams*.

**Redondance**

*(Redundancy)*

En matière de sécurité et de sureté, la redondance désigne le fait de multiplier des équipements informatiques critiques afin de garantir la poursuite d’activité (En cas de défaillance d’un équipement, les autres peuvent continuer à assurer sa fonction).

**Référencement**

Le référencement est l’opération qui vise à rendre un site Web accessible et visible par les moteurs de recherche. Un bon référencement conditionne la visibilité du site et donc son rendement lorsqu’il s’agit de commerce en ligne ou lorsqu’il peut générer des profits par la publicité ou du placement de produit. C’est un élément essentiel d’une stratégie commerciale numérique. En effet, le positionnement d’un site dans les résultats d’un moteur de recherche est un élément critique pour la création de trafic. Bien peu d’utilisateurs saisissent des URL\* « à la main », beaucoup préfèrent utiliser un moteur de recherche\*. Des statistiques démontrent que pour espérer recevoir des visites, un site doit apparaître dans les 10 premiers sur la page des résultats d’un moteur de recherche (moins de 1% des utilisateurs consultent la deuxième page d’une requête dans un moteur de recherche). Ainsi, en 2013, 40 millions de français effectuaient, au moins une fois par mois, des recherches de produits ou de service via *Google*. Le référencement n’est pas forcément « naturel » (c’est à dire purement algorithmique et fondé sur la pertinence), il peut être assuré par un prestataire de service spécialisé, ou bénéficier d’une offre de visibilité facturée par les moteurs de recherche\*.

**Référentiel**

*(Repository)*

En informatique, un référentiel est un ensemble structuré d’informations utilisé pour l’exécution d’un logiciel et constituant un cadre commun à plusieurs applications[[202]](#footnote-203).

**Référentiel général de sécurité (RGS)**

Ensemble de règles que doivent respecter les fonctions des systèmes d’information contribuant à la sécurité des informations échangées par voie électronique entre autorités administratives et usagers ou entre autorités administratives[[203]](#footnote-204).

**Règle de détection**

*(Detection rules)*

Les règles de détection sont utilisées dans les systèmes de défense des systèmes d’information (IDS\* par exemple). Elles sont définies comme une liste d’éléments techniques permettant d’identifier un incident (et donc de déclencher une alerte) à partir d’un ou plusieurs évènements. Une règle de détection peut être un ou des marqueurs, une ou des signatures\* ou une règle comportementale basée sur un comportement défini comme anormal. Une règle de détection peut provenir de l’éditeur des outils techniques d’analyse utilisés pour le service de détection, du prestataire (veille sur de nouveaux incidents, règle utilisée pour un autre commanditaire, etc.), ou encore avoir été créée spécifiquement pour répondre à un besoin du commanditaire[[204]](#footnote-205).

**Registre**

*(Register)*

Espace mémoire pouvant stocker des données temporaires. Dans les architectures de processeurs les registres sont en général spécialisés et ne peuvent contenir qu’un seul type de données. On trouve ainsi des registres entiers (pour stocker les nombres entiers), les flottants (pour les nombres à virgule flottante)…

Le registre est par ailleurs hiérarchisé ce qui en fait une sorte de base de données sur le fonctionnement et l’utilisation d’un système (on y trouve les informations de configuration et les instructions).

La connaissance fine des registres et leur manipulation constituent la base du « *hacking*».

**Registre Internet Régionaux (RIR)**

*(Regional Internet Registry)*

Dans une zone géographique spécifique, un RIR est chargé de l’allocation des numéros d’*autonomous system AS\**, et des blocs d’adresses IP\* (qu’il reçoit de l’IANA\*). Le monde est donc divisé en cinq RIR :

* RIPE-NCC (Réseaux IP Européens – Network Coordination Center) : pour l’Europe et le Moyen-Orient ;
* APNIC (*Asia Pacific Network Information Center*) : Asie et Pacifique ;
* ARIN (*America Registry for Internet Numbers*) pour l’Amérique du Nord ;
* LACNIC (*Latin American and Caribbean IP address Regional Registry*) pour l’Amérique du Sud et la zone Caraïbe ;
* AfriNIC (*African Network Information Center*) pour l’Afrique.

**Relais de trame**

*(Frame relay)*

Technique de multiplexage\* et d’acheminement de paquets\* de données numériques, assemblés en trame\* de longueur variable. Dans la transmission de données, une trame est une suite de bits consécutifs configurée selon un format dépendant du protocole de transmission[[205]](#footnote-206).

Voir *Frame relay.*

**Remédiation**

*(Remediation)*

Reprise à un état connu après l’échec d’un changement ou d’une mise en production[[206]](#footnote-207).

**Renifleur**

*(Sniffer)*

Outil matériel ou logiciel dont l’objet est de capturer les trames\* transitant sur le réseau.

Remarques : Si les trames contiennent des données non chiffrées, un utilisateur malveillant peut aisément récupérer des données confidentielles, comme des mots de passe, des courriers électroniques, des contenus de pages internet, etc. L’utilisateur malveillant peut aussi, à partir des trames, récupérer des informations sur les systèmes échangeant les trames, comme le système d’exploitation\* ou les services employés[[207]](#footnote-208).

De nombreux outils de *sniff* réseau existent, *tcpdump* et *Wireshark* en sont deux exemples courant dans la communauté de la sécurité informatique.

**Renseignement d’Intérêt Cyber-RIC**

*(Cyber intelligence)*

D’apparition encore récente, le terme désigne le renseignement susceptible d’améliorer la connaissance du « cyberespace » et des menaces qui peuvent y prendre forme. Il vise donc à anticiper les cyber-attaques potentielles et à en connaître les acteurs et les méthodes. Le RIC permet en outre d’améliorer la sécurité des systèmes en contribuant à faire évoluer les postures de défense. Pour évaluer ces menaces, le RIC doit se développer suivant trois axes distincts :

* la connaissance des outils (d’attaque et de défense) ;
* l’identification des structures support (infrastructures), des vecteurs de l’attaque ;
* la connaissance des hommes (acteurs) et de leurs compétences[[208]](#footnote-209).

**Renseignement d’Origine Cyber- ROC**

*(CYBINT – Cyber intelligence)*

Si nous présentions le RIC\* comme le renseignement « pour » le cyberespace, le renseignement d’origine cyber désigne pour sa part les renseignements issus de la collecte « dans » le cyberespace. Le concept demeure flou en raison notamment de l’usage du préfixe « cyber » dont on a présenté les limites (voir Cyber\* – Cyberespace\*). Ainsi, des zones de recouvrement apparaissent entre l’OSINT (*Open source intelligence),* le *SIGINT (Signal intelligence)* et le CYBINT. A ce stade il nous semble utile de considérer le ROC comme étant un renseignement issu de l’exploitation d’un des « nouveaux champs[[209]](#footnote-210) » de recherche indépendamment de la nature de son accessibilité (information ouverte – cachée –protégée). Cette approche traduit en fait la disparition progressive de la dualité « ouvert » « fermé » dans le traitement des données de masse. C’est en effet la capacité à traiter les données et à y accéder rapidement qui produira du renseignement.

**Renseignement d’Origine ÉlectroMagnétique - ROEM**

(*SIGINT – SIGnal INTelligence*)

Le ROEM désigne un renseignement qui provient de l’interception et de l’analyse d’un signal électromagnétique. Il peut s’agir de communications (radio, satellites), on parle alors dans la terminologie anglo-saxonne de COMINT – *COMmunication INTelligence*, d’émissions radar (ELINT – *ELectronic INTelligence*) ou d’instruments de télémesure (FISINT – *Foreign Instrumentation Signal INTelligence*).

**Répertoire**

*(Directory)*

Liste d’identificateurs, classés selon des arguments appropriés, permettant l’accès aux informations qu’ils désignent[[210]](#footnote-211).

**Répéteur**

*(Repeater - Transponder)*

Équipement réseau qui intervient sur la couche physique\* du modèle OSI\* pour amplifier un signal (il n’interprète pas les trames\* qu’il reçoit). Il est utilisé pour étendre les périmètres géographiques des segments réseau.

**Reprise (point de)**

Le point de reprise désigne, dans une communication, le point à partir duquel reprendre la communication à la suite d’une erreur.

**Répudiation**

Action qui consiste, pour un individu ou un système impliqué dans une communication, à nier avoir participé aux échanges.

En matière de sécurité, garantir la non-répudiation\* est ainsi essentiel dans les processus de preuve numérique par exemple.

Voir Non-répudiation.

**Réseau**

*(Network)*

Il existe de nombreuses utilisations du terme réseau et par conséquent des définitions sensiblement différentes. Ainsi un réseau est typiquement un ensemble d’objets ou d’êtres humains reliés les uns avec les autres et permettant la circulation d’éléments en respectant des règles spécifiques (quelles soient ou non explicites). Par exemple, le réseau routier relie des lieux physiques et permet la circulation de mobiles qui respectent (plus ou moins) un code spécifique (le code de la route). En informatique, un réseau sera donc un ensemble d’ordinateurs reliés capables d’échanger de l’information. Dans le modèle OSI\*, la couche réseau désigne la couche qui assure les fonctions de mise en relation des équipements. Pour y parvenir, elle utilise des protocoles spécifiques tels que IP (*Internet Protocol*) ou encore les protocoles de routage\* comme BGP\* ou OSPF\*.

**Réseaux ad hoc**

*(Ad hoc network)*

Le réseau ad hoc est un type d’architecture réseau sans infrastructure centralisée, c’est à dire sans points d’accès. Dans ce cas, les terminaux peuvent tous dialoguer avec leurs voisins. Ce type d’architecture s’applique surtout dans les réseaux locaux sans fil.

Voir Picoréseau.

**Réseau d’accès**

*(Access network)*

En télécommunications, un réseau d’accès désigne l’ensemble des moyens servant à relier des terminaux de télécommunication à un commutateur du réseau d’infrastructure[[211]](#footnote-212).

Voir Boucle locale.

**Réseau à valeur ajoutée – RVA**

*(Value Added Network – VAN)*

Dans les télécommunications, un réseau à valeur ajoutée (RVA) est un réseau dont l’utilisation est restreinte à un nombre d’usagers qui accèdent à des applications propres. Pour les applications bancaires, SWIFT (réseau notamment utilisé par *Western Union* pour les virements internationaux) est un exemple de RVA.

**Réseau d’infrastructure**

*(Core network – infrastructure network)*

Dans un réseau de télécommunication, le réseau d’infrastructure est la partie centrale qui regroupe les commutateurs et leurs liaisons. Les terminaux des utilisateurs sont reliés au réseau d’infrastructure par des réseaux d’accès. Même si son usage est déconseillé dans la terminologie française, l’expression « cœur de réseau »est très employée pour désigner un réseau d’infrastructure.

**Réseau de zombies**

*(Botnet)*

Voir *Botnet.*

**Réseau étendu**

*(Wide Area Network – WAN)*

Voir WAN.

**Réseau indépendant**

Le réseau indépendant est une notion définie en droit français pour désigner un réseau de communications électroniques réservé à l’usage d’une ou plusieurs personnes constituant un groupe fermé d’utilisateurs, en vue d’échanger des communications internes au sein de ce groupe[[212]](#footnote-213).

**Réseau local**

*(Local Area Network – LAN)*

Voir LAN.

**Réseau local d’entreprise – RLE**

*(Local Area Network – LAN)*

Voir LAN.

**Réseau privé virtuel**

*(Virtual Private Network)* Voir VPN.

**Résilience**

La résilience d’un système traduit sa capacité à continuer à opérer et à revenir « à son état initial » après un incident. Pour un système d’information, la résilience est essentielle dans le cadre de la poursuite d’activité et de la continuité de service. Ainsi, dans la conception d’une architecture réseau on cherchera, par construction, à assurer la résilience du système. Plusieurs techniques sont employées dont la redondance\* des systèmes critiques.

**Rétro-ingénierie**

*(Reverse engeniring – reverse)*

La retro-ingénierie est une activité qui consiste à analyser un programme informatique sans disposer de son code source. L’objectif est de comprendre la logique interne du programme, son fonctionnement et d’en déduire son comportement. Le *reverse* est une activité qui contribue à la sécurité générale d’un système d’information et est un élément clé dans les mécanismes d’attribution d’attaque informatique.

**RFC - *Request for comment***

Document de l’IETF mis en ligne à la disposition de tous et qui décrit les aspects techniques de l’Internet. Les RFC sont des « appels à commentaires » et ne deviennent pas toutes des standards. Les protocoles de communications sont donc présentés dans des RFC spécifiques. Les documents sont d’abord présentés sous forme de brouillon à l’IETF avec une date de péremption. Ceux qui suscitent l’intérêt de la communauté peuvent entraîner la création d’un groupe de travail dédié pour la rédaction d’une RFC. Quelques RFC deviennent des standards de l’Inter­net. La première RFC a été publié le 7 avril 1969 et porte sur le « logiciel hôte » (*host software,* RFC 1), les principaux protocoles de l’Internet sont aujourd’hui des standards. Ainsi, la définition d’UDP [RFC 786] est le STD 6, la définition du protocole internet IPv4 [RFC 791] le STD 5.

**RFID - *Radio Frequency Identification***

(Radio-identification)

Technique qui permet d’identifier des objets, des véhicules, des animaux ou des personnes au moyen d’un dispositif électronique transmettant par radiofréquence des informations préenregistrées à un lecteur qui l’interroge à faible distance[[213]](#footnote-214). On retrouve aujourd’hui des puces RFID dans de nombreuses situation (étiquettes – *tag*). Elles sont notamment très utilisés dans la gestion de flux logistiques et des stocks.

**RIP - *Routing Information Protocol***

Protocole développé pour l’échange d’informations de routage entre routeurs voisins. RIP est utilisé au sein d’un même système autonome (*autonomous system – AS\*)* et permet l’établissement des tables de routage\*. RIP appartient donc à la famille des IGP\* (*Interior Gateway Protocol)*, c’est un protocole à vecteur de distance\*, c’est à dire qu’il associe un « coût » à une route. Le coût est généralement le nombre de routeurs à traverser pour atteindre la cible (pour RIP le coût maximal est de 15 sauts, au-delà la route est considérée comme non valable). RIP permet la mise à jour des routes, chaque routeur envoie sa table de routage complète à l’ensemble du réseau (RIP *update*) de proche en proche. Chaque routeur compare alors la table qu’il reçoit avec la sienne et met à jour ou rejette les modifications. Ainsi, si une entrée reçue en *update* n’existe pas, le routeur va l’inscrire dans sa propre table et incrémenter le coût de 1. Si l’entrée existe déjà il va simplement comparer le coût de *l’update* avec celui qu’il a en table. Si le coût est inférieur, il accepte *l’update*, s’il est supérieur il le rejette. RIP est décrit dans la RFC 1058, la version 2, qui date de 1993 dans la RFC 2453.

**Riper**

*(Rip)*

Extraire directement d’un support enregistré des données numériques en vue de les reporter sur un autre support, sans recourir à la conversion analogique intermédiaire habituellement nécessaire[[214]](#footnote-215).

**Risque**

*(Risk)*

La notion de risque, notamment dans le contexte de la sécurité informatique, s’appuie sur la définition proposée par l’ISO 27005 qui la présente comme : la possibilité qu’une menace donnée exploite les vulnérabilités d’un bien (ou d’un actif) ou d’un groupe de biens (ou d’actifs) et nuise à l’organisation.

Les responsables de la sécurité doivent donc prendre des mesures pour réduire ces possibilités et traiter les risques identifiés. Toutefois, le risque zéro n’existe pas et il subsiste toujours un risque après traitement, qui est alors qualifié de risque résiduel.

**RJ 45**

Fiche permettant de connecter les cartes réseaux des réseaux locaux (Ethernet). La RJ 45 est munie de 8 fiches de connexion.

Voir Ethernet.

**RLC – *Radio Link Control***

Protocole qui, dans un réseau de données cellulaires, (souvent associé au *Medium Access Control* MAC\* – RLC/MAC) assure le transfert physique de l’information sur l’interface radio entre un terminal et le réseau (BSS\* – *Base Station System*). Le protocole assure également une fonction de correcteur d’erreur. Il permet la retransmission sélective des blocs en erreur suivant la technique du BEC – *Backward Error Correction*.

**RNIS - Réseau Numérique à Intégration de Services**

*(Integrated Services Digital Network – ISDN)*

Réseau entièrement constitué par des connexions numériques et qui permet à ses usagers d’échanger des informations de nature différente : sons, images, données. La forme la plus simple d’accès RNIS comprend deux canaux utilisables pour des communications téléphoniques indépendantes (canal de type B) et un canal de signalisation\* (canal de type D) de capacité plus faible destiné aux informations de service[[215]](#footnote-216).

**ROM – *Read Only Memory***

La ROM - *Read Only Memory*, ou mémoire morte, constitue la mémoire permanente d’un ordinateur. Appelée également mémoire non volatile, elle permet le fonctionnement de l’ordinateur car elle conserve les données nécessaires à son démarrage. La ROM contient par exemple le BIOS\* qui est le programme qui pilote les interfaces principales du système.

Voir également MBR

***Rootkit***

(Outils de dissimulation d’activité)

Programme ou ensemble de programmes permettant de dissimuler une activité, malveillante ou non, sur une machine. Par extension, tout programme ou ensemble de programmes permettant à une personne malveillante de maintenir un contrôle illégitime du système d’information en y dissimulant ses activités. L’activité dissimulée peut être une activité sur le système de fichiers (création, lecture, écriture), une activité réseau, une activité en mémoire. Pour cela, un *rootkit* peut travailler dans l’environnement de l’utilisateur, sans droits particuliers, ou en profondeur dans le système d’exploitation, nécessitant par conséquent des droits d’exécution élevés.

Remarques : L’installation de ces programmes nécessite que le système soit préalablement compromis (cheval de Troie, intrusion). Ces programmes modifient souvent les commandes usuelles de l’administrateur, afin de dissimuler toute trace de leur présence. Ils effectuent aussi fréquemment plusieurs opérations au niveau du noyau du système d’exploitation, comme l’installation de portes dérobées, la capture des frappes clavier, etc. Un outil de dissimulation d’activité n’a pas pour but d’offrir un accès quelconque à la machine hôte. En revanche, la plupart de ces outils malveillants embarquent des fonctionnalités de porte dérobée permettant à l’auteur un accès à distance et un maintien sur le système compromis[[216]](#footnote-217).

**Routage**

*(Routing)*

Acheminement des paquets\* de données sur le réseau. Cette action est effectuée par des machines spécialisées, les routeurs\*. On distingue typiquement plusieurs types de routage :

• *Unicast*: acheminement des données vers une destination unique et déterminée ;

• *Broadcast*: diffusion des données vers toutes les machines ;

• *Multicast*: le message est délivré vers un ensemble de machines ou un groupe de destinataire particulier ;

• *Anycast*: le message est délivré à un seul destinataire d’un groupe (généralement le plus proche au sens du réseau).

Le routage est un processus décentralisé, chaque élément du réseau dispose d’informations sur son voisinage. Les routeurs maintiennent à jour des tables de routage\*, qui listent les réseaux connus du routeur. Ces réseaux sont donc atteignables. Les tables de routage contiennent trois types de routes :

Les réseaux directement connectés, c’est à dire directement atteignable par un protocole de niveau 2 (réseau) ;

Les routes statiques, qui sont des routes configurées manuellement « en dur » dans le routeur par l’administrateur réseau ;

Les routes dynamiques qui sont « apprises » par la réception de messages spécifiques de protocoles de routage (comme RIP\* par exemple). Les routes sont ainsi mises à jour en fonction de leur état et de l’apparition ou disparition de réseaux.

Voir Protocole de routage.

**Routeur**

*(Router)*

Élément d’un réseau informatique en charge du routage\* des paquets\*. Ce routage est assuré entre des interfaces\* réseau et répond à un ensemble de règles (protocoles\*). Les routeurs sont donc des éléments clés du réseau et assurent des fonctions essentielles à la bonne transmission des informations, ils sont au cœur des enjeux de sécurité. De nombreuses polémiques ont émergé sur les failles de sécurité existantes sur les routeurs de certains équipementiers. L’exploitation de ces vulnérabilités permettrait la mise en œuvre d’une surveillance des flux.

**RSA - Rivest, Shamir, Adelman**

L’acronyme RSA désigne un algorithme\* de chiffrement\* développé par trois chercheurs en cryptographie, Rivest, Shamir et Adelman. Cet algorithme permet un chiffrement asymétrique\* basé sur un système des clés publiques et privés. Il permet également de signer numériquement un message. Les mathématiques sous-jacentes reposent sur la théorie des nombres premiers et le constat de la difficulté de factoriser les grands nombres. Le cryptosystème RSA fait partie des systèmes inclus dans les standards de l’ISO et de l’ITU (norme X.509\*) mais également dans le standard d’échange bancaire SWIFT (*Society for Worlwide Interbank Financial Telecommunications).*

**RSSI – Responsable de la Sécurité des Systèmes d’Information**

Le responsable de la sécurité des systèmes d’information est en charge du maintien à niveau de la sécurité des systèmes ainsi que de la gestion du risque informatique dans son périmètre. Le RSSI occupe également une place centrale dans l’information des utilisateurs, la sensibilisation et le développement de ce que l’on qualifie « d’hygiène » informatique. Le champ de responsabilité d’un RSSI ne cesse d’augmenter ; il couvre ainsi la sécurité des réseaux, des télécommunications, des applications (métiers et autres) ainsi que la sécurité physique de certaines emprises. Il doit en outre mettre en œuvre les moyens nécessaires à la redondance\* et au fonctionnement en mode dégradé.

**RSVP - *Resource Reservation Protocol***

Le protocole RSVP est un protocole\* qui vise à établir et maintenir un chemin réservé entre deux points du réseau. Le circuit n’est pas statique (comme pour un circuit virtuel) mais son état est maintenu par des messages spécifiques de rafraîchissement. RSVP est donc un protocole de signalisation\* qui permet également de garantir une qualité de service par l’allocation dynamique de bande passante\*. Il est décrit dans la RFC\* 2225.

Voir Signalisation.

**RTC - Réseau Téléphonique Commuté**

(PSTN - *Public Switched Telephone Network* ou POTS – *Plain Old Telephone Service*)

Appellation du réseau téléphonique public dit « fixe ». Il relie les abonnés par des liaisons filaires. L’usage du RTC est en décroissance permanente depuis une dizaine d’année, victime de l’émergence de la téléphonie mobile et sur IP. Ainsi, en France, le nombre d’abonnements RTC décroît d’environ 20% par an depuis 2011.

**RTCP - *Real-time Transport Control Protocol***

Voir RTP.

**RTP - *Real-time Transport Protocol***

Le protocole RTP a été développé pour permettre le transport (sur IP) de données ayant des contraintes temporelles et notamment le temps réel. RTP est donc nécessaire pour l’acheminement sur Internet de flux multimédia ou interactifs (téléphonie sur IP, vidéo à la demande, etc.). RTP numérote des séquences de paquets\* afin de pouvoir les reconstituer « dans l’ordre » à l’arrivée et ce, quel que soit le mode de transport. L’entête RTP permet de rajouter les numéros de séquence et les éléments nécessaires à la synchronisation. RTP est donc largement utilisé pour les services Internet, il utilise un mécanisme de contrôle appelé RTCP\*. Il véhicule les informations utiles sur la qualité de service RTP et sur les différents participants d’une session (il est possible de créer des groupes multiutilisateurs pour les conférences par exemple).

Voir RTCP.

**RTSP - *Real Time Streaming Protocol***

Protocole de niveau applicatif qui repose sur des protocoles de transport tel que RTP\* et RSVP\* pour fournir un service de flux temps réel sur Internet.

Voir RTP, RSVP.

# S

**S/MIME - *Secure / Multipurpose Internet Mail Extensions***

Le protocole S/MIME est un protocole\* développé pour la signature numérique\* et le chiffrement\* des messages électroniques.

Voir Signature numérique.

**Sabotage**

*(Sabotage)*

Le sabotage informatique est l’action qui consiste à rendre inopérant tout ou partie d’un système d’information par une attaque informatique.

La menace de sabotage informatique est aujourd’hui pleinement intégrée dans les missions des agences de cyberdéfense\*, en France comme à l’étranger. S’il s’apparente à une « panne organisée », le sabotage informatique de certains systèmes peut s’avérer extrêmement lourd de conséquences. En France, plusieurs secteurs stratégiques, qualifiés d’opérateurs d’importance vitale (OIV\*) font l’objet de mesures réglementaires spécifiques afin de garantir leur sécurité.

Un des exemples les plus documenté de sabotage informatique demeure l’attaque contre les systèmes d’enrichissement d’uranium iranien par le virus Stuxnet\*.

Voir Stuxnet, OIV.

***Sandbox***

(Bac à sable)

En sécurité informatique, une *sandbox* (ou bac à sable) est un environnement contrôlé qui permet d’exécuter un code inconnu que l’on souhaite tester. Typiquement les *sandbox* sont utilisées pour faire exécuter un code malveillant dans un environnement proche du système à protéger mais totalement isolé de celui-ci.

**Saut**

*(Hop)*

Dans un mécanisme de routage\*, un saut représente la distance entre deux routeurs\* voisins.

Voir Routage.

**Sauvegarde**

*(Back up)*

Procédure d’enregistrement des fichiers sur un support secondaire (externe, clé USB, disque dur, *cloud*) afin d’éviter leur destruction ou leur perte.

**SCADA - *Supervisory Control And Data Acquisition***

Les SCADA sont des logiciels de contrôle de surveillance et de supervision des installations industrielles et techniques. Ils permettent de surveiller et de commander (à distance) des processus industriels, des systèmes de gestion des transports, d’approvisionnement d’eau, de distribution électronique etc. Les SCADA assurent, en temps réel, le recueil de données sur un système, les télémesures et la télégestion de certains processus. Outre l’aspect logiciel, le SCADA s’appuie sur un réseau de communication, une base de données, une interface de gestion et des terminaux distants (ou automates programmables industriels).

La prise de contrôle, par un groupe malveillant, de ces systèmes présente donc de nombreux risques, faisant des SCADAs une cible prioritaire de recherche pour les *hackers*.

**Scan**

*(Scan)*

Un scan réseau est une action réalisée dans le cadre d’un audit de sécurité permettant par exemple d’établir la liste des équipements connectés sur le même réseau local\* (LAN), les ports\* ouverts, les services « à l’écoute » sur ces ports etc.

Le scan est une action « bruyante », elle laisse des traces car elle interroge les équipements et donc génère des échanges et des *logs\**. Cette étape est pourtant essentielle pour un attaquant distant cherchant à détecter et exploiter une vulnérabilité.

Voir Balayage de ports.

**Script**

*(Script)*

En informatique, un script est un programme constitué d’une suite de commandes dispensant l’utilisateur de les saisir, et permettant d’effectuer une fonction particulière ou de contribuer à l’exécution d’un autre programme. Un script peut être notamment un programme associé à un document décrit à l’aide d’un langage de balise destiné à améliorer l’interactivité. La terminologie française retient également les termes de macro ou macrocommande.

Un *script* est un programme écrit dans un langage interprété (c’est à dire qui sera exécuté lui-même par un autre programme). Par exemple PHP\* est un langage interprété, on va donc écrire des scripts PHP pour exécuter des commandes sur un serveur. Par ailleurs, le script est exécuté directement à partir du code source, sans être compilé.

Voir Code, Compiler.

***Scriptkiddies***

Type de « pirates » qui utilise les codes d’exploitations diffusés publiquement pour conduire des attaques. Leur niveau technique est souvent faible, ils ne cherchent généralement qu’à créer des pannes système ou des dysfonctionnements dans une démarche de mise en avant égocentrique. Le terme est évidemment péjoratif au sein de la communauté des hackers.

**SDLC - *Synchronous Data Link Control***

Protocole\* de contrôle de liaison en mode synchrone. Il a été remplacé par HDLC (*High Level Data Link Control)*.

Voir HDLC.

**SDMX – *Statistical Data and MetaData eXchange***

Projet lancé en 2002, SDMX cherche à définir un standard pour l’échange de données\* et de métadonnées\* statistiques. De nombreuses institutions économiques et financières soutiennent ce projet (Banque Centrale Européenne, Fond Monétaire International ou encore ONU). SDMX est reconnu par l’ISO depuis 2013 sous le standard ISO/TS 17369.

**SDU - *Service Data Unit***

(Unité de données service)

Dans le modèle OSI\* le SDU désigne une unité de données échangée entre couches du modèle pour qu’elles puissent assurer leurs fonctions.

**Sécurité d’un système d’information**

La sécurité d’un système d’information recouvre l’ensemble des moyens techniques et non techniques de protection, permettant à un système d’information de résister à des évènements susceptibles de compromettre la disponibilité, l’intégrité ou la confidentialité des données, traitées ou transmises et des services connexes que ces systèmes offrent ou rendent accessibles**[[217]](#footnote-218)**.

**Sémaphore**

Le sémaphore est un mode de signalisation\* hors bande pour les réseaux de téléphonie. Il sépare ainsi les informations de signalisation de celles liées à la communication. Le sémaphore est normalisé par le CCITT en 1981. Il est plus connu sous le nom de SS7\* (*Signaling System 7*). Ce protocole permet donc l’établissement de communications, il repose sur des points sémaphore (PS) qui sont des équipements émetteurs et récepteurs de messages de signalisation (exemple le MSC\*), le point de transfert sémaphore (PTS) assure pour sa part le routage\* de ces messages (le PTS peut être PS). Développé dans les années 70, SS7 est un protocole encore peu sécurisé. Des chercheurs ont ainsi exposé des failles de sécurité pouvant permettre d’accéder à des données sensibles telles que la localisation d’un téléphone portable ou l’interception d’appels[[218]](#footnote-219).

**Serveur**

(*server*)

Au sein d’un réseau, le serveur est un ordinateur chargé de fournir des réponses aux requêtes des autres ordinateurs (clients\*). Il permet par exemple de stocker des données partagées par plusieurs clients. La définition officielle propose alors : matériel, logiciel ou système informatique destiné à fournir un service déterminé à d’autres systèmes informatiques ou à des utilisateurs connectés sur un réseau[[219]](#footnote-220). Les serveurs sont au centre de l’architecture réseau et sont de plusieurs natures, serveurs de fichiers, d’impression, de bases de données, de courriers, Web ou encore de jeux vidéo.

**Serveur mandataire**

*(Proxy server)*

En règle générale, un serveur mandataire, ou plus improprement serveur proxy\*, est un dispositif informatique associé à un serveur qui réalise, pour des applications autorisées, des fonctions de médiation, telles que le stockage des documents les plus fréquemment demandés ou l’établissement de passerelles[[220]](#footnote-221). Il assure ainsi, par les fonctions de cache, une réponse rapide à des requêtes, il mémorise les pages fréquemment consultées de sorte qu’à la requête suivante, c’est la copie, stockée en local, qui est d’abord transmise au client (gain de temps de réaction). Outre ces fonctions de cache, le serveur proxy permet également d’améliorer la sécurité car il assure un filtrage des requêtes et masque le réseau interne en effectuant les requêtes en son nom. On peut ainsi utiliser un serveur proxy pour masquer sa propre adresse IP\* lors de consultation internet (le serveur cible enregistrera l’adresse du proxy et non celle du client initial).

Voir Proxy.

**Serveur racine**

*(Root server – root name server)*

Appelé également serveur de noms de la racine, il désigne le point de départ de l’arborescence du système de nommage DNS\*. Il existe actuellement 13 serveurs de noms de la racine répartis dans le monde : ces serveurs hébergent les données permettant le bon fonctionnement du système d’adressage par domaines (DNS) et des services qui utilisent ce système : internet, courrier électronique[[221]](#footnote-222)…

Voir DNS, Domaine.

**Service**

*(Service)*

Le mot service recouvre plusieurs champs en fonction du domaine dans lequel on l’utilise. Ainsi, dans le contexte de l’architecture OSI\*, permettant de modéliser les fonctions d’un réseau, un service est une fonction assurée par une des couches pour le niveau qui lui est immédiatement supérieur. Ainsi, la couche physique (couche 1) assure la fonction de connexion physique pour la couche 2 (liaison).

Un service sur une machine désigne un logiciel serveur, ce dernier est « en écoute » sur un port\* particulier de la machine. Il attend d’être activé par un logiciel client\*. Les services les plus courant utilisent des ports réservés par convention. Ils sont appelés les *well known services*. Sur une architecture Windows, un service est un composant logiciel qui fonctionne comme un module du système d’exploitation (OS).

Voir Port.

**Session**

*(Session)*

Une session est un intervalle de temps durant lequel la communication est possible. La session doit donc être ouverte avant de pouvoir échanger puis fermée pour libérer les ressources. De façon générale, la session désigne l’intervalle de temps durant lequel les ressources et les mécanismes sont mobilisés au profit d’un utilisateur.

Dans l’architecture OSI\*, le mot désigne la couche 5. La couche session a pour principale fonction de gérer et de synchroniser le contrôle de connexions entre les *process* applicatifs. Cette couche opère comme un « régulateur de temps de parole » entre applications et couches basses (transport).

Voir OSI.

**SGML - *Standard Generalized Markup Language***

(Langage standard de balisage généralisé)

Langage SGML, normalisé par ISO 8879, regroupe un ensemble de conventions de balisage de contenu qui permettent à une application d’exploiter un document. Un système de balises permet d’identifier les chapitres, les paragraphes, les commandes et le texte. HTML\* est, par exemple, un format qui respecte le standard SGML.

Voir HTML.

**SHA - *Secure Hash Algorithm***

SHA est un algorithme de hachage qui est utilisé pour l’authentification\* et la vérification de l’intégrité d’une donnée échangée. Développé par la NSA, les versions 0, 1 et 2 sont aujourd’hui supplantées par la version 3 issue d’un concours public (2007). SHA-0 est formellement déconseillée depuis 1996, SHA-1 est très utilisée dans les applications mais reste vulnérable (théoriquement) aux attaques par collision. La famille SHA-2 regroupe alors les SHA 256 et 512 par exemple (la différence réside dans la taille des mots en entrée de la fonction et la taille des blocs hachés suivant les algorithmes cryptographiques sous-jacents). La version 3 fait l’objet d’un standard du *National Institute of Standards and Technology* – NIST, publié le 5 août 2015.

Voir Fonction de hachage.

**Shannon**

*(Shannon)*

La définition officielle du Shannon le présente comme une unité de mesure de l'information, égale à la quantité d'information associée à la réalisation de l'un de deux évènements équiprobables qui s'excluent mutuellement. Son symbole est Sh et on doit cette définition au mathématicien Claude Shannon (1916-2001), père de la théorie de l’information.[[222]](#footnote-223)

Le Shannon représente donc la quantité d’information contenue dans un bit\*.

**Shannon (Théorème de)**

Egalement appelé théorème de Shannon Nyquist, il stipule que la numérisation\* correcte d’un signal nécessite de l’échantillonner\* à une fréquence au moins double de la fréquence du signal analogique\*.

Voir Numérisation, Echantillonnage.

***Shareware***

(Logiciel partagé)

Un *shareware* est un logiciel protégé par la propriété intellectuelle qui est utilisé gratuitement durant une période limitée. Au terme de cette période l’usager se voit proposer d’acheter le logiciel.

***Shellcode***

Un *shellcode* est une suite d’instructions utilisées par un *payload*\* lors de l’exploitation. Il est typiquement écrit en langage assembleur. Dans la plupart des cas, une invite de commande système (un *shell*) ou une invite de commande meterpreter (du Framework\* Metasploit\*) est utilisée après qu’une série d’instructions a été accomplie par la machine[[223]](#footnote-224).

**SHTTP- *Secure Hypertext Transfer Protocol***

S-HTTP, est une extension sécurisée du protocole HTTP\*. Il fonctionne avec plusieurs algorithmes de chiffrement qui sont définis entre le client\* et le serveur\* (DES\*, triple DES etc.). Le SHTTP est décrit dans la RFC\* 2660. Si SHTTP et HTTPS ont tous deux été développés pour sécuriser les échanges entre un navigateur et un serveur (notamment pour le commerce en ligne), HTTPS est devenu le standard de fait le plus répandu.

A la différence d’HTTPS, SHTTP ne chiffre qu’une partie des échanges (côté serveur) ainsi que les données soumises au serveur (POST). HTTPS utilise, pour sa part, le protocole SSL pour sécuriser les échanges (il utilise donc un port\* dédié, en général 443, différent du port 80 classiquement utilisé pour HTTP.

***Shunning***

Le *shunning* permet le blocage rapide d’une adresse IP considérée comme malveillante. L’action permet de reconfigurer certains équipements (typiquement des routeurs CISCO), et de modifier les ACL\* (listes d’autorisation d’accès). Cette reconfiguration dynamique par un routeur Cisco de ses ACL permet ainsi de stopper une attaque et d’en limiter les effets.

**SIEM – *Security Information and Event Management***

Ensemble logiciel qui permet la surveillance en temps réel d’un réseau en collectant et analysant les évènements de sécurité. Le SIEM assure donc la collecte et l’analyse de *logs\** et génère des rapports ou des tableaux de bord. L’efficacité d’un SIEM repose sur sa capacité à être paramétré en fonction du système d’information sur lequel il est implanté ainsi que sur l’anticipation du volume des données collectées afin d’analyse et de corrélation. Le SIEM est un outil qui peut être intégré dans un SOC\* - *Security Operations Center* afin de contribuer à la sécurité du système d’information considéré.

Voir SOC.

**Signal**

*(Signal)*

Un signal est un phénomène physique dont les caractéristiques varient dans le temps pour permettre la représentation d’une information. Dans ce cadre, un signal analogique\*, par exemple, est un signal électrique qui varie de façon *analogue* à un phénomène physique donné. Le microphone permet ainsi de transformer la variation de pression de l’air résultant de l’émission d’un son en un signal électrique analogique.

**Signal analogique**

*(Analog(e) signal)*

Signal tel que la caractéristique qui représente les informations peut à tout instant prendre la valeur d’un intervalle continu, par exemple suivre de façon continue les valeurs d’une autre grandeur physique représentant des informations[[224]](#footnote-225).

**Signal numérique**

*(Digital signal)*

Signal au moyen duquel les informations sont représentées par un nombre fini de valeurs discrètes bien déterminées qu’une de ses caractéristiques peut prendre dans le temps.

Voir Numérisation, Numérique.

**Signalisation**

*(Signaling)*

La signalisation est un processus qui permet d’assurer la circulation d’éléments sur un réseau. Dans un réseau de télécommunication la signalisation consiste à envoyer des messages de « service » entre les équipements pour permettre l’acheminement d’une communication. La signalisation permet ainsi d’établir et de rompre une communication entre deux usagers du réseau.

**Signalisation hors bande**

*(Out of band signaling)*

La signalisation hors bande est un type de signalisation qui utilise des canaux de transmission différents des canaux utilisés pour le transfert de l’information.

Voir Sémaphore.

**Signature d'attaque**

*(Attack signature)*

Une signature d’attaque est une modélisation d’activité malveillante. Les signatures sont regroupées dans des bases qui servent aux équipements de détection d’intrusion. Si l’on utilise indifféremment les termes de signature et de marqueur\*, il convient de privilégier celui de « mar­queur » car « signature » est également utilisé dans d’autres contextes (notamment cryptographique) mais également parce qu’un marqueur n’est pas nécessairement une « signature » du fait de l’existence de faux positifs. Ainsi, un marqueur peut être détecté sans être relié à une activité malveillante, il n’en constitue donc pas une « signa­ture ». De même on trouve également l’expression « marqueur de compromission » qui gagnerait à être appelé plus largement « marqueur d’activité malveillante » car un marqueur réseau peut détecter une attaque en déni de service sans pour autant qu’il y ait eu compromission du système au sens strict.

Voir Marqueur.

**Signature de virus**

*(Virus signature)*

Une signature de virus est une suite d’éléments binaires commune à chacune des copies d’un virus ou d’un ver particulier, et utilisé par les logiciels antivirus pour détecter leur présence[[225]](#footnote-226).

L’utilisation de signature de virus en sécurité informatique est la plus ancienne des méthodes de protection. Toutefois, elle est aujourd’hui très incomplète et ne permet pas, par exemple, la détection de virus polymorphes. Les antivirus développent donc en parallèle d’autres techniques de détection.

Voir Heuristique, Antivirus, IDS, Code malveillant, CVE.

**Signature électronique**

*(Electronic signature)*

La signature électronique est selon le Référentiel Général de Sécurité (RGS V2) une fonction de sécurité qui permet de garantir l’identité du signataire, l’intégrité d’un document signé et le lien entre document signé et la signature. Elle traduit ainsi la manifestation du consentement du signataire quant au contenu des informations signées.

Le Code civil, dans son article 1316-4 al.2 précise que la signature électronique consiste en l’usage d’un procédé fiable d’identification garantissant son lien avec l’acte auquel elle s’attache. La fiabilité de ce procédé est présumée, jusqu’à preuve contraire, lorsque la signature électronique est créée, l’identité du signataire assurée et l’intégrité de l’acte garantie, dans des conditions fixées par décret en Conseil d’Etat[[226]](#footnote-227).

**Signet**

*(Bookmark)*

A l’image d’un marque page pour un livre, le signet permet de garder en mémoire sur le navigateur une page consultée régulièrement. L’usage du signet (ou du favoris) évite de ressaisir l’adresse complète du site dans la barre de recherche.

**SIM - *Subscriber Identity Mobile***

Elément d’identification d’un abonné mobile.

Voir Carte SIM.

***Sinkholing***

Le DNS\* *sinkholing* ou plus simplement le *sinkholing* est une pratique utilisée pour lutter contre les programmes malveillants (le *botnets\** par exemple). Le *sinkholing* consiste à rediriger les noms de domaine\* malveillants vers un serveur\* (ou plusieurs) non maîtrisés par l’attaquant. Ce détournement peut ainsi empêcher les postes clients compromis de recevoir les commandes du pirate (via le serveur de commande et de contrôle C&C). Cette technique permet également d’analyser le flux reçu, de récupérer les informations transmises et d’établir des statistiques utiles à l’analyse en cybersécurité (répartition des victimes par pays, type d’activité etc.).

Si l’intérêt du *sinkholing* est manifeste pour démanteler des réseaux de *botnets* par exemple, se pose toutefois la question de la validité juridique du processus. En effet en détournant les flux, le propriétaire du *sinkhole* a accès aux données exfiltrées par exemple. Sur le plan technique, il convient d’installer un serveur DNS qui va rediriger vers un serveur d’analyse les noms de domaines malveillants sélectionnés[[227]](#footnote-228).

**SIP – *Session Initiation Protocol***

SIP est un protocole\* de communication utilisé pour établir et modifier des communications d’applications téléphoniques (et multimédia) basé sur IP. Il est utilisé pour les applications de voix sur IP (VoIP\*) et défini par la RFC\* 3261. SIP sert à initialiser la communication, le transport des données repose pour sa part sur d’autres protocoles (RTP\* et SDP).

***Slacktivisme***

Angliscisme formé de la contraction des mots *slack* (mou, lâche) et *activisme*, le slacktivisme est l’action qui consiste à soutenir une cause en publiant des contenus sur les réseaux sociaux. L’action est assez liée au mode de fonctionnement du réseau Twitter avec notamment l’utilisation de mots dièse (#, hashtag). Certaine campagnes de slacktivisme ont connu un véritable succès en s’appuyant sur des influenceurs et des communautés actives, on se souviendra par exemple de la campagne #BringBackOurGirls pour réclamer la libération des jeunes lycéennes nigérianes enlevées par le groupe terroriste Boko Haram en 2014.

**SMB - *Server Message Block***

Le protocole SMB permet à des stations (Windows) appartenant à un même réseau local\* d’accéder (en lecture et écriture) à des fichiers partagés. Il permet également l’accès à des services auprès d’un serveur. SMB est utilisé pour partager une imprimante réseau par exemple.

**SMF - *Single Mode Fiber***

*(Fibre monomode)*

Voir Fibre optique.

**SMS - *Short Message Service***

(Messagerie Texte)

Le SMS est un service créé en 1992 qui permet l’échange de messages texte sur le réseau de téléphonie mobile. Ce système d’échange est extrêmement populaire en dépit de l’apparition de nombreuses applications de messagerie instantanée (*whatsapp*, *viber,* *Skype,* etc). On estime en France que 180 milliards de SMS sont envoyés par an et près de 8000 milliards dans le monde). Le coût d’acheminement d’un SMS est d’environ un centime d’euro en France et en moyenne de 3,5 cent de dollar dans le monde.

Voir Messagerie Texte.

**SMTP - *Simple Mail Transfer Protocol***

Protocole\* standard de l’Internet élaboré, dès 1982 pour permettre le transport des courriers électroniques\*. Le protocole est décrit dans les RFC\* 821 (2821) et 822, il permet le transport du courrier entre un serveur source et destination par une liaison point à point\*. SMTP fonctionne par défaut sur le port\* 25, en mode connecté\*.

Voir Courrier électronique pour une présentation de l’ensemble des protocoles.

**SMURF (attaque)**

(Attaque par réflexion)

Type d’attaque informatique dans lequel un serveur\* de diffusion (*broadcast\**) est utilisé afin de relayer un paquet *ping\** modifié. Cette technique permet d’amplifier le nombre de requêtes vers une machine cible et provoque un déni de service\*. Cette attaque est possible car le mécanisme de *ping* utilise le protocole ICMP\* qui garantit une réponse de la machine visée par un test de connectivité. L’attaquant doit alors modifier l’adresse de réponse du *ping* et indiquer l’adresse IP\* de la victime, puis chercher un serveur de *broadcast* pour diffuser largement sa demande. Ainsi, chaque machine *pingée* va répondre vers l’adresse de la machine cible. Ce mode d’attaque est relativement ancien et des mécanismes de sécurité permettent de s’en prémunir.

***Snapshot***

(Instantané – capture d’écran)

Un *snapshot* est une reproduction partielle ou totale de l’état d’un système. On utilise également le terme pour désigner une capture d’écran.

**SNMP - *Simple Network Management Protocol***

(Protocole Simple de Gestion de Réseau)

Protocole\* de gestion et d’administration de réseau, SNMP est décrit dans la RFC\* 1157. Son architecture repose sur des agents et un superviseur. Les agents se trouvent sur chaque équipement (chaque interface\*) assurant une connexion. Les équipements réseaux classiques, tels que les routeurs, le *hub* et les *switch* hébergent des agents qui sont capables de collecter et de transmettre des données locales de gestion vers le superviseur.

**SNORT**

En sécurité informatique, SNORT désigne un système de détection d’intrusion (IDS\*) réseau. Outil libre (publié sous licence GNU GPL), il se base sur des règles de détection établies et diffusées par une communauté d’utilisateurs. SNORT peut être couplé avec d’autres outils afin de proposer une réponse active aux détections (ex, Guardian, SnortSam).

Voir IDS.

**SOA – *Service Oriented Architecture***

(Architecture Orientée Service)

Le principe d’une architecture orientée service est de formaliser les échanges et le partage entre applications au sein d’un système d’information. Ainsi, les systèmes d’information d’entreprise ont tendance à devenir de plus en plus hétérogènes et des processus métiers spécifiques augmentent encore ce phénomène. Pour y remédier, il faut organiser la communication entre applications. Pour ce faire on définit une interface standard, on réalise la mise en relation entre les logiciels clients et fournisseurs de service et on fixe un vocabulaire commun en définissant les services communs aux différents métiers.

**SOAP - *Simple Object Access Protocol***

Protocole\* de communication qui permet l’échange entre clients et fournisseurs de service Web\*. SOAP permet d’appeler des méthodes sur des objets distribués (distant). Il utilise la notation XML\* pour transmettre les paramètres de cet appel. SOAP peut utiliser HTTP\*, FTP\* ou SMTP\* pour transférer ses messages.

**SOC – *Security Operations Center***

Dans le contexte de la sécurité des systèmes d’information, un SOC, également appelé *Information Security Opertion Center*, désigne le lieu où la sécurité de l’ensemble des systèmes d’information d’une entité considérée est supervisée. On retrouve par exemple au sein du SOC, des outils logiciels de supervision de réseau et de détection d’évènements de sécurité (SIEM\*) ainsi que des moyens humains d’analyse et de réponse à incidents.

Voir SIEM.

***Social engineering***

(Ingénierie Sociale)

Voir Ingénierie Sociale.

**Sonde de détection d’attaque**

Outils déployé sur un réseau afin de détecter les attaques informatiques. Les agences de cyberdéfense réalisent et administrent leurs propres sondes pour protéger les réseaux gouvernementaux. Pour les autres réseaux, les vendeurs de solutions de sécurité fournissent ce type de service. Voir IDS.

***Spam***

(pourriel)

Message électronique généralement non sollicité. Les *spams* sont en quelque sorte l’équivalent numérique du prospectus publicitaire dans votre boite aux lettres. Certaines entreprises sont aujourd’hui spécialisées dans la diffusion de ces courriels et monnayent leurs services et plateformes d’envoi.

***Spanning Tree***

(Arbre recouvrant)

Protocole de routage\* qui a été développé afin de pouvoir interconnecter plusieurs types de réseaux avec ponts\* et sans boucles. Dans ce mécanisme, chaque nœud apprend progressivement la topologie\* du réseau en observant les trames\* qui lui sont envoyées.

Le *spanning tree* permet de détecter les boucles sur un sous-réseau et de les supprimer. Il n’existe alors qu’un seul chemin entre des segments distants. Le protocole est défini dans la norme IEEE 802.1D.

Voir Routage, Pont, Topologie.

**Spectre électromagnétique** -

*(Electromagnetic Spectrum)*

Le spectre électromagnétique désigne l’ensemble des ondes électromagnétiques classées en fonction de leur longueur d’onde, fréquence ou énergie.

* Les ondes les plus énergétiques, les rayons gamma, ont une longueur d’onde très courte comprise entre un centième de milliardième de millimètre et un milliardième de millimètre (inférieure à 10 picomètres dans tous les cas). Ce rayonnement est produit au cœur des noyaux atomiques (par désintégration), il faut plusieurs mètres de béton armé pour les stopper ;
* Avec une longueur d’onde légèrement supérieure (de l’ordre du nanomètre) et toujours très énergétique, les rayon X sont utilisés en médecine (radiographie) et dans l’industrie ;
* Toujours assez énergétique, le rayonnement ultraviolet est beaucoup moins nocif que les deux précédents. Egalement appelé lumière noire, il est le dernier rayonnement non visible ;
* Les rayonnements visibles, avec des longueurs d’ondes croissantes et une énergie décroissante, ils occupent une

portion très faible du spectre entre 400 et 700 nanomètres ;

* Au delà du visible, l’infrarouge (entre 750 et 3000 nanomètres) est un rayonnement naturel émis par tout corps dont la température est supérieure au zéro absolu. L’infrarouge est donc associé à la température d’un objet, il est utilisé par exemple par les caméras thermiques ou des détecteurs (capteurs de proximité) ;
* Avec des longueurs d’onde allant du centimètre au mètre, les ondes radar sont utilisées pour la télédétection et comme capteur actif (système radar) ;
* Viennent enfin les ondes radio, avec des longueurs d’onde allant de quelques centimètres à plusieurs kilomètres. Les applications des ondes radio sont nombreuses en télécommunication notamment.

***Spread Spectrum***

(Etalement de spectre)

L’étalement de spectre est une technique de modulation\* qui consiste à étaler l’information sur une bande de fréquence plus large que nécessaire. Les données sont transmises à faible puissance. Cette technique, proposée dans la norme IEEE 802.11 permet de lutter contre le bruit et les parasites. On distingue classiquement deux techniques d’étalement de spectre : à saut de fréquence (FHSS\*) ou à séquence directe (WCDMA\*).

Voir Modulation à spectre étalé, FHSS, WCDMA.

**SQL - *Structured Query Lanquage***

SQL est un langage qui permet d’effectuer des requêtes vers une base de données\*. Initialement développé par IBM, ce langage est aujourd’hui très rependu chez les développeurs Web\*. La requête la plus simple consiste à lire une donnée issue d’une base, elle s’effectue avec la commande SELECT en précisant le champ à retourner et la base qu’il faut interroger. Au delà de la manipulation de données, SQL permet également la création et la suppression de tables dans une base ainsi que les permissions utilisateur. Sa connaissance est essentielle dans le cadre de la sécurité informatique et de nombreux pirates exploitent des failles de configuration à l’aide de simple requête SQL.

Voir Injection SQL.

**SS7 - *Signaling System 7***

Voir Sémaphore.

**SSH - *Secure Shell***

SSH est un ensemble de protocoles\* qui permettent l’établissement d’une connexion chiffrée entre un serveur\* et un client\*. Le serveur, comme le client doivent disposer d’un logiciel permettant cette connexion et notamment la génération de clés pour le chiffrement\*. *OpenSSH* est, par exemple, un logiciel libre qui permet de configurer un serveur SSH et un client SSH.

**SSID – *Service Set IDentifier***

Le SSID est le numéro d’identification d’un réseau sans fil dans la norme IEEE 802.11. SSID est l’abréviation de ESSID.

Voir ESSID.

**SSII - Société de Service et d’Ingénierie Informatique**

Voir ESN.

**SSL - *Secure Socket Layer***

Protocole\* de sécurisation des échanges sur Internet. Il est situé entre la couche transport (couche 4 du modèle OSI\*), donc au-dessus de TCP/IP\*, et la couche session (couche 5). Le protocole utilise des certificats X.509\* pour les mécanismes d’authentification\*, les échanges alors sont chiffrés par un algorithme symétrique (AES\*, DES\*, etc.) avec des longueurs de clés variables. Deux sous protocoles principaux interviennent alors, le SSL *Handshake protocol*, pour la négociation des clés et du protocole de chiffrement entre deux entités communicantes et SSL *Record protocol* qui utilise les mécanismes de chiffrement négociés et effectue le contrôle sur les échanges. SSL permet ainsi la création d’un tunnel chiffré lors d’une connexion HTTP\* (on parle alors de HTTPS). Il existe une version libre de SSL : *openSSL* très rependue.

Voir SHTTP.

**SSL/TLS - Secure Socket Layer/Transport Layer Security**

Depuis sa création le protocole SSL a connu plusieurs versions, depuis la version 3, il est appelé TLS. On trouve donc régulièrement la notation SSL/TLS pour désigner en fait l’évolution du protocole SSL.

**SSO - *Single Sign-On***

(Authentification unique)

SSO est un ensemble de méthodes et d’outils qui permettent à un utilisateur un accès à plusieurs applications grâce à une authentification unique. Cette méthode permet de gérer l’ensemble des mots de passe d’un utilisateur afin de faciliter son usage quotidien.

**STAD – Système de Traitement Automatisé des Données**

Notion utilisée en droit pénal français pour qualifier un système d’information au sens large. Il n’existe pas de définition officielle afin de ne pas limiter l’interprétation du droit à un « état de l’art » de la technologie au moment de la rédaction du texte. Le terme STAD est utilisé dans le Code pénal français pour sanctionner les atteintes au fonctionnement des systèmes, les accès frauduleux (intrusion\*) et les atteintes frauduleuses aux données.

**Standards**

*(Standards)*

Dans le cadre de la sécurité réseau, les standards sont des documents de standardisation de normes et méthodes émanant d’organismes internationaux tels que l’ISO\* (*International Standardisation Organisation*), l’IETF\* (*Internet Engineering Task Force*), l’IEEE\* (*Institute of Electrical and Electronics Engineers*), etc[[228]](#footnote-229).

Voir IEEE, IETF.

**Station de base - BTS**

*(Base Transceiver Station).* Voir BTS.

**Stéganographie**

*(Steganography)*

La stéganographie est une technique qui consiste à cacher un message dans un autre support (une image par exemple). Ainsi, le message n’est pas rendu inintelligible, il est simplement dissimulé dans un autre. Les premiers usages de stéganographie semblent remonter à l’antiquité avec le témoignage d’Hérodote (env 450 av. JC). L’usage de l’encre invisible ou le recouvrement de message par de la cire ou de la peinture sont des exemples de techniques stéganographiques. Aujourd’hui des applications simples permettent d’insérer du texte dans une image qui peut alors être échangée normalement par courrier électronique ou autre support de communication.

Voir Chiffrement.

**STIX - *Structured Threat Information eXpression***

STIX est un projet du MITRE\* qui vise à développer un langage standard pour offrir une représentation structurée des menaces cyber. L’échange des données STIX utilise un mécanisme de transport spécifique *Trusted Automated of Indicator information (TAXII).* Ce système permet l’échange sécurisé et automatique des menaces cyber entre différents organismes et structures. STIX est associé à d’autres travaux du MITRE comme CAPEC\* (présentation des schémas et modes d’attaque), MAEC\* *Malware Attribute Enumeration and Characterization,* ou CybOx, un langage de description des évènements « cyber » (logs\*, *malware*, détection d’intrusion, *pattern* d’attaque).

***Store and Forward***

(Commutation de messages)

Le *store and forward* est un mode de fonctionnement standard d'un commutateur. Celui-ci stocke entièrement la trame\* qu'il reçoit avant d’entamer la retransmission. La terminologie française retient l’expression « commutation de messages » qui est définie comme un Mode d'acheminement de messages complets dans un réseau de télécommunication comprenant dans certains nœuds du réseau une réception, une mise en mémoire et une retransmission des messages vers la ou les destinations voulues[[229]](#footnote-230).

***Streaming***

(Flux – en flux)

Le *streaming* est une technique de transfert en temps réel qui permet la diffusion de contenus multimédia par Internet. Les données sont transmises en flot continu vers le client. De nombreux sites proposent de visionner des vidéos en *streaming*, utilisant ainsi une faiblesse dans les dispositions légales qui, en France, interdisent le partage de fichiers protégés par des droits d’auteurs.

**Stuxnet**

Stuxnet est un ver\* informatique utilisé dans une opération de sabotage\* informatique contre les sites d’enrichissement d’uranium iraniens. Probablement le plus célèbre (à ce jour) des outils d’attaque, Stuxnet représente avant tout un symbole, au-delà de son effet réel ou supposé. Au même titre que les attaques en déni de service distribué (DDoS) contre l’Estonie en 2007, Stuxnet demeure, sans équivalent, la première opération d’entrave contre un système de contrôle et de commande d’un système automatisé (SCADA\*). Michael Hayden, ancien directeur de la CIA déclarait alors :

*« STUXNET est la première attaque majeure de cette nature qui parvient à entraîner des destructions physiques affectant une infrastructure importante (…). Quelqu’un a franchi le Rubicon. Je ne veux pas dire que nous allons assister aux mêmes conséquences, mais, d’une certaine manière, nous sommes un petit peu en août 1945 ».*

Au mois de juin 2010, les autorités iraniennes confirment qu’un ver informatique a réussi à compromettre les systèmes de supervision et de contrôle du site d’enrichissement d’uranium de Natanz. A ce stade il est encore difficile de mesurer l’impact de cette compromission sur le programme nucléaire iranien et les travaux de recherche d’Ivanka Barzashka[[230]](#footnote-231) soutiennent même la thèse que cette attaque n’a pas atteint son objectif[[231]](#footnote-232). Les conclusions de son étude se fondent sur l’analyse des rapports de l’AIEA qui notent une évolution du nombre de centrifugeuses en service entre 2009 et 2010 mais pas de baisse significative de la production d’uranium enrichi.

***Stuxnet***

Type de *malware*: ver.

Objectif : Sabotage.

Cible : Sites nucléaires iraniens (le ver a cependant également touché l’Inde et l’Indonésie).

Date de création : Estimée au mois de janvier 2009 avec un début de développement vraisemblable en 2006.

Date de détection : Juin 2009

Versions connues : Il existe au moins quatre versions en circulation. Chaque détection a entrainé une modification du ver (juin 2009, mars 2010, avril 2010, juillet 2010). Ces enchaînements entre détection et modification du ver laissent à penser qu’une équipe était en charge du suivi de l’attaque et de la maintenance de celle-ci.

Taille : 500 ko à 1 Mo selon les versions.

Nombre de systèmes infectés : environ 15 000.

Caractéristiques principales : Stuxnet constitue un véritable tournant dans la perception par le grand public et les autorités de la réalité du concept de « cyberguerre ». Le ver a été construit spécifiquement à des fins de sabotage, il est le fruit d’un long travail de développement (certains évoquent un début de développement en 2006 dans le cadre de l’opération « *Olympic Game*» qui aurait été ordonnée par la Maison Blanche). Stuxnet utilise en outre quatre vulnérabilités 0-day\* du système d’exploitation Microsoft Windows.

**Suivre, suiveur**

*(Follow/Follower)*

Le terme désigne l’action de s’abonner au flux diffusé par une autre personne sur un réseau social. Les contenus publiés sur le compte sont alors consultables par la personne qui « suit ». L’expression est principalement utilisée sur le réseau *Twitter*\*. Des applications spécifiques permettent d’analyser le nombre, le profil et les centres d’intérêts de vos *followers*.

**Synchrone**

Dans une transmission, le mode synchrone est un mode dans lequel le récepteur et l’émetteur transmettent sur le même rythme.

Voir Mode de transmission asynchrone.

**Système d'exploitation**

*(Operating System - OS)*

Logiciel\* de base d'un ordinateur, le système d’exploitation permet la gestion des ressources matérielles et constitue « l’interface homme machine » (IHM). Ainsi, lorsqu’une application veut accéder à une ressource matérielle (mémoire ou processeur), elle va solliciter l’OS qui va gérer les demandes et y répondre via les pilotes (*drivers*). L’OS gère donc la mémoire vive (RAM\*), le ou les processeurs, et les applications. L’OS permet, en outre, un contrôle des accès au système (par les utilisateurs autorisés). Les OS les plus connus sont Windows, MacOS et Linux.

**Système d’information – SI**

*(Information system)*

Est considéré comme un système d’information, tout ensemble de moyens destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives[[232]](#footnote-233).

De façon plus simple, l’ANSSI présente le système d’information comme, un ensemble organisé de ressources (matériel, logiciels, personnel, données et procédures) permettant de traiter et de diffuser de l’information.

**Système d’information industriel**

*(Industrial Information System – IIS)*

Un système d’information industriel est un système d’information dédié aux systèmes industriels. Si chaque installation industrielle est spécifique, un système d’information regroupe en général les éléments suivants :

* Automates Programmables Industriels – API *(Programmable Logic Controller – PLC)*;
* Systèmes Numériques de Contrôle-Commande (SNCC) ;
* Systèmes Instrumentés de Sécurité (SIS) ;
* Capteurs et actionneurs ;
* Bus de terrain ;
* Logiciels de supervision et de contrôle (SCADA) ;
* Logiciel de gestion de production assistée par ordinateur (GPAO, MES) ;
* Logiciels d’ingénierie et de maintenance ;
* Système embarqué[[233]](#footnote-234).

Voir SCADA.

**Système d’information sensible**

Un système d’information sensible est un système d’information qui traite d’informations dont la divulgation à des personnes non autorisées, l’altération ou l’indispo­nibilité sont de nature à porter atteinte à la réalisation des objectifs des entités qui les mettent en œuvre[[234]](#footnote-235).

**Système de localisation GPS**

*(Global Positioning System - GPS)*

Le système de localisation GPS est un système mondial de satellites de navigation qui permet de déterminer la position d’un récepteur. Ce dernier reçoit plusieurs signaux (codés) des différents satellites qu’il peut capter. Le récepteur interprète, décode les signaux et en déduis sa position (dans un référentiel géodésique – WGS 84). La précision varie en fonction du code utilisé (certains étant réservés à des utilisateurs particuliers).

Ainsi, le code P assure une précision de l’ordre de 10 mètres, le mode standard code C/A délivre lui une précision de 100 mètres.

# T

**TA – *Time Advance***

Dans un réseau GSM\*, le *time advance -* TA est un décalage temporel entre les messages envoyés par les différents mobiles vers la station de base (BTS) afin d’éviter les collisions. En effet, sans ce paramètre, les *burst* émis par les mobiles utilisant deux *slots* consécutifs risquent de se chevaucher au niveau de la BTS en raison du temps de propagation. Le TA correspond au temps de propagation aller-retour entre un mobile et la BTS.

**Table de routage**

*(Routing table)*

Une table de routage est un ensemble de données structurées, stocké par un routeur\* ou un hôte IP (équipement connecté au réseau et utilisant le protocole IP pour communiquer), qui contient les informations nécessaires à l’acheminement des datagrammes\* vers leurs destinations. Les entrées de la table de routage possèdent généralement les champs suivants :

* Destination : la destination peut être une adresse IP\* complète ou celle d’un sous réseau ;
* Masque de réseau : qui permet de faire correspondre à une adresse IP de destination la valeur du champ Destination ;
* Tronçon suivant ou adresse de passerelle\* : qui détermine l’adresse IP vers laquelle le paquet IP est transféré ;
* Interface : qui désigne l’interface\* réseau à utiliser pour transférer le paquet ;
* Métrique : qui fait correspondre un coût à un itinéraire. Ce champ est utilisé par les protocoles de routage\* pour déterminer la meilleure route en fonction des choix de routage effectués.

Un administrateur réseau peut configurer manuellement des routes dans une table de routage, elles sont appelées routes statiques et sont à distinguer des routes dynamiques qui sont mises à jour par l’intermédiaire de protocoles de routage (BGP\* ou OSPF\* par exemple). En outre, une route par défaut est nécessaire pour indiquer la destination des paquets qui ne correspondent à aucune entrée de la table de routage. Voir BGP, Routage.

***Tag Switching***

(Commutation d’étiquette)

Le *tag Switching* est une technologie de commutation de paquets\* qui préfigure le *label switching* du protocole MPLS\*. Développé par CISCO *System*, il repose sur un mécanisme d’acheminement des paquets par l’utilisation d’étiquettes (*tag*).

Voir MPLS.

**Tarpit**

Service\* qui permet de ralentir les connexions entrantes dans un système. Le *tarpit* a été développé par Tom Liston afin de contrer la propagation du ver *CodeRed*. Un *tarpit* en fonction sur un port\* où l’on ne doit pas recevoir de trafic permet, en cas de tentative de connexion, de répondre favorablement mais avec une valeur de taille de paquets très faible afin de limiter l’infiltration.

**Taux d'erreurs**

*(Error Rate)*

Dans une transmission, le taux d’erreurs représente le rapport du nombre de bits erronés au nombre total de bits transmis.

**Taux d'erreurs Résiduelles**

*(Residual error-rate)*

Rapport du nombre des bits incorrectement reçus mais non détectés comme tels, au nombre total de bits transmis.

**TCP - *Transmission Control Protocol***

Protocole\* de transport de la couche 4 du modèle OSI\* (couche transport). Très utilisé dans des applications internet (associé au protocole IP, TCP/IP) TCP peut représenter jusqu’à 90% du trafic mesuré. Le protocole a été une première fois standardisé en 1981, dans la RFC\* 793, pour répondre au besoin de fiabilité dans le transport au profit de certaines applications (messagerie, transfert de fichiers). Ainsi, TCP établit des mécanismes de transfert bi-directionnels entre processus distants avec la possibilité pour chacun de moduler la vitesse du trafic en fonction de la disponibilité des ressources. Ce mécanisme de « con­trôle de flux » permet par exemple de demander la réexpédition d’un paquet\* non reçu. En outre TCP dispose d’un mécanisme de contrôle de congestion qui permet à un émetteur de vérifier que la vitesse d’émission ne va pas entrainer un engorgement du réseau (et donc des pertes de paquets). Cette évolution de TCP est dite *Tahoe* et est décrite dans la RFC 1122 qui date de 1989. En 1999, une autre version du protocole, dite *Reno* (RFC 2581) améliore *Tahoe* qui diminuait trop nettement l’efficacité des transmissions.

Le protocole TCP est orienté connexion et se découpe en trois phases : ouverture de la connexion, transfert des données, fermeture de la connexion. Le flot d’octets à transmettre est découpé en segments qui sont déposés dans des paquets IP avant d’être transmis sur le réseau, chaque segment est numéroté afin de permettre un mécanisme d’acquittement et de retransmission. TCP utilise deux méthodes pour détecter une perte de paquet. Ainsi, il y a perte si l’émetteur ne reçoit pas un acquittement (dans un certain délai) ou s’il reçoit plusieurs acquittements qui ne correspondent pas à un paquet émis récemment.

Dans le modèle Internet, il existe d’autres protocoles de transport, tel qu’UDP\* par exemple, lorsque la fiabilité n’est pas une priorité.

*L’entête TCP*

TCP mettant en œuvre des mécanismes de contrôle, l’en-tête des paquets est nécessairement porteuse de plus d’informations. Outre les ports\* source et destination (sur 16 bits chacun) qui indiquent la source et la destination du paquet, on trouve un champ numéro de séquence (sur 32 bits). Ce champ permet de numéroter un paquet dans une séquence afin de pouvoir respecter l’ordre de réassemblage et est nécessaire au mécanisme d’acquittement. Le numéro d’acquittement d’un paquet correspond au numéro de séquence du paquet attendu. Ce champ permet de renvoyer vers l’émetteur le décompte des paquets reçus et indique s’il y a eu des pertes.

Le champ « décalage des données » est aussi appelé « taille de l’en-tête » et indique la longueur de l’en-tête du paquet. On trouve ensuite un champ réservé avec un système de « drapeaux » (*flag\*)* chaque drapeau ayant une signification particulière :

• URG : urgent

• ACK : le paquet est un accusé de réception

• PSH : *push* données à « pousser », à envoyer sans délai ;

• RST : *reset*

• SYN : demande de synchronisation

• FIN : demande de fin de connexion.

Le champ fenêtre indique la taille souhaitée de la fenêtre de congestion (mécanisme de contrôle de congestion de TCP). Cela traduit le nombre d’octet que le récepteur peut recevoir sans accuser réception.

Le champ somme de contrôle, permet de vérifier l’intégrité du paquet (le checksum est calculé sur l’ensemble de l’en-tête TCP et du champ de données). Le champ pointeur Urgent, indique la position des dernières données urgentes

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **32 bits** | | | | | | | | | | | | | |
| Port source | | | | | | | | | | | | Port destination | |
| Numéro de séquence | | | | | | | | | | | | | |
| Numéro d’acquittement | | | | | | | | | | | | | |
| Taille de l’en-tête | Réservé | ECN/NS | CWR | ECE | URG | ACK | PSH | RST | SYN | FIN | | Fenêtre | |
| Somme de contrôle | | | | | | | | | | | Pointeur de données urgentes | | |
| Options | | | | | | | | | | | | | Remplissage |
| Données | | | | | | | | | | | | | |

Voir UDP *User Datagram Protocol.*

**TCP/IP (modèle)**

Reposant sur les mêmes principes d’abstraction que le modèle OSI\* (qui permet de normaliser les modes de communication entre ordinateurs en réseau), le modèle TCP/IP est une simplification appliquée à Internet. Le modèle ne contient que 4 couches qui regroupent plusieurs couches du modèle OSI.

* La couche accès, qui utilise les protocoles Ethernet\*, PPP\* ou *token ring\*.* Cette couche regroupe la couche physique\* et liaison de données du modèle OSI (couche 1 et couche 2), elle se charge de définir la forme suivant laquelle les données seront acheminées.
* La couche internet, qui utilise le protocole IP, c’est la couche réseau du modèle OSI (couche 3), elle constitue le datagramme\* (paquet de données) qui sera acheminé par la couche transport ;
* La couche transport (identique au modèle OSI), qui utilise le protocole TCP et assure le transport des datagrammes et le contrôle des connexions.
* La couche application, qui regroupe les couches application, présentation et session du modèle OSI.

Le principe repose sur un mécanisme d’encapsulation des données en fonction des couches (chacune ajoute les informations nécessaires à son traitement par la couche adjacente). Ainsi, lorsqu’une application souhaite envoyer un message vers une autre application, celui-ci est encapsulé (on lui rajoute une en-tête TCP) et devient un segment de la couche transport. Ce segment est lui-même encapsulé pour devenir un paquet de la couche IP avant de circuler sous forme de trame\* au niveau de la couche accès.

**TD/CDMA - *Time Division* / CDMA**

Mode d’accès radio utilisé pour la téléphonie mobile entre un terminal et une station de base\*. Il combine plusieurs types de multiplexage.

Voir Accès multiple

**TDM - *Time Division Multiplexing***

(Multiplexage temporel)

Le TDM est une technique de multiplexage\* qui permet de transmettre sur un même support de communication plusieurs canaux numériques. Chaque station dispose d’un intervalle de temps dédié (*slot\*)* pendant lequel elle peut transmettre sur le lien. Elle dispose donc, durant une courte période de temps, de l’ensemble de la bande passante\*.

Voir AMRT, Multiplexage.

**TDMA - *Time Division Multiple Access***

Technique de multiplexage\* temporel du signal utilisé dans les modes d’accès multiples\*.

Voir Accès multiple, AMRT.

**Téléchargement**

*(Download)*

Le téléchargement consiste à transférer un fichier depuis un ordinateur distant (serveur\*) vers un ordinateur local (client\*) par l’intermédiaire d’un réseau.

**Télécharger**

*(Upload)*

Action inverse du téléchargement\*, *l’upload* consiste à transférer une donnée (fichier) depuis un client vers le réseau.

**Téléphonie sur IP – TOIP**

*(Telephone over IP)*

La téléphonie sur IP est un service permettant la communication téléphonique en utilisant le protocole IP. La voix, après numérisation\*, est scindée en paquets et transportée comme n’importe quel autre type de données. On parle également de VoIP – *Voice over IP* ou de Voix sur IP\*.

**TELNET – *TELecommunication NETwork***

Telnet est un protocole\* de niveau applicatif qui permet d’assurer la communication entre deux machines en réseau (utilisant la suite TCP/IP\*). TELNET est présenté dans les RFC\* 854 et 855. Au-delà du protocole, Telnet est aussi la commande (dans un terminal\*) qui permet de créer une session\* Telnet entre un client et un serveur. Telnet, en raison de sa simplicité, ne prend pas en compte de mécanismes de sécurité. Aucun chiffrement des échanges n’est effectué. Il demeure cependant utile pour disposer d’un accès distant sur certains équipements lorsqu’ils ne disposent pas d’une interface Web de gestion par exemple.

**Témoin de connexion**  
*(Cookie)*

Voir Cookie.

**Temps de latence**

*(Latency)*

Le temps de latence d’un équipement réseau désigne la durée nécessaire pour qu’une trame\* soit traitée par l’équipement. Il s’agit donc typiquement du délai entre l’instant d’arrivée de la trame et sa sortie de l’équipement. A l’échelle d’un réseau, la latence est donc le temps minimal nécessaire à un paquet pour rejoindre une destination depuis la source. La latence a un fort impact sur certaines applications de communication (comme le transport de la voix par exemple). La variation dans le temps de la latence est par ailleurs appelée gigue\*.

Voir Gigue.

**Temps de réponse**

Le temps de réponse d’un système désigne la durée nécessaire à l’accomplissement d’une commande. C’est le délai de réaction d’une application.

**Terminal**

*(Terminal)*

Le terminal désigne, en informatique, l’ensemble des périphériques qui permettent de communiquer avec un ordinateur. L’expression vient du fait qu’à l’origine, la taille des ordinateurs interdisait qu’ils puissent être « physi­quement » dans les mêmes pièces que les utilisateurs. Ces derniers avaient donc recours à des équipements « ter­minaux » (clavier, écran) pour communiquer leurs instructions. Aujourd’hui, un terminal est une « invite de commande » (un *shell\**) qui permet de dialoguer avec le système par l’intermédiaire de lignes de commande. De façon synthétique, un terminal est donc un appareil qui permet l’accès à distance à un système informatique[[235]](#footnote-236).

**Test d’intrusion**

*(Pentest – pénétration test)*

Le test d’intrusion est l’un des outils d’évaluation de la sécurité d’un système d’information, il peut être effectué dans le cadre d’un audit de sécurité dans des conditions particulières. Dans son référentiel d’exigences, l’ANSSI le présente comme suit :

Le principe du test d’intrusion est de découvrir des vulnérabilités sur le système d’information audité et de vérifier leur exploitabilité et leur impact, dans les conditions réelles d’une attaque sur le système d’information, à la place d’un attaquant potentiel. Les vulnérabilités testées peuvent également avoir été identifiées au cours d’autres activités d’audit. Cette activité d’audit peut être réalisée soit depuis l’extérieur du système d’information audité (notamment depuis Internet ou le réseau interconnecté d’un tiers), soit depuis l’intérieur.

Un test d’intrusion seul n’a pas vocation à être exhaustif. Il s’agit d’une activité qui doit être effectuée en complément d’autres activités d’audit afin d’en améliorer l’efficacité ou de démontrer la faisabilité de l’exploitation des failles et vulnérabilités découvertes à des fins de sensibilisation.

Les tests de vulnérabilité, notamment automatisés, ne représentent pas à eux seuls une activité d’audit au sens du Référentiel[[236]](#footnote-237).

La relative facilité à se procurer des outils de test d’in­tru­sion, il existe d’ailleurs des *frameworks\** dédiés, ne doit pas faire oublier que ces pratiques sont rigoureusement encadrées par la loi française[[237]](#footnote-238) (Code Pénal art 321-1).

Voir Audit.

**TETRA - *Terrestrial Trunked Radio Access***

A l’inverse du GSM\* utilisé pour les communications personnelles, TETRA est un standard européen (de *l’European Telecommunications Standards Institute* - ETSI) développé pour le marché des communications radio mobile professionnelles. TETRA offre un moyen sécurisé et portable pour les radiocommunications de nombreuses unités de police ou des services d’urgence dans le monde. Ainsi, un réseau TETRA offre un canal radio ouvert en permanence à un groupe restreint d’utilisateurs (lorsqu’un utilisateur est en émission, l’ensemble du groupe reçoit l’appel).

**Tiers de confiance**

(*Trusted third party – TTP)*

Voir Confiance.

***Time Out***

Délai maximal pour qu’un équipement effectue une tâche. Au-delà de ce délai, un message d’erreur (ou une mise hors circuit) est envoyé.

Ainsi, le protocole de contrôle ICMP\* utilise le message ICMP\_TIME\_OUT pour informer une station émettrice d’un paquet\* que celui-ci va être détruit car son TTL\* (*Time To Live*) est à zéro. Ces mécanismes permettent d’éviter que des paquets ne circulent indéfiniment dans le réseau tout en informant la station émettrice de ce dysfonctionnement.

Voir ICMP, TTL.

**TKIP - *Temporal Key Integrity Protocol***

Protocole qui permet de sécuriser l’authentification\* dans un réseau Wi-Fi, TKIP a été développé pour palier aux faiblesses de sécurité de WEP\*. Le mécanisme TKIP (norme 802.11i) consiste à fournir de nouvelles clés de façon périodique (et non plus unique comme WEP). L’algorithme de cryptographie sous jacent demeure RC4.

**TLD – *Top Level Domain***

(Domaine de premier niveau)

Un domaine de premier niveau est un sous-domaine de la racine dans le système de noms de domaine\*. Sur Internet il existe environ 250 domaines de premiers niveau « nationaux », ce sont les .fr pour la France, .uk pour le Royaume-Unis, .be pour le Royaume de Belgique etc. Outre ces domaines nationaux, environ 300 sont dits génériques (.org, .com, .net). La gestion des noms de domaine relève de l’ICANN\*.

Voir Domaine, DNS, ICANN.

***Token Ring***

(Anneau à jeton)

*Token ring* est une technique d’accès pour réseau local\* où chaque station est reliée à une seule autre station par un lien unidirectionnel. Le *token ring* fonctionne sur le principe d’une communication alternée. Chaque station n’est autorisée à émettre que lorsque la précédente a terminé (principe du jeton). Dans une telle topologie\*, les stations sont reliées à un équipement spécifique qui est en charge de la « gestion du jeton ». Cet équipement est un répartiteur appelé MAU *Multistation Access Unit.* Ce type de réseaux locaux est standardisé par l’IEEE 802.5.

**Tolérance aux pannes**

*(Fault tolerance)*

Aptitude d’un système informatique à demeurer fonctionnel malgré certaines pannes et ses constituants[[238]](#footnote-239).

**Topologie de réseau**

*(Network topology)*

La topologie de réseau désigne le mode d’organisation physique ou logique d’un réseau. On distingue ainsi plusieurs topologies classiques initialement décrites suivant les connexions physiques entre machines.

* Topologie en bus : les stations sont reliées entre-elles via un câble unique.
* Topologie en anneau : les stations sont reliées une à une suivant une boucle.
* Topologie en étoile : une station centrale connecte des stations périphériques. Cette station est un concentrateur.
* Topologie en « arbre » ou hiérarchisée : une topologie sous forme de pyramide avec une station « mère ».
* Topologie maillée : les stations sont reliées entre-elles suivant plusieurs liaisons point à point sans hiérarchie. Une station peut ainsi être reliée à plusieurs autres en point à point.

Ces différentes topologies sont présentes dans les réseaux locaux\*. Elles sont en général mixées en fonction des besoins particuliers de l’entité. La sécurité d’un réseau repose ainsi largement sur les combinaisons de topologies mises en place. Dans les architectures hiérarchisées, les hub

et concentrateurs sont évidemment des points d’intérêts majeurs pour la sécurité.

**TOR – *The Onion Router***

TOR est un réseau décentralisé qui permet d’anonymiser les connexions sur Internet. Le principe du « routage en oignon » permet de protéger l’utilisateur de l’enregistrement de son adresse IP\* par les sites Web visités mais également réduit les risques d’analyse simple de flux. TOR fait donc transiter les paquets TCP\* par une série de routeurs\* dédiés. Les échanges entre ces routeurs sont en outre chiffrés et un « circuit » est établi entre le nœud TOR d’entrée et celui de sortie. TOR propose également des services particuliers appelés services cachés pour lesquels l’adresse IP du serveur est cachée. Celui-ci dispose d’une adresse en .onion (du type monsite.onion) et est accessible uniquement via TOR. Orienté sur la préservation de l’anonymat et la sécurité des échanges, TOR est ainsi recommandé pour tous ceux qui cherchent à se protéger des systèmes de contrôle ou de filtrage mis en place. Les journalistes, opposants politiques, activistes font donc naturellement parti du public ciblé pour l’usage de TOR. Malheureusement, ce système permet également à des réseaux criminels de développer leurs activités avec une certaines impunité. Certains « services cachés » étant de véritables marchés en ligne pour l’achat de produits stupéfiants ou encore de contrefaçon. Reposant sur le principe de préservation de l’anonymat des usagers et du contournement de la censure, TOR génère de nombreuses attentes et est régulièrement confrontés à des rumeurs de découvertes de failles de sécurité. En la matière, il convient de souligner qu’aucun système ne peut garantir une sécurité totale, de nombreux usagers de TOR ont pu être mis en cause en raison d’erreurs de comportement. Le code étant libre, les bases techniques de l’application sont connus (y compris leurs faiblesses). Pour autant, TOR demeure un outil puissant de sécurisation des usages numériques.

**Trace**

Voir Log.

**Trafic**

*(Trafic)*

Densité d'un événement donné sur un canal de transmission.

**Traitement automatique de données**

*(Automatic data processing – ADP)*

Ensemble des opérations réalisées par des moyens automatiques, relatif à la collecte, l’enregistrement, l’élaboration, la modification, la conservation, la destruction, l’édition de données et, de façon générale, leur exploitation[[239]](#footnote-240).

**Traitement de données à caractère personnel**

La Loi Informatique et Liberté présente le traitement de données à caractère personnel comme : toute opération ou tout ensemble d’opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l’enregistrement, l’organisation, la conservation, l’adaptation ou la modification, l’extraction, la consultation, l’utilisation, la communication par transmission, diffusion ou tout autre forme de mise à disposition, le rapprochement ou l’interconnexion, ainsi que le verrouillage, l’effacement ou la destruction[[240]](#footnote-241).

**Trame**

*(Frame)*

La commission générale de terminologie et de néologie définit en France une trame comme : un ensemble structuré d'éléments numériques consécutifs, spécifié par un protocole de communication.

En multiplexage\* dans le temps, une trame est un cycle du signal multiplex, constitué par les éléments numériques insérés dans les créneaux temporels d'un ensemble répétitif de créneaux temporels consécutifs. Dans la procédure HDLC\* de transmission de données, une trame comporte des champs de commande de longueur fixe qui encadrent un champ de données de longueur variable[[241]](#footnote-242).

Dans un réseau informatique une trame est l’unité de données qui circule sur la couche 2 du modèle OSI\*. Ainsi un paquet\* IP (unité de données de la couche 3) est encapsulé dans une trame pour pouvoir être acheminé.

Voir Paquet.

***Transceiver***

(Émetteur – récepteur)

En télécommunication (radio) un *transceiver* est un équipement qui assure la réception et l’émission de signaux. Dans un réseau informatique, il s’agit d’un équipement qui assure le lien entre une interface\* physique d’une station et la liaison Ethernet\* du réseau local\*.

**Transcodage**

*(transrating)*

Action qui consiste à modifier le format d’encodage d’une information (type de compression utilisée pour les fichiers audio et vidéo). Il peut ainsi s’agir de changer le débit du signal comprimé, ou le nombre de pixels sur une image.

**Transfert de paquets**

Le transfert de paquets dans un réseau est une technique générique qui consiste à transporter des blocs d’information de nœud en nœud pour les acheminer vers un récepteur[[242]](#footnote-243).

**Transfert de zone (DNS)**

(*Zone transfer*)

Le transfert de zone est un mécanisme qui permet de répliquer les données DNS\* entre serveurs. Ainsi, pour améliorer la fiabilité globale du réseau, une zone doit être servie par au moins deux serveurs (qui doivent donc disposer de la même information). Les TLD\* (*Top Level Domain*) par exemple utilisent *rsync* ou d’autres mécanismes de réplication de bases. AXFR\* qui n’est pas une norme mais un standard décrit par les RFC\* 1034 et 1035, est toutefois largement utilisé par les logiciels de serveurs de noms. AXFR se distingue du transfert incrémental (IXFR) par le fait qu’il assure une recopie complète de la base sur la base d’une transaction en mode « client-serveur » entre un serveur client dit « esclave » et un maître (nota : il y a toujours un serveur primaire maître par zone, voir RFC 2136).

**Transhumanisme**

*(Transhumanism)*

Le transhumanisme ou post-humanisme est une idéologie assez controversée, essentiellement représentée dans les sociétés occidentales, qui affirme qu’il est du devoir de l’homme d’utiliser toutes les avancées des sciences et des nouvelles technologies pour augmenter ses performances (physiques et cognitives).

Le mouvement diffuse ses théories via de nombreux relais, le plus célèbre étant la « *Singularity University*» fondée par Ray Kurzweil en Californie. Cet établissement bénéficie entre autre des financements de Google\* et, dans une moindre mesure, de la NASA. Dans le domaine de « l’homme augmenté » deux visions s’opposent, les détracteurs du transhumanisme condamnent les dérives possibles qui conduiraient à l’émergence d’une nouvelle race d’hominidé. Le monde de demain serait ainsi divisé entre deux humanités l’une biologique et l’autre formée de *cyborgs*, plus résistants, plus performants, plus rapides…

Comment et sur quels critères aura-t-on accès à cette « sur-humanité » ?

**TRANSPAC**

Transpac est un réseau à commutation de paquets\* créé en 1979 par l’opérateur national français, France Télécom. Il s’agissait d’un service public de transmission de données utilisant un réseau national suivant la norme X.25\*. Le réseau comptait 10 000 abonnés en 1981 et 45 000 en 1986. L’arrivée des technologies IP et le déploiement de l’Internet a rapidement conduit à l’abandon de TRANSPAC dont la gestion a été arrêtée le 1er octobre 2011. Quelques mois plus tard, l’opérateur Orange stoppait également l’exploitation de X.25.

**Transport** (couche)

*(Transport layer)*

De façon classique le transport désigne une fonction particulière qui assure l’acheminement des informations entre deux points appartenant à un réseau. Dans le modèle OSI\*, la couche transport (couche 4) assure cette liaison de « bout en bout » entre une source et une destination. Elle opère au niveau logique entre des processus présents sur des hôtes\* distants. Par l’intermédiaire de protocoles de transport, la couche 4 assure, les services suivants :

* Livraison fiable, en point à point\* et séquencée : via le protocole TCP\* ;
* Livraison non fiabilisée, point à point ou multicast, en mode « *best effort*» : via le protocole UDP.

**TRAU – *Transcoding Rate and Adaptation Unit***

(Unité de transcodage et d’adaptation du débit)

Unité dans un réseau GSM\* qui permet le transcodage et la conversion des signaux de 13 kb/s en signaux de 64 kb/s (et vice et versa). Cette fonction est nécessaire pour l’interconnexion avec le réseau fixe (RTC\*) dont le canal de liaison est à 64 kb/s.

**Triple DES**

Algorithme de chiffrement\* symétrique par bloc qui repose sur trois applications successives de DES\*. Développé pour dépasser les limites de DES, dont la taille de clés permettait l’attaque par force brute, triple DES consiste alors à chaîner trois chiffrements DES avec deux ou trois clés distinctes.

Voir DES.

**Trojan :** Voir Cheval de Troie.

**Troll**

Personnage de la mythologie scandinave, le troll est un être de la nuit, associé aux forces de la nature. Généralement repoussant, il a mauvais caractère et est souvent impatients. Par extension, un troll sur Internet est une personne qui intervient sur un forum, un *chat*, ou dans des commentaires, dont le seul but est de choquer, critiquer et agresser les participants. Il cherche systématiquement la polémique et génère des contre débats qui éloignent, en général du sujet principal de la conversation.

**TTL - *Time-To-Live***

(Durée de vie)

Le TTL est utilisé dans les en-têtes de paquets\* IP mais également dans les serveurs DNS\*. Dans ce dernier cas Le TTL représente la durée de rétention d’une information en mémoire cache du serveur DNS. Au delà de cette durée, la donnée est considérée comme obsolète est doit être mise à jour. Dans le cas d’un paquet IP, le TTL indique le nombre maximal de routeurs que peut traverser le paquet. Au-delà, le paquet est détruit s’il n’est pas arrivé à destination. Dans l’en-tête du paquet, un champ codé sur huit bits permet de fixer le TTL, au passage de chaque routeur, le TTL est décrémenté et le paquet détruit lorsque celui-ci arrive à zéro. Ce mécanisme permet d’éviter que des paquets ne circulent en boucle dans le réseau.

Voir ICMP, *Time Out.*

**Tunnel**

*(Tunnel)*

Un tunnel est une connexion sécurisée (chiffrée) entre deux systèmes via un réseau non contrôlé.

Voir VPN.

***Typosquatting***

(Faute de frappe opportuniste, coquille)

Action malveillante qui consiste à déposer un nom de domaine\* très proche d’un autre nom de domaine, dont seuls un ou deux caractères diffèrent[[243]](#footnote-244).

Remarques : Les objectifs de cette action sont de capter une partie du trafic adressé au site officiel.

Voir *Cybersquat*.

# U

**UAC – *Unified Access Control***

(Contrôle d’Accès Unifié)

UAC est une solution de contrôle d’accès réseau (NAC\*) développé par Juniper. *Unified Access Control* (UAC) crée et propage les stratégies dynamiques en fonction de l'identité et du rôle de l'utilisateur, du type d'équipement et de son intégrité, ainsi que de son emplacement.

*Juniper* le présente comme une solution qui assure un contrôle d'accès au réseau pour les environnements réseau, *cloud*\* et d'applications les plus complexes, (…). L'accès au réseau, au *cloud* et aux applications est basé sur les identités, en sécurisant l'accès des équipements personnels, ce qui améliore la gestion, la visibilité et le contrôle de l'accès au réseau.(…)

*Unified Access Control* s'appuie sur les normes de l'industrie, notamment 802.1X, RADIUS\*, IPsec et IF-MAP de TNC, qui permettent l'intégration de la solution UAC à n'importe quel équipement de sécurité et réseau tiers[[244]](#footnote-245).

Voir NAC.

**UCS – *Universal Character Set***

(Jeu de caractères universel)

Jeu de caractères universel défini par l’ISO 10646, permettant de coder l’ensemble des systèmes d’écriture (ou quasiment) pour faciliter leur traitement par les ordinateurs.

Voir ASCII, Unicode, UTF.

**UDP - *User Datagram Protocol***

Protocole de transport (couche 4 du modèle OSI\* ou encore couche transport du modèle TCP/IP\*), il est dit « non orienté connexion » (à l’inverse de TCP\*). UDP ne fournit donc aucune information de contrôle de flux, ni de mécanisme de correction d’erreur. Le protocole est décrit dans la RFC\* 768.

Avec TCP, UDP est le protocole de transport le plus utilisé d’Internet. Sa simplicité en fait un protocole très utile pour l’échange rapide de données qui ne craignent pas la perte d’un nombre limité de paquets\* (il est par exemple utilisé pour la voix sur IP\*). Les informations de l’en-tête UDP sont donc très limitées, et regroupées dans quatre champs distincts représentés ci-dessous :

|  |  |
| --- | --- |
| **32 bits** | |
| Port source | Port destination |
| Taille | Somme de contrôle (*checksum*) |
| Données | |

* Port Source (16 bits) : indique le port source du paquet ;
* Port destination (16 bits) : le port destination du paquet ;
* Taille (16 bits) : indique la taille du segment complet UDP (données inclues) ;
* Checksum (16 bits) : Le *checksum* ou somme de contrôle indique l’intégrité du paquet reçu.

**UIT - Union Internationale des Télécommunications**

*(ITU – International Telecommunication Union)*

Organisme international qui regroupe 193 pays et environ 700 entités du secteur privé ou du monde universitaire. L’UIT est l’organisme des Nations Unies en charge des technologies de l’information et de la communication (TIC). Il est chargé de promouvoir et de coordonner le développement des TIC et est « déterminé à connecter tous les habitants de la planète ». En outre, l’UIT attribue des fréquences radioélectriques et des orbites de satellite. Il élabore des normes techniques qui permettent l’interconnexion des réseaux. Voir le site officiel http://www.itu.int

**UML – *Unified Modeling Language***

(Langage de modélisation unifié)

Langage graphique de modélisation utilisé pour la conception de logiciels, UML permet de représenter, à l’aide de diagrammes, un logiciel en cours de développement. Le langage comprend 14 diagrammes regroupés en trois familles distinctes. On trouve ainsi :

* des diagrammes structurels (ou statiques), qui permettent de représenter des classes ou des objets ;
* des diagrammes comportementaux, pour représenter les activités, les états ou les interactions entre les utilisateurs et le système ;
* et les diagrammes d’interactions dynamiques, qui modélisent les échanges entre objets, ou les représentions séquentielles des interactions.

UML est un standard de l’OMG – *Object Management Group* très utilisé pour la conception d’applications orientées objet.

Voir Programmation orientée objet.

**UMTS - *Universal Mobile Telecommunication System***

(Système de télécommunication mobile universel)

UMTS est une norme de télécommunication mobile pour les systèmes de radiocommunication dits de troisième génération (3G). Cette norme a été retenue en Europe elle reprend les spécifications d’IMT 2000\*. UMTS, basée sur une technologie d’accès radio de type WCDMA\*, permet d’élargir la gamme de service en intégrant les échanges de données et d’images en plus de la voix. Ces services sont rendus possible par une augmentation de la bande passante\* de chaque cellule qui dérive de l’amélioration du codage des signaux et permet la réutilisation de fréquences entre cellules adjacentes sans interférences.

**UMTS -TDD - *Universal Mobile Telecommunication System Time Division Duplex***

Variante d’UMTS qui propose en lieu et place de la division par fréquence (FDD\*) du WCDMA\*, une division temporelle. UMTS-TDD utilise deux bandes de fréquences séparées du spectre (1900 – 1929 MHz et 2010 – 20125 MHz). En France, la plupart des fréquences UMTS-TDD ne sont pas accessibles au public et réservées à un usage professionnel.

**UNI - *User to Network Interface***

UNI est un protocole de signalisation\* dans les réseaux ATM\*. Il permet d’établir une connexion entre deux utilisateurs terminaux du réseau. UNI est normalisé par l’ISO sous l’appellation Q2931 UNI *Signalling*.

Le *user to network interface* désigne également l’interface de raccordement entre un commutateur ATM\* et un utilisateur. L’interface de raccordement entre les commutateurs ATM est appelée NNI\* *Network to Network Interface.*

Voir NNI.

**Unicast**

*(Envoi individuel)*

Unicast est un mode de transmission point à point\* qui consiste à communiquer entre deux hôtes distincts d’un réseau identifiés par leur adresse (d’un émetteur unique vers un destinataire unique). L’adresse IP\* étant unique elle permet ce mode de transmission. Il existe d’autres modes de transmission dans un réseau : le *multicast* (diffusion d’un émetteur vers un groupe de récepteurs) et le *broadcast* (diffusion d’un émetteur vers tous les récepteurs potentiels).

Voir Multicast, Broadcast.

**Unicode**

Pour permettre à un processeur d’interpréter un caractère, il est nécessaire de le coder et de lui faire correspondre un nom unique et un nombre entier positif qui sera lui même manipulé sous forme binaire (d’ou le mécanisme de transformation UTF). Dans ce contexte, Unicode est un standard qui assure le codage de caractères dans n’importe quel système d’écriture au niveau mondial. Unicode permet le codage d’environ 110 000 caractères différents, il est compatible avec la norme ISO 10646 (il permet de coder le jeu universel de caractères – *Universal Character Set* – UCS).

Voir ASCII, UTF.

**URI - *Uniform Resource Identifier***

(Identificateur Uniforme de Ressources)

L’URI est un chaine de caractères qui permet d’identifier une ressource sur un réseau. L’URI est présentée dans le RFC\* 3986. Elle est très répandue pour définir et localiser une ressource sur Internet. Il existe deux types d’URI :

L’URL, *Uniform ressource locator* (voir ci-dessous) et l’URN, *Uniform ressource name.*

Voir URL, URN.

**URL - *Uniform Resource Locator***

(Adresse réticulaire – adresse universelle)

L’URL est une URI\*, donc un format de nommage commun, qui désigne une ressource sur Internet. Il permet de « localiser » cette ressource et ainsi d’y accéder. Le format d’une URL est décrit une première fois en 1994 dans la RFC\*1738.

**URN – *Uniform Ressource Name***

Forme particulière d’URI\* qui permet d’identifier une ressource dans un espace de nommage et non par sa localisation. L’URN permet donc de parler d’une ressource ou d’un objet sans avoir d’information sur sa localisation (dans un réseau) ou le moyen d’y accéder. Le code ISBN est un exemple d’URN pour les livres. Il permet de classer les ouvrages dans une base de noms sans pour autant utiliser les titres. L’ISBN est plus simple à manipuler.

**USB - *Universal Serial Bus***

(Bus série universel)

Interface entrée-sortie d’un équipement basé sur l’architecture série[[245]](#footnote-246). Le port USB permet donc la connexion de nombreux périphériques différents. Il existe trois versions d’USB en fonction de l’évolution des débits.

• USB 1.0 : 12 Mb/s

• USB 2.0 : 480 Mb/s

• USB 3.0 : 4,8 Gb/s

Voir Clé USB.

**USENET  - UNIX user network**

Usenet, abréviation de UNIX *user network*, est un réseau de forums, aujourd’hui interconnecté à l’Internet, qui utilise le protocole NNTP. Il permet la diffusion et la lecture de contenus associés à des communautés d’intérêts.

**Usurpation d’adresse**

*(Address spoofing)*

Action malveillante qui consiste à utiliser délibérément l’adresse d’un autre système en lieu et place de la sienne.

Remarques : Il faut rapprocher cette action de l’usurpation d’identité, considérée comme un délit par le droit pénal français. L’idée est de faire passer son système d’information pour un autre. L’adresse usurpée peut être une adresse MAC\* (pour *Medium Access Control*), une adresse IP\*, une adresse de messagerie, etc[[246]](#footnote-247).

Voir Mystification – *spoofing*.

**UTF – *Unicode Transformation Format***

UTF est un système qui permet la transformation de tout point de code du répertoire universel de caractères définit par la norme ISO 10646. Unicode\* permet le codage des caractères dans l’ensemble des systèmes d’écriture, chaque caractère se voit attribuer un nom unique et un nombre entier positif. Ce dernier constitue le « point de code ». UTF – 8 est ainsi un standard de l’internet (STD 63) compatible avec ASCII qui assure la transformation des points de code sur 8 bits, il est utilisé par environ 90% des sites Internet. UTF-8 est un format de transformation de la norme ISO 10646, il est standardisé par la RFC\* 3629.

Voir Unicode, ASCII.

# V

1. **Valence**
2. *(Valance)*
3. En théorie du signal, la valence d’un signal modulé est le nombre *m* de moments de la porteuse\* modulée. C’est à dire le nombre d’états significatifs d’un signal. De façon concrète, les signaux transmis ont en général des valences d’ordre 2n où n est le nombre de bits nécessaires pour décrire ces états en binaire.
4. **VBR - *Variable bit rate***
5. (Débit variable)
6. Le VBR est une technique d’échantillonnage du signal qui s’oppose au CBR – *constant bit rate*. Dans le cas du VBR, le nombre d’échantillons varie en fonction du contexte du signal (il n’est donc pas une constante). Le VBR est utilisé pour l’encodage de fichiers multimédias car il permet de trouver des compromis entre les besoins en bande passante\*, la taille du fichier et la qualité du signal reçu.
7. Voir Echantillonnage.
8. **Ver informatique**
9. *(Worm)*
10. Programme malveillant s’auto reproduisant à travers le réseau mais n’infectant pas forcément d’autres programmes. Le ver se propage au sein du réseau (par l’envoie de copie de lui-même). Un ver est donc un virus\* qui se propage au sein du réseau et, par voie de conséquence provoque des nuisances (il peut saturer la bande passante\* par exemple).
11. Voir Logiciel malveillant.
12. **Virtuel**
13. *(Virtual)*
14. Dans sa définition la plus technique, un objet « virtuel » est un objet qui ne correspond pas à une configuration physique. Ainsi, on pourrait établir un circuit virtuel direct entre A et B sans pour autant qu’il existe une configuration physique, donc un lien direct, entre A et B. Le circuit est virtuel, il doit être établi (mode connexion) sur la base d’informations d’adressage (source et destination) qui doivent accompagner le message.
15. Dans les usages plus courants, le terme virtuel s’oppose à réel, il est ainsi utilisé pour décrire les activités en ligne et tout ce qui ne se rattache pas à une réalité physique.
16. ***Vine***
17. Application sociale qui permet l’échange de courtes vidéos (six secondes). Vine appartient à *Twitter* mais est une application distincte.
18. **Virus**
19. *(Virus)*
20. Un virus est un programme ou morceau de programme malveillant dont le but est de survivre sur un système informatique (ordinateur, serveur, appareil mobile, etc.) et, bien souvent, d’en atteindre ou d’en parasiter les ressources (données, mémoire, réseau). Le mode de survie peut prendre plusieurs formes : réplication, implantation au sein de programmes légitimes, persistance en mémoire, etc. Pour sa propagation, un virus utilise tous les moyens disponibles : messagerie, partage de fichiers, portes dérobées, page internet frauduleuse, clés USB[[247]](#footnote-248)…
21. Voir Logiciel malveillant
22. **Virus polymorphe**
23. *(Polymorphic virus)*
24. Un virus polymorphe est un virus dont l’apparence change dans le temps (à chaque infection). Cette caractéristique rend le virus plus difficilement détectable par un anti-virus. Typiquement en changeant de forme, le virus change également de signature\* et donc ne permet plus une détection fondée exclusivement sur une analyse par signature.
25. Pour y parvenir, une méthode consiste à chiffrer le corps du virus avec une clé différente à chaque infection. Ainsi la partie principale du virus a une apparence différente. Le virus embarque également une « routine de déchiffrement » qui doit prioritairement donner l’ordre de déchiffrer le corps principal du virus pour qu’il soit opérationnel (sinon tous cela ne sert pas à grand-chose). Cette boucle de déchiffrement change également (sous peine d’être potentiellement détectable par un anti-virus). Pour assurer cette modification aléatoire de la routine de déchiffrement, le virus insère également des instructions légitimes mais inutiles dans son code (ces instructions sont choisies parmi les routines connues).
26. Voir Signature de virus, Logiciel malveillant, Marqueur.
27. **VLAN - *Virtual Local Area Network***
28. (Réseau local virtuel)
29. Un réseau local virtuel est un ensemble de stations appartenant au même réseau local reliées de façon logique. Les stations peuvent appartenir à des segments physiques différents.
30. **VLR - *Visitor Location Register***
31. La VLR est un élément de l’architecture d’un réseau de téléphonie mobile. La VLR est une base de donnée qui contient les informations sur les usagers présents dans la zone de couverture de la MSC\*. Il y a donc une VLR par MSC.
32. Par rapport à la base centrale contenue dans le HLR\*, la VLR enregistre le TMSI\* - *temporary mobile subscriber identity* (identité temporaire d’un utilisateur).
33. Voir GSM, MSC, VLR
34. **VLSM - *Variable-Length Subnet Mask***
35. (Masque de sous-réseau de longueur variable)
36. Dans le système d’adressage IP\*, la notion de sous-réseau a été introduite, en 1984, par la RFC\* 917. Il permet une utilisation plus flexible de l’espace d’adressage (initialement au sein d’une même classe d’adresse) en permettant la création de sous-réseaux par l’utilisation d’un masque. Le masque de sous-réseau est de même longueur qu’une adresse IP et permet de définir un espace d’adressage propre. A partir de 1992, et la RFC 1338, il est proposé d’abandonner la notion de classe (Voir *Pour aller plus loin* Adresse IP). Outre l’utilisation du *Classless Inter-Domain Routing* (CIDR) qui diminue la taille des tables de routage\*, on développe des masques de longueur variable (VLSM) afin d’optimiser l’espace d’adressage (celui-ci étant découpé en blocs de taille variable).
37. Voir Adresse IP.
38. **VOD – *Video On Demand***
39. (Vidéo à la demande)
40. Service qui permet de visionner des flux vidéos directement sur une télévision sans nécessairement télécharger le fichier complet.
41. **Voie**
42. *(Channel).* Voir Canal de transmission.
43. **Voix sur IP**  
    *(VoIP)*
44. L’expression voix sur IP (VoIP) désigne les mécanismes qui consistent à acheminer sur un canal de communication, une conversation vocale en utilisant le protocole IP.
45. Voir ToIP, téléphonie sur IP.
47. **VPN - *Virtual Private Network***
48. (Réseau Privé Virtuel - RPV)
49. Le concept de réseau privé virtuel repose sur l’utilisation de réseaux ouverts (non-sécurisés) par un groupe d’utilisateurs. Ainsi, lorsqu’une entreprise, qui dispose d’un réseau privé (LAN\*), souhaite interconnecter des sites distants, elle peut utiliser Internet pour acheminer les données. Cet usage non sécurisé a conduit à développer le concept de réseau privé virtuel où les données sont « encapsulées » entre les deux sites, créant ainsi l’illusion d’appartenir au même LAN. Des solutions VPN sont également très utilisées dans des contextes de nomadisme des employés.
50. **VPS - *Virtual Private Server***
51. (Serveur privé virtuel)
52. Appelé également serveur dédié virtuel (*Virtual Dedicated Server* VDS), un VPS est une partition virtuelle d’un serveur d’hébergement. Il s’agit donc d’une machine virtuelle qui se comporte comme un serveur dédié. Les VPS permettent d’héberger des sites WEB ou des applications logicielles (e-commerce, extranet, *wiki*). Par rapport à une solution d’hébergement mutualisé, le VPS permet une plus grande souplesse de gestion. Un accès *root* (avec une connexion SSH) ainsi qu’un accès au PHP\* *init* (qui permet de modifier les variables PHP) assurent à l’utilisateur un contrôle avancé sans pour autant assumer la responsabilité d’un serveur physique dédié. Toutefois, les solutions de VPS, qui reposent donc sur la mutualisation d’une infrastructure physique, doivent être adaptées aux besoins du client en matière de ressources nécessaires aux applications hébergées. La plupart des hébergeurs offrent des solutions VPS.
53. **VSAT - *Very Small Aperture Terminal***
54. Le terme VSAT désigne initialement le terminal émetteur - récepteur satellite permettant l’échange de données. Il regroupe aujourd’hui un système non normalisé de communication par satellite qui repose sur une architecture avec un site principal (le *hub\**) et des sites distants multiples (les stations VSAT). Ces dernières ne prennent aucune décision dans la gestion du réseau (qui relève du hub). Cette caractéristique permet le déploiement rapide d’un réseau avec des terminaux relativement peux couteux. La VSAT peut aujourd’hui être utilisée pour déployer un réseau de transmission de données, de téléphonie, de télévision et d’accès Internet. La particularité d’une VSAT réside dans la gestion de la bande passante (qui reste d’un coût important). Les trois bandes de fréquences allouées à la VSAT sont connues sous les dénominations de bande C, bande Ku et bande Ka.
55. **Vulnérabilité**
56. *(Vulnerability)*
57. En sécurité informatique, une vulnérabilité ou faille de sécurité caractérise une faiblesse dans un système informatique permettant de modifier son fonctionnement normal. Les vulnérabilités logicielles sont la conséquence d’erreurs de programmation (involontaires) ou volontaires (réalisées avec la volonté de nuire). Une fois découvertes, les failles sont publiquement documentées et des correctifs peuvent alors être déployés (patch). Il est donc essentiel de maintenir à jour ses applications pour se prémunir d’une attaque utilisant une vulnérabilité connue.
58. Le glossaire de l’ANSSI[[248]](#footnote-249) en donne la définition suivante :
59. Faute, par malveillance ou maladresse, dans les spécifications, la conception, la réalisation, l'installation ou la configuration d'un système, ou dans la façon de l'utiliser.
60. Une vulnérabilité peut être utilisée par un code d’exploitation\* (*exploit)* et conduire à la compromission d’un système.
61. De plus en plus de chercheurs en sécurité découvrent des vulnérabilités, ainsi pour l’année 2014, l’entreprise Secunia a recensé près de 15 435 vulnérabilités dans environ 3870 applications différentes[[249]](#footnote-250).
62. Les vulnérabilités sont classées en fonction de leur criticité suivant un système de notation qui permet de caractériser leur impact. Ce système est appelé CVSS\* (*Common Vulnerability Scoring System*).

# W

1. **W3C - *World Wide Web Consortium***
2. Organisme qui vise à proposer des normes et protocoles\* ouverts et libres pour assurer une interopérabilité maximale. L’objectif de W3C se retrouve dans sa devise « Un Web pour tous et partout ». Créé par Tim Berners-Lee (co-créateur du Web) en 1994, le consortium regroupe environ 400 entreprises partenaires.
3. **WAN - *Wide Area Network***
4. (Réseau étendu)
5. Un WAN est un réseau étendu, fédérateur, qui regroupe plusieurs sites éloignés. Sa définition est peu précise et l’expression désigne le plus souvent un réseau qui est constitué de l’interconnexion de plusieurs réseaux élémentaires.
6. **WAP - *Wireless Application Protocol***
7. Protocole\* de communication qui permet à des terminaux mobiles de se connecter à internet. Il permet à un utilisateur GSM\* d’accéder à Internet via une passerelle. Cette dernière, par l’intermédiaire d’un serveur WAP redéfinit les formats de présentation HTML\* pour les rendre compatibles avec les terminaux (WML – *Wireless Markup Language* ou XHTML).
8. Voir également xHTML.
9. **WCDMA - *Wideband Code Division Multiple Access***
10. (Multiplexage par code large bande)
11. Dans un réseau de téléphonie mobile, le WCDMA est une technologie utilisée par la partie accès\* radio du réseau. Avec WCDMA, les utilisateurs émettent tous sur un même canal radio (large bande) et sont discriminés par un code distinct partagé avec le récepteur. Ce code est une séquence d’étalement pseudo-aléatoire. WCDMA utilise les bandes de fréquence de l’UMTS\*. Le WCMA correspond à de la téléphonie « 3G » (IMT 2000\*), il est progressivement remplacé par l’ OFDMA (*Orthogonal Frequency Division Multiple Access)* et SC-FDMA (*Single Carrier – Frequency Division Multiple Access)* pour la 4G LTE\* et LTE Advanced.
12. Voir Accès multiple.
13. **Web**
14. (Toile)
15. Le *Web* est l’appellation courante du *World Wide Web (WWW)*, et désigne de façon impropre l’Internet.
16. Voir WWW.
17. **WEP - *Wired Equivalent Privacy***
18. WEP est un protocole\* de sécurité défini en 1999 pour la norme 802.11b (réseau sans fil Wi-fi\*). Il sécurise les échanges entre un point d’accès sans-fil et un terminal. Ce protocole est aujourd’hui considéré comme faible et plusieurs failles ont été mises à jour. Il est déconseillé de l’utiliser et il convient de privilégier WPA 2.
19. Voir WPA.
20. ***White List -* WL**
21. (Liste blanche)
22. Liste qui recense les entités qui disposent de privilèges particuliers. Ainsi, on peut regrouper les sites, qui ne doivent pas faire l’objet de mesures de filtrage, les usagers ou noms de domaines. Voir Filtrage, ACL.
23. **Wi-Fi - *Wireless Fidelity***
24. Protocole de communication sans fil, le Wi-Fi est normalisé par l’IEEE sous la dénomination 802.11. Il permet des échanges de données\* sur une distance de quelques dizaines de mètres. La connexion d’équipements permet de créer un réseau local sans-fil (WLAN\* – *Wireless Local Area Network*). En fonction de la norme implémentée, un réseau Wi Fi supporte le haut débit.
25. • 802.11b : 6Mbit/s – 11 Mbit/s théorique
26. • 802.11g : 25 Mbit/s
27. • 802.11n : 600 Mbit/s théorique
28. • 802.11ac : 1,3 Gbit/s théorique
29. La norme 802.11 définit deux modes principaux :
30. Le mode infrastructure, mode par défaut, dans lequel les stations se connectent sans-fil au réseau via le point d’accès (*access point*) ;
31. Le mode *ad hoc,* pour lequel les stations sont interconnectées sans point d’accès.
32. Ce type de réseau est largement répandu pour un usage domestique via l’utilisation de « box » louées par les fournisseurs d’accès internet (FAI\*). En outre de plus en plus de « *hotspot* Wi-Fi », points d’accès publics, permettent de se connecter en haut débit à l’Internet dans les lieux publics, ou certains commerces et hôtels. En matière de sécurité, la prolifération de ces réseaux « ouverts » est problématique dans la mesure où l’utilisateur peut faire l’objet d’une surveillance, à son insu, via le point d’accès. S’il n’utilise pas un VPN\*, ses paramètres de connexion (login et mot de passe) peuvent être subtilisés par un simple *snif* réseau.
33. ***Wiki***
34. Application Web\* collaborative qui permet de créer, modifier et consulter des pages Web. Un Wiki est donc un outil de gestion de contenus qui est principalement utilisé pour regrouper et échanger des informations au sein d’une communauté. Le site *Wikipedia* (encyclopédie en ligne alimentée par les internautes) est un exemple de *wiki*.
35. **WiMAX - *Worldwide Interoperability for Microwave Access***
36. Protocole\* de communication normalisé IEEE 802.16, le WiMAX permet de raccorder des clients terminaux à un réseau haut débit d’opérateur. Il permet ainsi de relier des *hotspots* Wi-Fi et est commercialisé comme une alternative aux réseaux câblés (fibre optique) et ADSL\*. Il repose sur une architecture avec une station de base (portée environ 10km) et des clients. Le WiMAX permet ainsi de couvrir des zones non reliées à l’ADSL ou au câble, et s’avère une option utile dans le cas de certaines communautés rurales.
37. **WLAN - *Wireless Local Area Network***
38. (Réseau local sans fil)
39. L’expression WLAN regroupe l’ensemble des technologies permettant de constituer un réseau local\* d’équipements interconnectés sans fil. La taille d’un WLAN est nécessairement réduite (usage domestique ou site de taille limité). Les technologies les plus rependues sont regroupées dans l’ensemble 802.11 (qui décrit les modalités d’utilisation des deux premières couches du modèle OSI\*). Le WiFi\* est par exemple, une technologie de WLAN.
40. **WPA - *Wi-Fi Protected Access***
41. Mécanisme de sécurité mis au point en avril 2003 pour remplacer le WEP\* dans la sécurisation des connexions Wi-Fi\*. Son évolution, en 2004, WPA2 répond aux spécifications de la norme IEEE 802.11i. Alors que WPA repose sur le protocole de chiffrement TKIP\* – *Temporal Key Integrity Protocol*, WPA2 fait lui le choix de CCMP – *Counter mode, CBC Mac Protocol*. Pour TKIP, la clé de 128 bits est générée aléatoirement pour chaque paquet\*. CCMP est lui basé sur AES\*, il permet de vérifier l’intégrité des messages (par l’intermédiaire d’un code d’authentification\*) ainsi qu’un chiffrement sûr en évitant les faiblesses liées à la génération de vecteurs d’initialisation (comme pour WEP par exemple).
42. Voir WEP.
43. **WPAN - *Wireless Personnal Area Network***
44. (Réseau sans fil personnel)
45. Un WPAN est un réseau personnel sans fil de courte portée. Il est déployé essentiellement pour relier des périphériques à une station. La technologie *bluetooth,* par exemple, permet l’établissement d’un WPAN mais également des liaisons infrarouges.
46. **WWW - *World Wide Web***
47. Le *World Wide Web* (WWW), appelé trivialement « le Web », littéralement la toile, est un système hypertexte\* qui fonctionne sur le réseau Internet en utilisant le protocole HTTP\* (sur la couche applicative du modèle OSI\*). Ce protocole\* permet à l’aide d’un navigateur de consulter des pages stockées sur des serveurs. Issu des recherches conduites au CERN par, Tim Berners-Lee et Robert Cailliau le Web ouvrit sa première adresse publique en 1993. Dès la création, on annonça qu’il serait libre d’utilisation pour le monde, posant ainsi les bases d’un des mythes fondateur de l’Internet.

# X

1. **X**
2. La lettre X est utilisée comme préfixe par le CCITT (Comité consultatif international téléphonique et télégraphique) devenu UIT-T\* (Voir UIT) pour ses recommandations dans le domaine des réseaux.
3. On peut ainsi citer par exemple:
4. • X.500 : norme qui définit les services d’annuaire (modèles de services, organisation) ;
5. • X.501 : modèles d’annuaires ;
6. • X.509 : systèmes d’authentification
7. • X.518 : annuaires distribués ;
8. • X.519 : Protocoles ;
9. • X.525 : la réplication d’annuaires.
10. **X.25**
11. X.25 est un protocole\* réseau pour la commutation de paquets point à point\*. Il définit le mode d’échange de données (comme TCP\*) mais ajoute un contrôle de flux entre les terminaux (les DTE – *Data Terminal Equipment*) ou entre les nœuds (les DCE – *Data Communications Equipment*). Au niveau paquet, X.25 prend en charge la notion de circuit virtuel et assure la distribution des données dans l’ordre d’émission. Ce dernier aspect est une fonction très utile des réseaux X.25 mais entraine un taux de transfert relativement lent (moins de 64kb/s).
12. En France X.25 était utilisé pour les services Minitel, la commercialisation a pris fin en 2012. X.25 est ainsi supplanté par les réseaux TCP/IP\*.
13. **xDSL – *x Digital Subscriber Line***
14. (Ligne d’abonnés numérique)
15. xDSL regroupe l’ensemble des technologies d’accès numérique d’abonnés. Il permet d’établir des liaisons par l’intermédiaire du réseau câblé cuivre (ligne téléphonique analogique). xDSL regroupe ainsi plusieurs normes de transmissions de données à haut débit telle que:
16. • ADSL\* (Asymetric Digital Subscriber Line) ;
17. • SDSL (Symmetric Digital Subscriber Line) ;
18. • HDSL (High bit rate Digital Subsriber Line).
19. **XKMS – *XML key management system***
20. (Système de gestion des clés XML)
21. Recommandation du W3C\* du 28 juin 2005, XKMS est un protocole\* d’enregistrement de clés\* publiques entre applications et services du Web. Il permet la gestion d’une infrastructure à clé publique (PKI\*) permettant de sécuriser les échanges. La spécification regroupe un protocole pour l’enregistrement, le renouvellement et la révocation des clés (XKRSS – XML *Key Registration Service Specification*) et un second assurant la validation des clés publiques (XKISS – XML *Key Information Service Specification*).
22. Voir Clé de chiffrement, PKI.
23. **XLL - *eXtensible Link Language***
24. Dans un document au format XML\*, le XLL est un langage qui permet de spécifier et gérer des liens (internes ou externes) au document.
25. **XML - *eXtensible Markup Language***
26. XML est un format de notation qui permet de structurer les informations pour faciliter leur traitement. Un document XML se caractérise par l’usage de balises qui encadrent l’information. Dans une page XML il est possible d’imbriquer des balises, donc de hiérarchiser les informations, et de définir des balises propres. HTML\* utilise, par exemple, la syntaxe XML.
27. **XOR – *eXclusive OR***
28. Opérateur logique booléen dit « OU exclusif ». Le OU exclusif donne 0 si les deux valeurs comparées sont à 0 ou à 1. Il vaut 1 dans les autres cas.
29. On utilise la notation ⊗ ou ⊕.
30. Cet opérateur est très utilisé dans les fonctions cryptographiques et en informatique.

# Z

1. **Zero-day (0-day)**
2. Un « *zero-day*» est une vulnérabilité sur un système n’ayant jamais fait l’objet d’une publication ou d’un correctif. Ces vulnérabilités garantissent donc à celui qui en dispose un avantage immédiat qui permet une exploitation malveillante. Mais cette situation est très volatile puisque le « *zero-day*» et son ou ses exploits associés perdent de leur intérêt dès lors que la communauté de la sécurité informatique découvre la vulnérabilité. Une fois dévoilée, elle est documentée et les correctifs sont apportés (normalement).
3. **Zombie**
4. *(Zombie)*
5. Système informatique compromis (infecté) répondant aux commandes d’un pirate (on parle également de maître).
6. Voir *Botnet*, Logiciel malveillant.

# Acronymes

1. ACL : *Acces Control List.*
2. ACSSI :Article Contrôlé de la sécurité des informations.
3. ADSL : ***Asymmetrical Digital Subscriber Line***
4. AES : *Advanced Encryption Standard*
5. AET : *Advanced Evasion Techniques.*
6. AFF : *Advanced Forensic Format.*
7. AFNIC : Association Française pour le Nommage Internet en Coopération.
8. AFNOR : Association Française de NORmalisation
9. AMRC : Accès Multiple par répartition en code.
10. AMRF : Accès Multiple par répartition en fréquence.
11. AMRT : Accès multiple par répartition temporelle.
12. ANFR : Agence Nationale des Fréquences.
13. ANSSI : Agence Nationale de la Sécurité des Systèmes d’Information.
14. API : *Application Programming Interface.*
15. APT : *Advanced Persistant Threat.*
16. ARPANET : *Advanced Research Projects Agency NETwork.*
17. ASCII : *American Standard Code for Information Interchange.*
18. AuC : *Authentication Center.*
19. BAN : *Body Area Network.*
20. BECN : *Backward explicit congestion notification.*
21. BGP : *Border Gateway Protocol.*
22. BI : *Business Intelligence*.
23. BIOS : *Basic Input Output System.*
24. BSC : *Base Station Controller.*
25. BSS : *Base Station Subsystem.*
26. BTS : *Base Transceiver Station.*
27. CA : *Certification Auhority.*
28. CALID : Centre d’Analyse et de Lutte Informatique Défensive.
29. CAPEC : *Common Attack Pattern Enumeration and Classification.*
30. CASE : *Common Application Services Elements.*
31. CBAC : *Context-Based Access Control*.
32. CBC : *Cypher block chain.*
33. CBR : *Constant Bit Rate.*
34. CC : *Creative Commons.*
35. CCC : *Chaos Computer Club.*
36. CDMA : *Code Division Multiple Access.*
37. CDN : *Content Delivery Network.*
38. CEI : Commission Electrotechnique Internationale.
39. CEN : Comité Européen de Normalisation.
40. CERT : *Computer emergency response team.*
41. CFB : *Cipher FeedBack.*
42. CFU : *Call Forwarding Unconditional.*
43. CIDR : *Classless Inter-Domain Routing.*
44. CMS : *Content Management System.*
45. CNA : *Computer Network Attack*.
46. CNE : *Computer Network Exploitation*.
47. CNIL : Commission Nationale Informatique et Liberté.
48. CNO : *Computer Network Operation*.
49. COIN : Contre insurrection.
50. CPE : *Common Platform Enumeration.*
51. CPL : Courant Porteur en Ligne.
52. CSMA/CD : *Carrier Sense Multiple Acces with Collision Detection.*
53. CSS : *Cascading Style Sheets.*
54. CTR : *Common Technical Regulation.*
55. CVE : *Common Vulnerabilities and Exposure.*
56. CVSS : *Common Vulnerability Scoring System.*
57. CWE : *Common Weakness Enumeration.*
58. DARPA : *Departement of Advanced Research Projects Agency.*
59. DCS : *Digital Communication System.*
60. DDOS : *Distributed Deny Of Service.*
61. DECT : *Digital Enhanced Cordless Telecommunication.*
62. DEFCON : *Defense Condition.*
63. DEP : *Data Execution Prevention.*
64. DES : *Data encryptions Standard.*
65. DHCP : *Dynamic Host Configuration Protocol.*
66. DLCI : *Data Link Channel Identifier.*
67. DLL : *Dynamic Link Library,* bibliothéque de liens dynamique.
68. DMZ : *DeMilitarized Zone.*
69. DNS : *Domain Name System*.
70. DOS : *Deny Of Service.*
71. DPI : *Deep packet inspection.*
72. DRM : *Digital Right Management.*
73. DSS : *Digital Signature Standard.*
74. EAP : *Extensible Authentication Protocol.*
75. EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité.
76. EFF : *Electronic Fontier Foundation.*
77. EGP : *Exterior Gateway Protocol.*
78. EIGRP : *Enhanced Interior Gateway Routing Protocol.*
79. EIR : *Equipment Identity Register.*
80. EIR : *Excess Information Rate.*
81. ENISA : *European Network for Information Security Agency.*
82. ESN : Entreprise de Service du Numérique.
83. ESSID : *Extended Service Set Identifier.*
84. ETCD : Equipement de Terminaison de Circuits de Données.
85. ETSI : *European Telecommunications Standard Institute.*
86. ETTD : Equipement Terminal de Traitement de Données.
87. FAI : Fournisseur d’Accès à Internet.
88. FDM : *Frequency Division Multiplexing.*
89. FDMA : *Frequency Division Multiple Access.*
90. FEC : *Forwarding Equivalence Class.*
91. FECN : *Forward Explicit Congestion Notification.*
92. FH : *Frequency Hopping.*
93. FHSS : *Frequency Hopping Spread Spectrum*.
94. FIFO : *First in First out.*
95. FM : *Frequency Modulation.*
96. FPS : *Fast Packet Switching.*
97. FTP : *File Transfert Protocol.*
98. GAFA : *Google, Apple, Facebook, Amazon.*
99. GGSN : *Gateway* GPRS *Support Node*.
100. GMSC : *Gateway Mobile Switching Center.*
101. GMSK : *Gaussian Minimum Shift Keying.*
102. GPRS : *General Packet Radio Service.*
103. GRE : *Generic Routing Encapsulation.*
104. GSM : *Global System for Mobile Communications.*
105. HD : Haut débit
106. HDLC : *Hight level Data Link Control.*
107. HIDS : *Host Intrusion Detection System.*
108. HIPS : *Host-based Intrusion Prevention System.*
109. HLR : *Home Location Register.*
110. HSDPA : *High Speed Download Packet Access*
111. HSN : *Hopping Sequence Number.*
112. HSUPA : *High Speed Uplink Packet Access.*
113. HTML : *HyperText Markup Language.*
114. HTTP : *Hypertext transfer protocol*.
115. HTTPS : *Hypertext transfer protocol secured.*
116. IAB : *Internet Activities Board.*
117. IAB : *Internet Architecture Board.*
118. IANA : *Internet Assigned Numbers Authority.*
119. ICANN : *Internet Corporation for Assigned Names and Numbers.*
120. ICMP : *Internet Control and error Message Protocol.*
121. IDoT : *Identity of things.*
122. IDP : *Internet Datagram Protocol*
123. IDS : *Intrusion Detection Systems*,
124. IEC : *International Electrotechnical Commission.*
125. IEEE : *Institute of Electrical and Electronics Engineers.*
126. IETF : *Internet Engineering Task Force.*
127. IGP : *Interior Gateway Protocol.*
128. IHM : Interface Homme Machine.
129. IMEI : *International Mobile Station Equipment Identity.*
130. IMS : *IP Multimédia Subsystem.*
131. IMSI : *International Mobile Subscriber Identity.*
132. IMT 2000 : *International Mobile Telecommunications 2000.*
133. IOT : *Internet Of Things.*
134. IPBX : *Internet Protocol-Private Branch Exchange.*
135. IPS - *Intrusion Prevention System.*
136. IPSEC : *Internet Protocole Security.*
137. IRTF : *Internet Research Task Force.*
138. ISDN : *Integrates Services Digital Network.*
139. IS-IS : *Intermediate Sytem to Intermediate System.*
140. ISL : *Inter Switch Link.*
141. ISO : *International Standard Organisation.*
142. ISOC : *Internet SOCiety.*
143. ISTAR : *Intelligence, surveillance, target acquisition, and recon­naissance.*
144. ITA : Information Technology Agreement.
145. ITIL : *Information Technology Infrastructure Library.*
146. ITU : *International Telecommunication Union*.
147. IXFR : *Incremental Zone Transfer.*
148. J2SE : *Java 2 Standard Edition.*
149. J2EE : *Java 2 Entreprise Edition.*
150. J2ME : *Java 2 Micro Edition.*
151. JPEG : *Joint Picture Expert Group.*
152. JS : *Java Script.*
153. JSON : *JavaScript Object Notation.*
154. LA : *Location Area.*
155. LAC : *Location Area Code.*
156. LAI : *Location Area Identification.*
157. LAN - *Local Area Network.*
158. LAP - *Link Access Protocol*.
159. LAPB : *Link Access Protocol D-channel.*
160. LAPD : *Link Access Protocol D-channel.*
161. LCP : *Link Control Protocol.*
162. LDAP : *Lightweight Directory Access Protocol.*
163. LDP : *Label Distribution Protocol.*
164. LIB : *Label Information Base.*
165. LLC : *Logical Link Control.*
166. LMI : *Local Management Interface.*
167. LSR : *Label Switching Router*.
168. LTE : *Long Term Evolution.*
169. MA : *Mobile Allocation.*
170. MAC : *Media Access Control.*
171. MAEC - *Malware Attribute Enumeration and Characterization.*
172. MAIO : *Mobile Allocation Index Offset.*
173. MAN : *Metropolitan Area Network*
174. MBR : *Master Boot Record.*
175. MCC : *Mobile Country Code.*
176. MD5 : *Message Digest 5.*
177. MGCF : *Media Gateway Control Function.*
178. MIB (SNMP) : *Management Information Base.*
179. MIC : Modulation par Impulsions Codées.
180. MIME : *Multipurpose Internet Mail Extensions.*
181. MIMO : *Multiple Input / Multiple Output*.
182. MISO : *Multiple In / Single Out*.
183. MNC : *Mobile Network Code.*
184. MMF : *Multimode Fiber.*
185. MMS : *Multimedia Messaging Service.*
186. MML : *Man Machine Language.*
187. MOA : Maitrise d'OuvrAge.
188. MOE : Maitrise d’œuvre.
189. MOSPF : *Multicast extension Open Shortest Path First.*
190. MPLS - *MultiProtocole Label Switching.*
191. MSC : *Mobile Switching Center.*
192. MSIN : *Mobile Subscriber Identification Number.*
193. MSISDN : *Mobile station ISDN number.*
194. MTA : *Message Transfer Agent*.
195. MTBF : *Mean Time Between Failure.*
196. MTS : *Message Transfer System*.
197. MTU : *Maximum Transmission Unit.*
198. MVNO : *Mobile Virtual Network Operator.*
199. NAC : *Network Access Control*.
200. NAP : *Network Access Protection.*
201. NAS : *Network Access Server.*
202. NAS : *Network Attached Storage*.
203. NAT : *Network Address Translation.*
204. NAT- PT : *Network Address Translation - Protocol Translator.*
205. NBMA : *Non-Broadcast Multi-Access.*
206. NCIRC : NATO *Computer Incident Response Capability*.
207. NEB : Numérisation de l’espace de bataille.
208. NFC : *Near Field Communication.*
209. NFS : *Network File System.*
210. NIC : *Network Information Center.*
211. NIC : *Network Interface card.*
212. NIDP : *Network Intrusion Detection and Prevention.*
213. NIDS : *Network Intrusion Detection System.*
214. NIS : *Network Information Services*.
215. NIST : *National Institute of Standards and Technology*.
216. NMS : *Network Management System.*
217. NNI : *Network to Network Interface*
218. NNTP : *Network News transfert Protocol*
219. NRA : Nœud de Raccordement d’Abonné.
220. NRO : Nœud de Raccordement Optique .
221. NSA : *National Security Agency*.
222. NSAP : *Network Service Access Point*.
223. NSS : *Network Sub System*.
224. NSS : *Network Security Services.*
225. NTI : Nœud de Transit International.
226. NTIC - Nouvelles Technologies de l’Information et de la Communication.
227. OBL : Opérateur de Boucle Locale.
228. OFDM : *Orthogonal Frequency Division Multiplexing*.
229. OIV : Opérateur d’importance vitale.
230. OLSR : *Optimized Link State Routing Protocol.*
231. OMG : *Object Management Group.*
232. OODA : Observer, Orienter, Décider, Agir (*Observe, Oriente, Decide, Act)*.
233. OS : *Operating System*.
234. OSI (modèle) : *Open System Interconnexion.*
235. OSI : *Open Source Initiative.*
236. OSPF : *Open Shortest Path First.*
237. OSS : *Operating System and Service*.
238. OTAN : Organisation du traité de l’atlantique nord.
239. OTP : *One Time Pad.*
240. PABX : *Private Automatic Branch Exchange.*
241. PAN : *Personal Area Network*
242. PAP : *Password Authentication Protocol.*
243. PBX : *Private Branch Exchange*.
244. PCA : Plan de continuité d’activité.
245. P-CSCF : *Proxy Call Session Control Fonction*
246. PDN : *Public Data Network.*
247. PGP : *Pretty Good Privacy****.***
248. PIN : *Personnal Identification Number.*
249. PKI : *Public Key Infrastructure*.
250. PKCS : *Public Key Cryptography Standard.*
251. PLMN : *Public Land Mobile Network.*
252. PMR : *Professional Mobile Radio.*
253. PNNI : *Private Network Network Interface*.
254. PoP : *Point of Presence.*
255. POP3 : *Post Office Protocol* 3.
256. POTS : *Plain Old Telephone Service.*
257. PPP : *Point to Point Protocol.*
258. PPTP : *Point-to-Point Tunneling Protocol.*
259. PRA : Plan de Reprise d’Activité.
260. PRI : *Primary Rate Interface*.
261. PSTN : *Public Switched Telephone Network.*
262. PUK : *PIN Unblocking Key.*
263. QOS : *Quality Of Service.*
264. RAM : *Random Access Memory*
265. RARP : *Reverse Address Resolution Protocol.*
266. RAT : *Remote Acces Trojan*.
267. RAT : *Remote Administration Tool.*
268. RBL : *Realtime Blackhole List.*
269. RFC : *Request For Comment.*
270. RFID : *Radio Frequency Identification.*
271. RIC : Renseignement d’intérêt Cyber.
272. RIP : *Routing Information Protocol.*
273. RIR : Registre Internet Régionaux, *Regional Internet Registry.*
274. RLC : *Radio Link Control.*
275. RNIS : Réseau Numérique à Intégration de Services.
276. ROC : Renseignement d’Origine Cyber.
277. ROM : *Read Only Memory.*
278. RPC : *Remote Procedure Call.*
279. RSA : Rivest, Shamir, Adelman.
280. RSSI : Responsable de la Sécurité des Systèmes d’Information.
281. RSVP : *Resource Reservation Protocol*.
282. RTC : Réseau Téléphonique Commuté.
283. RTCP : *Real-time Transport Control Protocol*.
284. RTP : *Real-time Transport Protocol.*
285. RTSP : *Real Time Streaming Protocol.*
286. S/MIME : *Secure / Multipurpose Internet Mail Extensions*.
287. SAP : *Service Advertising Protocol*.
288. SCADA : *Supervisory Control And Data Acquisition*.
289. SDLC : *Synchronous Data Link Control*.
290. SDMX : *Statistical Data and MetaData eXchange.*
291. SDU : *Service Data Unit*.
292. SGML : *Standard Generalized Markup Language*.
293. SHA : *Secure Hash Algorithm.*
294. SHTTP : *Secure Hypertext Transfer Protocol.*
295. SIEM : Security Information and Event Management System.
296. SIM : Subscriber Identity Mobile.
297. SIP : *Session Initiation Protocol.*
298. SMB : *Server Message Block.*
299. SMF : *Single Mode Fiber*.
300. SMS : *Short Message Service*.
301. SMTP : *Simple Mail Transfer Protocol*.
302. SNMP : *Simple Network Management Protocol.*
303. SOA : *Service Oriented Architecture.*
304. SOAP : *Simple Object Access Protocol.*
305. SOC : *Security Operations Center.*
306. SPX : *Sequenced Packet eXchange.*
307. SQL : *Structured Query Lanquage*.
308. SS7 : *Signaling System 7.*
309. SSH : *Secure Shell*.
310. SSID : *Service Set IDentifier.*
311. SSII : Société de Service et d’Ingénierie Informatique.
312. SSL : *Secure Socket Layer.*
313. SSL/TLS : Secure Socket Layer/Transport Layer Security.
314. SSO : *Single Sign-On.*
315. STAD : Système de traitement automatisé de données.
316. STIX : *Structured Threat Information eXpression.*
317. TA : *Time Advance.*
318. TAXII : *Trusted Automated of Indicator Information.*
319. TCP : *Transmission Control Protocol.*
320. TD/CDMA : *Time Division* / CDMA.
321. TDM : *Time Division Multiplexing.*
322. TDMA : *Time Division Multiple Access.*
323. TKIP : *Temporal Key Integrity Protocol*.
324. TLD : *Top Level Domain.*
325. TOR : *The Onion Router.*
326. TRAU : *Transcoding Rate and Adaptation Unit.*
327. TTL : *Time-To-Live.*
328. UAC : *Unified Access Control.*
329. UCS: *Universal Character Set.*
330. UDP : *User Datagram Protocol.*
331. UIT : Union Internationale des Télécommunications.
332. UMTS : *Universal Mobile Telecommunication System.*
333. UMTS -TDD : *Universal Mobile Telecommunication System Time Division Duplex*.
334. UNI : *User to Network Interface*.
335. URI : *Uniform Resource Identifier.*
336. URL : *Uniform Resource Locator.*
337. URN : *Uniform Ressource Name.*
338. USB : *Universal Serial Bus.*
339. USENET : UNIX *user network*.
340. UTF: *Unicode Transformation Format.*
341. VBR : *Variable bit rate.*
342. VLAN : *Virtual Local Area Network.*
343. VLR : *Visitor Location Register*.
344. VLSM - *Variable-Length Subnet Mask.*
345. VOD : *Video On Demand.*
346. VPN : *Virtual Private Network.*
347. VPS : *Virtual Private Server.*
348. VSAT : *Very Small Aperture Terminal.*
349. W3C : *World Wide Web Consortium.*
350. WAN : *Wide Area Network*.
351. WAP : *Wireless Application Protocol.*
352. WCDMA : *Wideband Code Division Multiple Access.*
353. WEP : *Wired Equivalent Privacy.*
354. WLAN : *Wireless Local Area Network*.
355. WPA : *Wi-Fi Protected Access.*
356. WPAN : *Wireless Personnal Area Network.*
357. WWW : *World Wide Web.*
358. XKMS : *XML key management system.*
359. XLL : *eXtensible Link Language.*
360. XML : *eXtensible Markup Language*.

A

**Accès** · 11

***Acces Control List*** · 13, 389

**Accès de base** · 11

**Accès direct** · 12

**Accès multiple** · 12, 24

**Accès Multiple par Répartition en Code** · 23

**Accès Multiple par Répartition en Fréquence** · 24

**Accès multiple par répartition temporelle** · 24

**accès primaire** · 11, 12

**Accès séquentiel** · 12

*Access* · 11

*Access Control* · 18, 69, 90, 390

*Access network* · 305

*Access Point* · 278

*Access provider* · 156

Accord cadre sur les technologies de l’information · 204

**Acheminement** · 13

*ACK* · 13, 346

*Acknoledgement* · 13

**ACL** · 13

**Acquittement** · 13

ACSE · 68

**ACSSI** · 34, 35

**Action d’exploitation informatique** · 14, 86

**Action d’influence** · 14

**Action d’information** · 14

**Action de lutte informatique défensive** · 13

**Action de lutte informatique offensive** · 13

*Ad hoc network* · 305

Additif · 15

***Add-on*** · 14

*Address* · 16

***Address Resolution Protocol*** · 32

*Address spoofing* · 366

**Administration de réseau** · 15

*ADP* · 355

**Adressage** · 15, 16, 264

Adressage absolu · 15

Adressage hiérarchique · 15

Adressage logique · 15

Adressage physique · 16

**Adresse** · 16, 18

**Adresse IP** · 16

**Adresse MAC** · 18

Adresse réticulaire · 365

adresse universelle · 18, 365

**Adresse URL** · 18

**ADSL** · 19

***Advanced Encryption Standard*** · 19, 389

***Advanced Evasion Techniques*** · 19

***Advanced Forensic Format*** · 19

***Advanced Persistant Threat*** · 29, 389

***Advanced Research Projects Agency Network*** · 33

**AES** · 19

**AET** · 19

**AFF** · 19

**Affaiblissement du signal** · 19

**AFNIC** · 20, 252, 389

**AFNOR** · 20

AFP · 248

AfriNIC · 301

**Agence Nationale de la Sécurité des Systèmes d’Information** · 28, 292, 389

**Agence Nationale des Fréquences** · 25

**Agent** · 20, 242

agent intelligent · 21

agent logiciel · 21

AH · 200

***Air gap*** · 21

***air wall*** · 21

**Algorithme** · 21

algorithme de Bellman-Ford · 23

**Algorithme de Dijkstra** · 22

**Algorithme de Karn** · 22

**Algorithme de routage** · 22, 261

**Algorithme de routage à état de liaisons** · 22

**Algorithme de routage par vecteur de distance** · 22

**Alice** · 21, 58, 78, 79, 120, 121

**Allocation de ressources** · 23

Allocation mobile · 227

Alternat · 171

***American Standard Code for Information Interchange*** · 35, 389

**Amorce** · 23

**AMRC** · 23

**AMRF** · 24

**AMRT** · 24

*Analog(e) signal* · 324

*Analogic* · 24

**Analogique** · 24

Analyse intelligente des données · 110

*Anchor* · 25

**Ancre** · 25, 179

ancre de lien · 25

**Android** · 25, 164, 222

**ANFR** · 25

Anneau à jeton · 352

**Anonymat** · 25

**Anonymisation** · 26

*Anonymity* · 25

**Anonymous** · 27

**ANSSI** · 28

**Antivirus** · 28

**API** · 28

APNIC · 301

**Appairage** · 29, 272

*Apple Filing Protocol* · 248

**Application** · 29

*Application Common Service Elements* · 68

***Application Programming Interface*** · 28

Apprentissage automatique · 228

**APT** · 29, 389

Arbre recouvrant · 331

Architecture Orientée Service · 330

**archivage** · 31

**Archive** · 31

ARIN · 301

**Arobase** · 34

**ARP** · 32, 230, 244

**ARP *poisoning*** · 32

**ARP *spoofing*** · 32

**ARPANET** · 33, 34, 109, 110

**Article Contrôlés de la Sécurité des Systèmes d’Information** · 34

**AS** · 43, 51, 52, 136, 181, 211, 301

**ASCII** · 35, 264, 389

*Assembler* · 35

**Assembleur** · 35

**Association Française de NORmalisation** · 20, 389

**Association Française pour le Nommage Internet en Coopération** · 20, 389

*Asymetric* · 36

**Asymétrie** · 36

*Asymmetrical Digital Subscriber Line* · 19, 389

*Asynchronous Transfer Mode* · 237

*Asynchronus Transmission Mode* · 237

*ATM* · 148, 237, 241, 264, 278

*at-sign* · 34

*Attachment* · 274

*Attack* · 37, 67, 85, 100, 325, 390

*Attack signature* · 325

**Attaque** · 37

**Attaque par canal auxiliaire** · 38

**attaque par force brute** · 61, 358

**Attaque par point d’eau** · 39

Attaque par réflexion · 329

**Attribution** · 39

**Audience** · 40

**Audit** · 40, 41, 95, 272

**Auditabilité** · 41

*Authentication Header* · 200

**Authenticité** · 41

*Authenticity* · 41

**Authentification** · 42

Authentification unique · 335

**Autoclave** · 42

Autocommutateur · 199

Autocommutateur privé · 199

Autocommutateur téléphonique privé · 269

*Automatic data processing* · 355

**Autonomous System** · 43

**Autorité d’homologation** · 44

**Autorité de certification** · 43

*Availability* · 122

**Avatar** · 44

**AXFR** · 44, 357

**Ayant droit** · 44

B

Bac à sable · 316

*Back up* · 316

***Backbone* *Internet*** · 47

***Backdoor*** · 47

*Backward Error Correction* · 309

***Backward explicit congestion notification*** · 51

Baie · 295

**Balayage de ports** · 48, 317

**Balisage** · 48

**Balise** · 48

**Balise (voie)** · 48

**BAN** · 58, 389

bande C · 374

**Bande de fréquence banalisée** · 49

bande Ka · 374

bande Ku · 374

**Bande passante** · 49

*bandwidth* · 49, 215

**Banque de données** · 50

**Barrière** · 50

**Base de données** · 50, 234

***Base Station Subsystem*** · 61

***Bash*** · 51

***Basic Input Output System*** · 55

*Basic Rate Interface* · 11

*beacon* · 49

*Beacon Channel* · 48

*Beaconing* · 48

BEC · 309

**BECN** · 51, 149

*best effort* · 293

**BGP** · 43, 51, 52, 53, 185, 264, 286, 390

**BI** · 62

**Bibande** · 53

Bibliothèque de l’infrastructure des technologies de l’information · 204

Bibliothèque de liens dynamiques · 123

Bidirectionnel non simultané · 171

Bidirectionnel simultané · 159

**Bien informationnel** · 53

***Big Brother*** · 53

**Big data** · 54, 125

*billing* · 186

**Bimode** · 54

**Binaire** · 55

*Binary* · 55

**BIOS** · 55, 232, 310

**Bitcoin** · 55

*Black list* · 219

*blackhat* · 72, 73

***blog*** · 27, 56, 82

*blogger* · 57

*blogosphere* · 57

**Blogosphère** · 57

**Blogue** · 56

**Blogueur** · 57

**Bluetooth** · 57

**Bob** · 57

***Body Area Network*** · 58, 389

**Bogue** · 58

**Bombardement de courriels** · 58

**Bombe logique** · 59

bombe programmée · 59

*Bookmark* · 326

*Boot* · 23, 231, 394

***Border Gateway Protocol*** · 51

Borne WiFi publique · 176

**Botnet** · 59, 306

**Boucle locale** · 59

***Bourne Again Shell*** · 51

*Breach* · 147

**Bribe** · 60

*Bridge* · 280

*Broadband* · 215

***Broadcast*** · 60, 249, 311, 394

**Brouillage** · 61

*Browser* · 26, 249

**Brute force** · 61

*brute-force attack* · 61

**BSS** · 61, 62, 193, 266, 309

**BTS** · 62, 70, 335

*Buffer overflow* · 116

**Bug** · 58

**Bus** · 62, 366

Bus série universel · 366

***Business Intelligence*** · 62

***Buzz*** · 63

*Byte* · 260

C

*CA* · 43, 276, 390

**Câblage** · 65

**Cache** · 65

*cache ARP* · 32

Cadre d’application · 157

cadriciel · 157

**CALID** · 66

**Canal caché** · 66

**Canal de fréquence** · 66

**Canal de transmission** · 66, 372

**CAPEC** · 67, 228, 336

capture d’écran · 284, 329

***Capture The Flag*** · 67

**Caractérisation** · 67

*Carrier* · 282, 378

*Carrier Sense Multiple Acces with Collision Detection* · 141, 390

**Carte électronique** · 67, 68

**Carte fille** · 67

**Carte mère** · 68

**Carte réseau** · 68, 252

***Cascading Style Sheets*** · 98, 390

**CASE** · 68

*CB* · 49

**CBAC** · 69, 390

**CBC** · 69, 390

**CBR** · 69, 369, 390

**CC** · 94, 95

**CCC** · 73, 390

CCITT · 318, 383

CCMP · 380

*CDMA* · 12, 24, 149, 188, 201, 390

**CDN** · 69, 390

**CEI** · 50, 69, 185

*Cell* · 70

**Cellule** · 70

CEN · 20, 142, 254

*Central Processing Unit* · 285

**Centre d’Analyse et de Lutte Informatique Défensive** · 66

Centre d’Evaluation de la Sécurité des Technologies de l’Information · 72

Centre de commutation mobile · 163

**Centre de commutation radio mobile** · 70, 242

Centre de traitement de données · 110

**CERT** · 70, 390

**Certificat** · 71

*Certificate* · 71

*Certification Authority* · 43

**Certification de sécurité** · 71

**Certification de sécurité de premier niveau** · 72

CESTI · 72

*channel* · 38, 48, 66, 123, 372

**Chaos Computer Club** · 73

**Chapeau blanc** · 72

**chapeau noir** · 72

*Characterization* · 67, 336

*Charge* · 186, 271

Charge active · 271

Charge utile · 271

*Chat* · 77

*chat room* · 77

**Cheval de Troie** · 73

**Chien de garde** · 74

**Chiffrement** · 74

Chiffrement parenchaînement des blocs · 69

*chip* · 60, 288

***Chroot Jail*** · 76

**Cible** · 76

CIDR · 372

CIFS · 248

***Cipher Block Chaining*** · 69

**Circuit** · 77, 83, 217

*Circuit switched connection* · 217

*Circuit switching* · 83

**Circuit virtuel** · 77

**Circuit virtuel commuté** · 77

*Citizen’s band* · 49

*Class of Service* · 293

*Classified Information* · 190

*Classless Inter-Domain Routing* · 372

**Clavardage** · 77

clavardoir · 77

**Clé de chiffrement** · 78

clé privée · 43, 71, 79

clé publique · 71, 79

*Clé symétrique* · 78

**Clé USB** · 79

*Clés asymétriques* · 79

Cliché · 129

**Client** · 80

**Clonage de serveur DNS** · 80

***Cloud computing*** · 80

**CMS** · 81

**CNA** · 85, 86, 390

**CND** · 85, 86

**CNE** · 85, 86, 390

**CNIL** · 81, 390

**CNO** · 85, 390

**Code** · 81

Code de zone de localisation · 214

*Code Division Multiple Access* · 12, 24, 390

**Code malveillant** · 82

*Code point* · 279

code source · 40, 82, 84, 165, 249, 261, 307, 317

cœur de réseau · 226, 306

COFRAC · 72, 292

COMINT · 303

Comité consultatif international téléphonique et télégraphique · 383

Comité Européen de Normalisation · 142, 254

Comité Français d’Accréditation · 72, 292

*Comment* · 82, 396

**Commentaire** · 82

**Commission Electrotechnique Internationale** · 50, 69

**Commission Nationale Informatique et Liberté** · 81, 390

***Common Application Services Elements*** · 68

***Common Attack Pattern Enumeration and Classification*** · 67

*Common criteria* · 95

*Common Internet File System* · 248

***Common Platform Enumeration*** · 93

***Common Technical Regulation*** · 98

***Common Vulnerability Enumeration*** · 98

***Common Vulnerability Scoring System*** · 99

***Common Weakness Enumeration*** · 99

**Communauté** · 82

Communication dans un champ proche · 251

*COMmunication INTelligence* · 303

**Communications électroniques** · 84

*Community* · 82

*Community manager* · 162

Commutation d’étiquette · 344

**Commutation de circuits** · 83

**Commutation de paquets** · 83

Commutation de paquets rapide · 148

*Compile* · 84

**Compiler** · 36, 84

**Compromission** · 84

***Computer Emergency Response Team*** · 70

***Computer Network Attack*** · 85

***Computer Network Defense*** · 86

***Computer Network Exploitation*** · 85, 86

***Computer Network Operations*** · 85

***Computer Security Incident Response Team*** · 71, 98

**Concentrateur** · 86

**Confiance** · 86

**Confidentialité** · 87

*Confidentiality* · 87

*Conflict* · 88

**Conflit** · 88

**Connecteur** · 89

*Connection Less Network Service* · 238

*Connection oriented communication* · 237

**Connexion** · 89, 264

***Constant Bit Rate*** · 69, 369, 390

**Constat d’audit** · 89, 95

***Content*** · 69, 81, 89, 97, 390

*content curation* · 98

***Content Delivery Network*** · 69, 390

***Content Management System*** · 81

**Contenu** · 89, 273

**Contournement de la politique de sécurité** · 89

**Contrôle d’accès** · 90, 227

Contrôle d’accès au support · 227

Contrôle d’Accès Unifié · 361

Contrôle de la liaison logique · 220

Contrôle en profondeur des paquets · 127

**Contrôle parental** · 90

**Convention d’audit** · 90

**Convergence** · 90

**Cookie** · 91, 349

*Core network* · 306

**Corruption** · 91

CoS · 293

**Couche physique** · 91

couche réseau · 305

*Counter mode, CBC Mac Protocol* · 380

**Coupe-feu** · 93

**Courant Porteur en Ligne** · 94

**Courrier électronique** · 93

*Covert channel* · 66

**CPE** · 93

**CPL** · 94

*CPU* · 285

***Creative Commons*** · 94

**Créneau temporel** · 94

**Critère d’audit** · 95

**Critères communs** · 95

*Critical infrastructure* · 260

***Cross Site Scripting*** · 95

***Crowdfunding*** · 9, 96

***Crowdsourcing*** · 96

**Cryptanalyse** · 97

*Cryptanalysis* · 97

**Cryptographie** · 97

*Cryptography* · 97, 276, 395

*Cryptolocker* · 297

**Cryptologie** · 98

*Cryptology* · 98

**CSIRT** · 71, 98

CSMA/CD · 141, 390

**CSPN** · 72

**CSS** · 98, 249, 390

**CTF** · 67

**CTR** · 98

**Curation** · 98

**CVE** · 98, 390

**CVSS** · 99, 375

**CWE** · 99

**Cyber** · 99, 100, 101

*Cyber intelligence* · 302, 303

*Cyber résilience* · 107

**Cyberattaque** · 100

**Cybercommand** · 101

**Cybercriminalité** · 102

*Cybercriminality* · 102

*Cyberdefence* · 102

**Cyberdéfense** · 102

**Cyberdéfense militaire** · 102

*Cyberdetterence* · 103

**Cyberdissuasion** · 103

**Cyberespace** · 104

**Cyberguerre** · 106

**Cyberharcèlement** · 106

**Cyberprotection** · 107

**Cyberrésilience** · 107

**Cybersécurité** · 107

*Cybersecurity* · 107

*Cyberspace* · 85, 104

*Cyberspace* *Opérations* · 85

**Cybersquat** · 108

*Cybersquatting* · 108

*Cyberstalking* · 106

*Cyberwar* · 106

*CYBINT* · 303

D

DAP · 216

*Dark Fiber* · 150

**Darknet** · 109

**DARPA** · 110, 390

*Data* · 110, 117, 123, 125, 141, 142, 173, 217, 272, 316, 318, 391, 395, 396

*Data bank* · 50

*Data base* · 50

***Data center*** · 110

*Data circuit terminating equipment* · 157

*Data Communication Equipement* · 141, 142

*data curation* · 98

*Data Encryptions Standard* · 117

*Data Link* · 217

***Data mining*** · 110

***Data scientist*** · 111

*Data Terminal Equipement* · 142

*Data terminal equipment* · 157

*Data warehouse* · 139

*Datagram* · 111, 296, 347, 362, 397

**Datagramme** · 111

*Daughter board* · 67

*Daughtercard* · 67

Davies, Donald · 33

*DCE* · 141, 142, 157

**DDOS** · 38, 126

**Débit** · 112

Débit variable · 369

**Déception** · 112

**Déchiffrement** · 113

*Decipher* · 113

Décrypter · 113

*Decryption* · 113

**DECT** · 113

**défaçage** · 114

**Défacement** · 114

*Defacing* · 114

**Défaut** · 114

**DEFCON** · 114, 391

**Défense en profondeur** · 115

*defense in depth* · 115

**défiguration** · 114

**Dématerialisation** · 115

***Demilitarized zone*** · 123

**démodulateur** · 238

**Démultiplexage** · 116

*Demultiplexing* · 116

**Déni de service** · 115

*Denial of service* · 38, 115, 126

**Dépassement ou débordement de mémoire** · 116

**DES** · 117

Désinformation · 117

**Détection** · 118, 184

**Détection d’erreur** · 118

*Detection rules* · 300

**Détournement de DNS** · 118

**Détournement de domaine** · 118

**DHCP** · 119

*Dialler* · 224

*Die* · 288

*differenciated service* · 293

**Diffie-Hellman** · 120

**Diffusion de Rayleigh** · 121

Diffusion générale · 60

Diffusion groupée · 243

*Digital* · 19, 201, 256, 284, 389, 391, 392

***Digital Enhanced Cordless Telecommunication*** · 113, 391

*Digital proof* · 284

***Digital Right Management*** · 128

*Digital Rights Management* · 162

*Digital signal* · 324

***Digital Signature Standard*** · 128

***Digital Subscriber Line*** · 128, 255, 384

***Digital Subscriber Line Multiplexer*** · 128

*Digitizing* · 257

*Direct access* · 12

*Directiry Acces Protocol* · 216

*Directory* · 215, 216, 304, 393

**Dispersion** · 122

**Disponibilité** · 122

**Disque dur** · 122

distorsion · 294

**Distribué** · 122

*Distributed* · 38, 122

*Distributed denial of service* · 38

**DLCI** · 123

**DLL** · 123, 391

**DMZ** · 123

**DNS** · 18, 123, 391

*DNS Pharming* · 80, 119

*DNS Tunneling* · 118

DNSSEC · 124

*Domain name* · 253

***Domain Name System*** · 123, 281, 391

**Domaine** · 124

Domaine de premier niveau · 352

**Domotique** · 124

donnée à caractère personnel · 126

**Données** · 125

Données de masse · 54

**Données massives** · 125

**Données ouvertes** · 125

**Données personnelles** · 125

**Données sensibles** · 126

**Dorsale** · 47, 126

Dorsale Internet · 47

**DOS** · 38, 115, 126

***Downlink*** · 127, 177, 217

*Download* · 177, 348

*Downloader* · 223

***Doxing*** · 127

**DPI** · 127, 391

**Drapeau** · 128

*Driver* · 274

**DRM** · 128, 162

*Dropper* · 223

**DSL** · 128

**DSLAM** · 128, 254

**DSS** · 128

*DTE* · 142, 157

*Dual band* · 53

*Dual mode* · 54

***Dump*** · 129

***Duplex*** · 129, 159, 171

Durée de vie · 112, 359

***Dynamic Host Configuration Protocol*** · 119

E

EAL · 95

**EAP** · 133

eBGP · 52

**EBIOS** · 134, 135, 259, 391

**Échantillonnage** · 135, 257

**EFF** · 135

**EGP** · 135

**EI** · 14

**EIGRP** · 136

**EIR** · 136, 137, 168, 391

*Electromagnetic Spectrum* · 331

*Electronic board* · 67

*Electronic communications* · 84

***Electronic Fontier Foundation*** · 135

*ELectronic INTelligence* · 303

*Electronic signature* · 326

**Elévation de privilège** · 137

ELINT · 303

E-mail · 93

**Embrouillage** · 137

Émetteur – récepteur · 356

Empoisonnement de cache ARP · 32

Empreinte · 173

**Emulation** · 137

**En ligne** · 138

*Encapsulating Security Payload* · 200

*Encryption* · 19, 74, 389

*Encryption key* · 78

***Enhanced Interior Gateway Routing Protocol*** · 136

**ENISA** · 138, 391

**Enregistreur de frappe** · 138, 212

**Entrepôt de données** · 139

**Entreprise de Service du Numérique** · 140

*Envoi individuel* · 364

*EPC* · 226

**Equipement de Terminaison de Circuits de Données** · 141

***Equipement Identity Register*** · 136

**Equipement Terminal de Traitement de Données** · 142

**E-réputation** · 139

**Erlang** · 139

*Error Rate* · 344

**ESN** · 140, 189, 334

ESP · 200

ESSID · 49, 140

Etalement de spectre · 150, 333

*Etalement de spectre par saut de fréquence* · 150

**Etat de l’art** · 140

**ETCD** · 141, 142

**Ethernet** · 140, 148, 264

Ethernet commuté · 141

**Ethical hacking** · 141

**Étiquette du Net** · 141

**ETSI** · 142, 187, 188

**ETTD** · 142

***European Network for Information Security Agency*** · 138, 391

***European Telecommunications Standard Institute*** · 142

eUTRAN · 226

*Evaluation Assurance Level* · 95

**Evaluation des besoins et identification des objectifs de sécurité** · 134

**Evanouissement** · 143

**Evénement lié à la sécurité de l’information** · 143

*Evolved Packet Core* · 226

***Excess Information Rate*** · 137

***eXclusive OR*** · 385

*Executable file* · 151

**Exfiltration** · 143

**Exploit** · 144

Exploitation · 85, 144, 390

Exploration des données · 110

**Exposé** · 144

***Extended Service Set Identifier*** · 140

***Extensible Authentication Protocol*** · 133

***eXtensible Link Language*** · 384, 398

***eXtensible Markup Language*** · 384, 398

*eXtensive Messaging and Presence Protocol* · 207

*exterior* BGP · 52

***Exterior Gateway Protocol*** · 135

**Externalisation** · 144

Extranet · 145

F

facturation · 175, 186, 266, 272

*Fading* · 143

**FAI** · 147

**Faille** · 147

**Faisceau Hertzien** · 148, 149

**Fanion** · 148

*Fast Basic Service Transition* · 205

***Fast Ethernet*** · 148

**Fast Packet Switching** · 148

*Fault tolerance* · 353

**FDM** · 148

*FDMA* · 12, 24, 148, 391

**FEC** · 149, 214, 241

FECN · 51, 149

**Femtocell** · 149

**Fenêtre contextuelle** · 149

Feuilles de styles en cascade · 98

**FH** · 148, 149

FHSS · 57, 150

*Fiber To The Home* · 255

*Fibre monomode* · 328

**Fibre noire** · 150

**Fibre optique** · 150

**Fichier exécutable** · 151

**FIFO** · 151

***File Transfert Protocol*** · 158

**Filoutage** · 151

*Filter* · 152

**Filtrage** · 152

Financement participatif · 96

*Firewall* · 93, 152, 271

***FireWire*** · 152

***Firmware*** · 152

***First in First out*** · 151

FISINT · 304

*flag* · 128, 148

**Flame** · 152

*Flow* · 112

Flux · 337

**FM** · 154, 391

FNTC · 87

***Follower*** · 154, 339

**Fonction de hachage** · 155, 170

**Fonction de sécurité** · 154

*Fora* · 156

*Foreign Instrumentation Signal INTelligence* · 304

*Forensic* · 155

**Forensique** · 155

**Format** · 156, 209

**Forme** · 156, 365

**Forum** · 156

*Forward Explicit Congestion Notification* · 51, 149

***Forwarding Equivalence Class*** · 149, 214

**Fournisseur d’accès** · 156

**FPS** · 148

FQDN · 253

*frame* · 123, 136, 355

Frame Relay · 156, 220, 301

*frame tagging* · 202

***Framework*** · 29, 157, 271, 322

***Freeware*** · 157, 162

**Fréquence** · 157

**Fréquence d'Echantillonnage** · 157

*Frequency* · 12, 24, 66, 150, 154, 157, 260, 307, 378, 391, 395, 396

*Frequency channel* · 66

*Frequency Division Multiple Access* · 24, 148, 378, 391

***Frequency Division Multiplexing*** · 148, 260, 395

***Frequency Hopping Spread Spectrum*** · 150

***Frequency Modulation*** · 154

**FTP** · 158, 264

FTTH · 255

**Fuite d’information** · 158

***Full-duplex*** · 159

*Fully Qualified Domain Name* · 253

G

*Galiléo* · 166

Gateway · 43, 51, 162, 163, 390, 392

***Gateway Mobile Switching Center*** · 163, 392

***Gaussian Minimum Shift Keying*** · 163, 392

**GDN** · 162

***Generic Routing Encapsulation*** · 166

**Gestion des droits numériques** · 162

**Gestionnaire de communauté** · 162

**GGSN** · 163

GHDB · 165

**Gigabit Ethernet** · 163

**Gigue** · 163, 208

**GIX** · 163

***Global Internet eXchange*** · 163

***Global Packet Radio System*** · 165

***Global Positioning System*** · 165, 341

***Global System for Mobile communications*** · 167

*Glonass* · 166

**GMSC** · 163, 392

**GMSK** · 163, 392

*Going viral* · 273

***Google*** · 110, 163, 164, 165, 299, 357

***Google Dorks*** · 165

*Google Hacking DataBase* · 165

**GPRS** · 163, 165, 392

**GPS** · 165, 340, 341

Gratuiciel · 157, 162

**Gravité** · 166

**GRE** · 166

**GSM** · 62, 142, 163, 165, 167, 168, 392

*guarented service* · 293

H

**Hachage** · 170

**Hack** · 169

**Hacker** · 169, 276

Hacking éthique · 141

**HADOPI** · 45, 170

***Half-Duplex*** · 171

Hameçonnage · 151, 171

**Hameçonnage ciblé** · 171

***Handover*** · 173

*Hard disk* · 122

*hard QoS* · 293

*Hardware* · 231

**Harponnage** · 173

***Hash*** · 173, 321, 396

*Hash code* · 170

*Hash function* · 155

***Hashtag*** · 173

**Haut Débit** · 173

**HD** · 173

**HDLC** · 173, 215, 264, 318, 356

*heartbeat* · 49, 174

*Heuristics* · 174

**Heuristique** · 174

HIDS · 184, 392

***High Level Data Link Control*** · 173

***High Speed Download Packet Access*** · 177

***High Speed Uplink Packet Access*** · 177

*hit* · 11

**HLR** · 167, 174, 256, 392

***Hoax*** · 175

*Home eNodeB* · 149

***Home Location Register*** · 174, 392

*Home NodeB* · 149

*Home page* · 269

*Home Subscriber Server* · 187

Homme au milieu · 229

**Homologation de sécurité** · 175

**Honey Pot** · 175

***Honey words*** · 176

*Hop* · 52, 316

***Hopping Sequence Number*** · 177, 392

Hors ligne · 260

*Host* · 176, 392

*Host based IDS* · 184

*host id* · 17

***Hosts*** · 176

***Hot Spot*** · 176

**Hôte** · 176

**HSDPA** · 177

**HSN** · 177, 392

HSS · 187

**HSUPA** · 149, 177

**HTML** · 178

**HTTP** · 178, 264, 392

HTTPS · 178, 281, 323

*Hub* · 86

***Hyper Text Transmission Protocol*** · 178

*Hypertext* · 178, 392

***HyperText Markup Language*** · 178

***Hypertext Preprocessor*** · 273

**Hypertexte** · 178

**Hypertrame** · 179

I

*I.T. Management* · 189

**IAB** · 181

**IANA** · 181, 182

iBGP · 52

**ICANN** · 16, 17, 181, 182, 183

**ICMP** · 183

**ICP** · 190, 276

I-CSCF · 187

Identifiant de zone de localisation · 214

Identificateur Uniforme de Ressources · 365

**Identification** · 112, 183, 188, 213, 242, 275, 391, 394, 395

Identifieur de voie logique · 123

Identité des objets · 183

***Identity of things*** · 183

**IDoT** · 183

**IDP** · 184, 200, 392

**IDS** · 184, 392

**IEC** · 69, 185

**IEEE** · 57, 141, 152, 163, 185, 335

**IETF** · 120, 181, 185, 307, 335

**IGC** · 191

**IGP** · 43, 185, 287, 392

**IHM** · 185

*IIS* · 340

**IMEI** · 136, 168, 186, 392

*Implement* · 186

**Implémenter** · 186

**Imputation** · 186

**IMS** · 186, 187

**IMSI** · 68, 175, 188, 232, 236, 242, 392

**IMT 2000** · 188, 189

*In depth defense* · 115

**Incident** · 189, 394

***Incremental Zone Transfer*** · 205, 393

*Indicator Of Compromise* · 230

*Industrial Information System* · 340

*Influence Activity* · 14

**Infobésité** · 189

**Infogérance** · 189, 204

infonuagique · 80, 190

*Information Activity* · 14

*Information Assurance* · 255

**Information classifiée** · 190

*Information overload* · 189

*Information system* · 339

***Information Technology Agreement*** · 204, 393

***Information Technology Infrastructure Library*** · 204, 393

**Informatique dans les nuages** · 190

Informatique décisionnelle · 62

Informatique en nuages · 80

**Infrastructure** · 190

Infrastructure à clés publique · 276

**Infrastructure de clés publique** · 190

**Infrastructure de gestion de clés** · 191

*infrastructure network* · 306

**Ingénierie sociale** · 191, 330

Injection de code indirecte · 95

**Injection SQL** · 191

**Inmarsat** · 192

Institut des ingénieurs électriciens et électroniciens · 185

***Institute of Electrical and Electronics Engineers*** · 185, 335

***Integrated Service Digital Network*** · 201

*Integrated Services Digital Network* · 309

**Intégrité** · 192

*Integrity* · 192

*Intellectual property* · 287

**Intelsat** · 192

***Inter Switch Link*** · 202, 393

***Interconnected Networks*** · 194

*Interconnection* · 193

**Interconnexion** · 193

**Interface** · 12, 185, 193, 284, 389

Interface de programmation · 29

**Interface homme machine** · 185

Interface locale de management · 220

Interface réseau à réseau · 252

**Interférence** · 194

Intergiciel · 234

*interior* BGP · 52

***Interior Gateway Protocol*** · 185

***Intermediate Sytem to Intermediate System*** · 201, 393

***International Electrotechnical Commission*** · 69, 185

***INternational MARitime SATellite Organisation*** · 192

***International Mobile station Equipment Identity*** · 186

***International Mobile Subscriber Identity*** · 188, 392

***International Mobile Telecommunications 2000*** · 188

***International Standard Organisation*** · 20, 202, 393

***INTernational TELecommunication SATelitte consortium*** · 192

***International Telecommunication Union*** · 205, 393

**Internet** · 11, 16, 17, 18, 25, 27, 29, 33, 34, 43, 45, 47, 51, 57, 65, 80, 89, 90, 93, 98, 100, 101, 104, 105, 109, 110, 119, 120, 123, 126, 127, 135, 138, 139, 144, 147, 149, 162, 170, 171, 176, 181, 182, 183, 185, 194, 195, 196, 198, 199, 200, 201, 203, 204, 212, 265, 273, 307, 366, 392, 393, 396

***Internet Activities Board*** · 181

***Internet Architecture Board*** · 181

***Internet Assigned Numbers Authority*** · 181, 182

***Internet Control and error Message Protocol*** · 183

***Internet Corporation for Assigned Names and Numbers*** · 16, 182

***Internet Datagram Protocol*** · 184, 200, 392

**Internet des objets** · 195, 196

***Internet Engineering Task Force*** · 181, 185, 335

***Internet eXchange Point*** · 206

*Internet Of Things* · 195, 392

***Internet Packet eXchange*** · 200

**Internet Protocol** · 16, 194, 195, 196, 305, 392

*Internet Protocol v4* · 198

*Internet Protocol v6* · 198

***Internet Protocole Security*** · 199, 392

***Internet Protocol-Private Branch Exchange*** · 199

***Internet Relay Chat*** · 200

***Internet Research Task Force*** · 181, 201, 392

*Internet Service Provider* · 147

***Internet SOCiety*** · 203, 393

*Interrogating CSCF* · 187

**Intranet** · 196

**Intrusion** · 184, 197, 199, 392, 394

***Intrusion Detection System*** · 184, 392, 394

***Intrusion Prevention System*** · 199, 392

**Invitation à émettre** · 197

**Invitation à recevoir** · 197

*IOC* · 230

*IOT* · 195, 392

*IP address* · 16

***IP Multimédia Subsystem*** · 186

**IP V4** · 198

**IP V6** · 198

**IPBX** · 199

**IPS** · 199, 392

**IPSEC** · 71, 199, 200, 392

**IPX** · 136, 200, 283

**IRC** · 27, 173, 200, 225, 281

**IRTF** · 181, 201, 392

**IS-95** · 201

**ISDN** · 201, 242, 309, 392, 394

**IS-IS** · 201, 393

**ISL** · 202, 393

**ISO** · 20, 50, 97, 142, 174, 201, 202, 203, 264, 335, 393

**ISOC** · 203, 204, 393

Isolation physique · 21

*ISP* · 147, 148, 283

**IT Management** · 204

**ITA** · 204, 393

**ITIL** · 204, 393

**Itinérance** · 204

**ITU** · 188, 205, 393

**IXFR** · 205, 393

**IXP** · 163, 206

J

J2EE · 208

J2ME · 208

J2SE · 208

Jabber · 207

*Jamming* · 61

Java · 29, 82, 194, 207

JavaScript · 208

***JavaScript Object Notation*** · 209, 393

Jeton · 208

*Jitter* · 163, 208

***Joint Picture Expert Group*** · 209, 393

**Jonction** · 208

JOOMLA · 81

**Journalisation** · 209

JPEG · 209, 393

**JSON** · 209, 393

*Junction* · 208

K

KDC · 211

Kerberos · 211

***Kernel*** · 211

*Key Distribution Center* · 211

*Keylogger* · 138, 212

*Keystroke Logger* · 138

***Kill Switch*** · 212

*Killer Services* · 212

L

Label · 214, 218, 241

***Label Distribution Protocol*** · 216, 393

***Label Information Base*** · 218, 393

Label Switching Router · 218, 225, 242, 393

**LAC** · 214, 393

*lack of QoS* · 293

LACNIC · 301

**LAI** · 213, 214, 393

LAN · 123, 214, 393

Langage de modélisation unifié · 363

Langage standard de balisage généralisé · 321

**LAP** · 214, 215, 393

LAPB · 215

LAPD · 215, 393

**Large bande** · 215

**Largeur de bande** · 215

*Latency* · 349

**LCP** · 215, 282, 393

**LDAP** · 215, 216, 393

**LDAP Injection** · 216

**LDP** · 216, 393

*leak* · 158

***Least Cost Routing*** · 216

Leurre de mots de passe · 176

Liaison · 216, 264

**Liaison commutée** · 217

**Liaison de données** · 217

**Liaison descendante** · 217

**LIB** · 218, 393

**LID** · 13, 86

**Lien** · 218

Lien descendant · 127

***Lightweight Directory Access Protocol*** · 215, 216, 393

Ligne d’abonné numérique · 128

Ligne d’abonnés numérique · 384

**Ligne de défense** · 218

**Ligne de transmission** · 219

*Ligne of défense* · 218

*Link* · 123, 173, 218, 391

***Link Access Protocol*** · 214, 215

***Link Control Protocol*** · 215, 282, 393

**LIO** · 13

**liste blanche** · 219, 378

Liste de contrôle d’accès · 13

**Liste noire** · 219

**LLC** · 219, 393

**LMI** · 220, 393

Local Area Network · 214

*Local loop* · 59

***Local Management Interface*** · 220, 393

***Location Area*** · 213, 214, 393

***Location Area Code*** · 214, 393

***Location Area Identification*** · 214, 393

**Log** · 220

*log in* · 89

*log on* · 89

*logic bomb* · 59

***Logical Link Control*** · 219, 393

**Logiciel** · 28, 138, 162, 221, 297, 339

logiciel embarqué · 152

**Logiciel espion** · 221

**Logiciel malveillant** · 222, 229

Logiciel médiateur · 234

Logiciel partagé · 322

**Logiciel système** · 221

**Loguer** · 225

**Loi de Moore** · 240

***Long Term Evolution*** · 225, 393

LSR · 216, 218, 225, 242, 393

LTE · 188, 225, 393

LTE-*advanced* · 226

lutte informatique active · 85

Lutte Informatique Défensive · 66, 86, 390

Lutte informatique offensive · 85

M

**MA** · 227, 393

MAC · 18, 136, 220, 227, 264, 393

***Machine Learning*** · 228

macro · 317

macrocommande · 317

**MAEC** · 228, 393

*Mail bombing* · 58

***Mail Harvesting*** · 228

**Maillage** · 228

**MAIO** · 229, 393

**Maitrise d'OuvrAge** · 236, 394

**Maitrise d’œuvre** · 237, 394

maliciel · 222

*Malware* · 82, 222, 228, 229, 336, 393

***Malware Attribute Enumeration and Characterization*** · 228, 393

MAMBO · 81

**MAN** · 229, 394

***Man in the middle*** · 229

***Man Machine Language*** · 236, 394

***Management Information Base*** · 234, 394

***Manager* SNMP** · 230

**Marqueur (d’attaque)** · 230, 241

marqueur d’activité malveillante · 230

marqueur de compromission · 230

Masque de sous-réseau de longueur variable · 372

Masque jetable · 267

***Master Boot Record*** · 231, 394

**Matériel** · 231

MAU · 353

***Maximum Transmission Unit*** · 242, 394

**MBR** · 231, 232, 394

**MCC** · 188, 232, 394

MD5 · 133, 232, 394

***Mean Time Between Failure*** · 242, 394

***Media Access Control*** · 227, 393

*Media Gateway* · 234, 394

***Media Gateway Control Function*** · 234, 394

*Medium Access Control address* · 18

mégadonnées · 54

*Memory stick* · 79

*mesh* · 229

***Mesh Network*** · 232

*Message Digest 5* · 133, 232, 394

***Message Transfer Agent*** · 242, 394

***Message Transfer System*** · 242, 394

**Messagerie multimédia** · 233

**Messagerie texte** · 233

*Métadata* · 233

**Métadonnée** · 233

**Metasploit** · 233, 271, 322, 323

***Metropolitan Area Network*** · 229, 394

**MGCF** · 234, 394

MGW · 234

**MIB** · 234, 394

**MIC** · 234, 394

Micrologiciel · 152

microprocesseurs multi-cœur · 285

*Microsoft Active directory* · 216

***Middleware*** · 234

*Millitary Cyberdefence* · 102

**MIME** · 235, 394

**MIMO** · 235, 394

**Mise à jour** · 235

**MISO** · 235, 394

***MITM*** · 229

**MITRE** · 67, 93, 99, 228, 236, 336

MMF · 151, 236, 394

**MML** · 236, 394

*MMS* · 233, 236, 394

**MNC** · 188, 213, 236, 394

**MOA** · 236, 394

***Mobile Allocation*** · 227, 393

***Mobile Allocation Index Offset*** · 229, 393

***Mobile Country Code*** · 188, 232, 394

***Mobile Network Code*** · 188, 213, 236, 394

***Mobile service Switching Centre*** · 242

***Mobile station ISDN number*** · 242, 394

***Mobile Subscriber Identification Number*** · 188, 242, 394

***Mobile Virtual Network Operator*** · 243, 394

**Mode connecté** · 237

**Mode de transfert asynchrone** · 237

**Mode de transmission asynchrone** · 237

**Mode de transmission synchrone** · 237

mode infrastructure · 48, 62, 379

**Mode non connecté** · 238

**Modèle** · 216, 238, 264

**Modem** · 238

**Modérateur** · 239

*Moderator* · 239

**Modulateur** · 238

Modulation · 163, 234, 239, 391, 394

Modulation à déplacement minimum gaussien · 163

**Modulation à spectre étalé** · 239

Modulation de fréquence · 154

**Modulation par Impulsions Codées** · 234, 394

Module complémentaire · 15

**MOE** · 236, 237, 394

**Moindre privilège** · 240

Moisson de courriels · 228

**Moore** · 240

**MOSPF** · 240, 266, 394

Mot dièse · 173

**Moteur de recherche** · 240

*Mother board* · 68

*mothercard* · 68

**Motif** · 241

**MPLS** · 149, 214, 216, 218, 241, 394

**MSC** · 242

**MSIN** · 188, 242, 394

MSISDN · 175, 242, 394

**MTA** · 242, 394

**MTBF** · 242, 394

**MTS** · 242, 394

**MTU** · 242, 394

*Multi Mode Fiber* · 151

***Multicast*** · 240, 243, 266, 311, 394

***Multicast extension Open Shortest Path First*** · 240, 394

**Multimédia** · 186

*Multimedia Messaging Service* · 233

***Multimode Fiber*** · 236, 394

*Multiple Access* · 12, 24, 148

***Multiple In / Single Out*** · 235, 394

**Multiple Input / Multiple Output** · 235, 394

**Multiplex** · 243

**Multiplexage** · 243

Multiplexage par code large bande · 378

Multiplexage par répartition autonome de fréquence · 260

Multiplexage temporel · 348

Multiplexeur d’accès à la ligne d’abonné numérique · 128

***MultiProtocole Label Switching*** · 241, 394

***Multipurpose Internet Mail Extensions*** · 235, 394

*Multistation Access Unit* · 353

multi-trames · 179

**MVNO** · 243, 394

**Mystification** · 243

N

**NAC** · 245, 394

***Name Service Switch*** · 245

*Namming* · 254

**NAP** · 245, 246, 247, 394

**NAS** · 247, 248, 394

**NAT** · 248, 394

**NAT- PT** · 249, 394

***National Institute of Standards and Technology*** · 128, 252, 395

***National Security Agency*** · 255, 395

**Navigateur** · 249

**NBMA** · 249, 394

NCP · 215, 282

***Near Field Communication*** · 251, 394

**NEB** · 257, 394

*net id* · 17

**Netbios** · 249

**Nétiquette** · 250

***Netware*** · 200, 250

*Network* · 15, 68, 85, 86, 90, 138, 167, 188, 213, 215, 236, 238, 243, 245, 246, 247, 248, 249, 251, 252, 253, 255, 256, 266, 278, 282, 296, 301, 304, 390, 391, 392, 394, 395, 396

**Network Access Control** · 245, 394

***Network Access Protection*** · 245, 246, 394

***Network Access Server*** · 247, 394

***Network Address Translation*** · 248, 249, 394

***Network Address Translation - Protocol Translator*** · 249, 394

***Network Attached Storage*** · 248, 394

***Network Basic Input Output System*** · 249

*Network Control Protocol* · 215, 282

***Network File System*** · 248, 251, 394

***Network Information Center*** · 251, 394

***Network Information Services*** · 252, 395

***Network Interface card*** · 252, 394

*Network Intrusion Detection System* · 184

*Network management* · 15

***Network Management System*** · 252, 395

***Network News Transfert Protocol*** · 253, 395

***Network Security Services*** · 256, 395

***Network* *Service Access Point*** · 255, 395

***Network Sub System*** · 256, 395

***Network Time Protocol*** · 256

***Network to* *Network Interface*** · 252, 395

*Network topology* · 353

*Newsgroup* · 156

**NFC** · 251, 394

**NFS** · 251, 394

**NIC** · 68, 251, 252, 394

NIDS · 184, 394

**NIS** · 252, 395

**NIST** · 252, 395

**NMS** · 252, 395

**NNI** · 252, 395

**NNTP** · 253, 366, 395

Node · 163, 253

**Noeud** · 253

**Nœud de Raccordement d’Abonné** · 254, 395

**Nœud de raccordement d’abonnés** · 253

**Nœud de Raccordement Optique** · 255, 395

**Nœud de Transit International** · 253, 395

**Nom de domaine** · 124, 253

**Nommage** · 254

***Non Broadcast Multiple Access*** · 249

*Non-repudiation* · 254

**Non-répudiation** · 254

**Normalisation** · 254

**Norme** · 201, 254

Noyau · 211

**NRA** · 253, 254, 255, 395

**NRO** · 255, 395

NSA · 27, 101, 255, 395

**NSAP** · 255, 395

***NSS*** · 167, 193, 245, 246, 256, 266, 395

**NTI** · 253, 395

**NTP** · 256

*Numbering Plan* · 277

**Numérique** · 256

**Numérisation** · 257, 394

**Numérisation de l’espace de bataille** · 257, 394

O

**Obfuscation** · 259

***Object Management Group*** · 261, 395

**Objectif de sécurité** · 259

*Objet-oriented programming* · 286

**OBL** · 259, 395

**Octet** · 260

**OFDM** · 260, 395

OFDMA · 189, 378

***Off-line*** · 260

**OIV** · 260, 315, 395

**OLSR** · 261, 395

**OMG** · 261, 395

OMI · 262

*On line* · 138

***One Time Pad*** · 78, 267

*One-way hash function* · 155

*Open data* · 125

***Open source*** · 261

***Open Source Initiative*** · 265, 395

*Open source intelligence* · 303

***Open System Interconnexion*** · 264, 395

**Opérande** · 262

**Opérateur** · 243, 259, 262, 395

**Opérateur d’importance vitale** · 260, 395

**Opérateur de Boucle Locale** · 259, 395

*Operating System* · 266, 339, 395

***Operating System and Service*** · 266, 395

**Opération d’information** · 262

**Opération militaire d’influence** · 262

*Operation Support Sub system* · 266

Opérations Informatiques · 85

*Operator* · 262

*Optical Fiber* · 150

***Optimized Link State Routing Protocol*** · 261, 395

*Optional Nontransitive* · 52

*Optional Transitive* · 52

Ordinateur quantique · 55, 263

Organisation Internationale de normalisation · 202

*Orthogonal Frequency Division Multiple Access* · 378

***Orthogonal Frequency Division Multiplexing*** · 260, 395

**OSI** · 264, 265, 395

OSINT · 303

OSPF · 22, 201, 241, 264, 265, 266, 287, 395

**OSS** · 266, 395

OTAN · 395

**OTP** · 78, 267

*Out of band signaling* · 325

*Outed* · 144

Outil d’administration à distance · 298

Outils de dissimulation d’activité · 310

*Outsourcing* · 144

P

*P2P* · 269

**PABX** · 269, 395

*Packet* · 83, 127, 136, 148, 165, 177, 226, 270, 392

*Packet switching* · 83

**Page d'accueil** · 269

**Pair à pair** · 269

**PAN** · 270, 395

**PAP** · 270, 395

**Paquet** · 270

Pare-feu · 152, 271

*Parental Controls* · 90

Paris · 3

**Parité** · 271

Passerelle · 162, 271

***Password Authentication Protocol*** · 270, 395

**patrimoine informationnel** · 53

*Pattern* · 67, 156, 230, 241, 390

***Payload*** · 271

**PBX** · 269, 272, 395

**PCA** · 277

*PCM* · 234

**P-CSCF** · 187, 272, 395

**PDN** · 272, 395

*Peer to peer* · 269

*peering* · 29, 272

*Pentest* · 350

**Périmètre d’audit** · 272

**Permutation** · 272

***Personal Area Network*** · 270, 395

*Personnal data* · 125

***Personnal Identification Number*** · 275, 395

**PGP** · 273, 395

*Pharming* · 118

**Phénomène viral** · 273

*Phishing* · 151, 171

**PHP** · 273, 317, 373

***Phreaker*** · 273

*Physical layer* · 91, 274

**Physique (couche)** · 274

*Piconet* · 274

**Picoréseau** · 274

**Pièce jointe** · 274

***Piggyback*** · 274

**Pilote de périphérique** · 274

**PIN** · 68, 275, 395

***PIN Unblocking Key*** · 288, 396

**Ping** · 275

Ping de la mort · 275

***Ping of Death*** · 275

*Piracy* · 275

**Piratage** · 275

**Pirate informatique** · 276

**PKCS** · 256, 276, 395

**PKI** · 276, 395

*Plain Old Telephone Service* · 313, 396

**Plan de continuité d’activité** · 277

**Plan de numérotation** · 277

**Plan de reprise d’activité** · 277

**PLMN** · 277, 395

**PMR** · 277, 395

**PNNI** · 278, 396

**Point à point** · 279

**Point d'accès** · 278

point d’ancrage · 25

Point d’échange Internet · 206

**Point de code** · 279

Point de Présence · 280

point de transfert sémaphore · 319

***Point of Presence*** · 280, 396

*Point to point* · 215, 279

***Point to Point Protocol*** · 270, 279, 282, 396

**Pointeur** · 279

points sémaphore · 319

***Point-to-Point Tunneling Protocol*** · 283, 396

**Politique de sécurité de système d’information** · 279

**Politique en matière de protection des renseignements personnels** · 279

*Polling* · 197, 280

*Polymorphic virus* · 371

**Pont** · 280

*Ponter* · 279

**PoP** · 280, 396

**POP3** · 93, 280, 396

*Pop-up* · 149

**Port** · 250, 281

**Portabilité** · 281

Porte dérobée · 47, 282

**Porteuse** · 282

*Ports scanning* · 48

*Post* · 280, 288, 396

***Post Office Protocol* 3** · 280, 396

Pot de miel · 175

POTS · 313, 396

**Pourriel** · 282, 331

*Power Line Communication* · 94

**PPP** · 133, 215, 270, 279, 282, 283, 396

**PPTP** · 283, 396

**PRA** · 277

**Prestataire d’audit** · 95, 283

***Pretty Good Privacy*** · 273, 395

**Preuve numérique** · 284

**Preuves d’audit** · 284

**PRI** · 284, 396

*Primary Rate Interface* · 11, 284, 396

**Principe de sécurité** · 285

*Privacy Policy* · 279

***Private Automatic Branch Exchange*** · 269, 395

***Private Branch Exchange*** · 272, 395

***Private Network Network Interface*** · 278, 396

*Privilege Escalation* · 137

**Procédure** · 285

**Processeur** · 285

*Processor* · 285

Production participative · 96

**Produit de sécurité** · 285

***Professional Mobile Radio*** · 277, 395

**Programmation objet** · 286

**Programmation orientée objet** · 286

propriété industrielle · 287

**Propriété intellectuelle** · 287

propriété littéraire et artistique · 287

Protection d’accès réseau · 246

**Protocole** · 286

Protocole d’accès aux annuaires légers · 215

Protocole d’authentification par mot de passe · 270

Protocole de contrôle de liens · 215

Protocole de distribution de label · 216

Protocole de résolution d’adresse · 32

**Protocole de routage** · 261, 265, 278, 286

Protocole de transfert de fichiers · 158

Protocole Internet Sécurisé · 199

Protocole IP · 196

Protocole Simple de Gestion de Réseau · 329

***Proxy*** · 187, 272, 288, 395

***Proxy Call Session Control Fonction*** · 272, 395

*Proxy server* · 319

***Proxy serveur*** · 288

**PSSI** · 279, 285

**PSTN** · 288, 313, 396

***Public Data Network*** · 272, 395

***Public Key Cryptography Standard*** · 276, 395

***Public Key Infrastructure*** · 276, 395

***Public Land Mobile Network*** · 277, 395

***Public Switched Telephone Network*** · 288, 313, 396

**Publication** · 288

**Puce** · 288

**PUK** · 288, 396

*Pulse Code Modulation* · 234

Q

**Qualification** · 291

**Qualification de produits de sécurité** · 292

**Qualité de service** · 293

*quality of expérience* · 293

*Quality of service* · 293

**Quantification** · 294

*Quantizing* · 294

*Quantum processing* · 263

R

***Rabbit*** · 295

***Rack*** · 295

***Radio Frequency Identification*** · 307, 396

***Radio Link Control*** · 309, 396

Radio-identification · 307

RADIUS · 133, 295

***Rainbow tables*** · 297

**RAM** · 68, 297, 396

**Rançongiciel** · 297

*Random access* · 12

***Random Access Memory*** · 297, 396

*Ransomware* · 297

**Rapport signal / bruit** · 298

**RARP** · 298, 396

**RAT** · 129, 130, 298, 396

*rate* · 112, 384

*Rayleigh scattering* · 121

**RBL** · 298, 396

***Read Only Memory*** · 310, 396

***Real Time Streaming Protocol*** · 314, 396

***Realtime Blackhole List*** · 298, 396

***Real-time Transport Control Protocol*** · 313, 396

***Real-time Transport Protocol*** · 313, 396

*Record* · 31, 167

**Redondance** · 299

*Redundancy* · 271, 299

**Référencement** · 299

**Référentiel** · 40, 41, 89, 90, 95, 140, 143, 154, 183, 272, 284, 300, 318, 326, 351

**Référentiel général de sécurité** · 300

*Regional Internet Registry* · 301, 396

*Register* · 300

*registered ports* · 281

**Registre** · 300, 396

**Registre Internet Régionaux** · 301

**Règle de détection** · 300

Relai de trame · 156

**Relais de trame** · 301

*Remediation* · 302

**Remédiation** · 302

*Remote Access Trojan* · 130, 298

***Remote Administration Tool*** · 298

*Remote Authentication Dial-In User Service* · 133

***Remote Authentification Dial In Users Services*** · 295

*Remote Procedure Call* · 252

**Renifleur** · 302

*Reno* · 345

**Renseignement d’Intérêt Cyber** · 302

**Renseignement d’Origine Cyber** · 303, 396

**Renseignement d’Origine ÉlectroMagnétique** · 303

*Repeater* · 304

**Répertoire** · 304

**Répéteur** · 304

*Repository* · 276, 300

**Reprise (point de)** · 304

**Répudiation** · 304

***Request for comment*** · 307

**Réseau** · 69, 70, 109, 201, 229, 232, 264, 265, 272, 277, 288, 304, 306

**Réseau à valeur ajoutée** · 305

Réseau corporel · 58

**Réseau d’accès** · 305

**Réseau d’infrastructure** · 306

Réseau de distribution de contenus · 69

**Réseau de zombies** · 306

**Réseau étendu** · 306, 377

**Réseau indépendant** · 306

Réseau Local · 214

Réseau local sans fil · 380

Réseau local virtuel · 371

Réseau maillé · 232

Réseau métropolitain · 229

Réseau Mobile Terrestre Public · 277

Réseau Numérique à Intégration de Données · 201

**Réseau Numérique à Intégration de Services** · 309, 396

**Réseau privé virtuel** · 306, 373

Réseau public de transmission de données · 272

Réseau sans fil personnel · 380

**Réseau Téléphonique Commuté** · 313, 396

**Réseaux ad hoc** · 305

Réseaux radio mobiles professionnels · 277

*Residual error-rate* · 345

**Résilience** · 307

***Resource Reservation Protocol*** · 313, 396

**Responsable de la Sécurité des Systèmes d’Information** · 312, 396

**Rétro-ingénierie** · 307

*reverse* · 307

***Reverse Address Resolution Protocol*** · 298

*Reverse engeniring* · 307

**RFC** · 17, 43, 44, 51, 52, 93, 120, 133, 158, 166, 181, 185, 198, 199, 202, 205, 209, 211, 215, 216, 233, 235, 249, 250, 251, 253, 261, 265, 266, 270, 276, 280, 282, 283, 307, 357, 396

**RFID** · 196, 307, 396

**RGS** · 40, 41, 89, 90, 95, 140, 154, 272, 284, 292, 300

RIC · 302, 396

**RIP** · 23, 265, 287, 308, 396

RIPE-NCC · 301

**Riper** · 308

**RIR** · 43, 182, 301, 396

*Risk* · 309

**Risque** · 309

risque résiduel · 309

**Rivest, Shamir, Adelman** · 312, 396

**RJ 45** · 309

**RLC** · 309, 396

RNIS · 12, 167, 174, 201, 309, 396

*Roaming* · 204

ROC · 303, 396

**ROEM** · 255, 303

**ROM** · 68, 152, 297, 310, 396

*root name server* · 320

*Root server* · 320

***Rootkit*** · 310

**Routage** · 43, 166, 185, 216, 311

Routage à moindre coût · 216

Routage Générique par encapsulation · 166

route par défaut · 344

*Router* · 218, 242, 312

routes dynamiques · 311, 344

routes statiques · 311, 344

**Routeur** · 312

*Routing* · 13, 23, 136, 166, 261, 311, 395

***Routing Information Protocol*** · 23, 308, 396

*Routing protocol* · 286

*Routing table* · 343

RPC · 252

RPV · 373

**RSA** · 273, 276, 312, 396

**RSSI** · 312, 396

**RSVP** · 241, 313, 396

**RTC** · 83, 167, 234, 237, 273, 288, 313, 396

**RTCP** · 313, 396

**RTP** · 187, 313, 396

**RTSP** · 314, 396

**RVA** · 305

S

**S/MIME** · 256, 315, 396

**Sabotage** · 315

*Sampling Frequency* · 157

***Sandbox*** · 316

SAP · 251, 396

**Saut** · 316

**Sauvegarde** · 316

**SCADA** · 316, 396

**Scan** · 317

SC-FDMA · 378

*Scrambling* · 137

**Script** · 317

***Scriptkiddies*** · 317

Scrutation · 280

S-CSCF · 187

**SDLC** · 318, 396

**SDMX** · 318, 396

**SDU** · 318, 396

*Search engine* · 240

secteur d’amorçage · 231, 232

***Secure / Multipurpose Internet Mail Extensions*** · 315, 396

***Secure Hash Algorithm*** · 321, 396

***Secure Hypertext Transfer Protocol*** · 323, 397

***Secure Shell*** · 281, 334, 397

***Secure Socket Layer*** · 334, 397

**Sécurité d’un système d’information** · 318

***Security Information and Event Management*** · 323, 397

***Security Operations Center*** · 324, 330, 397

*Security Policy* · 279

*Selecting* · 197

**Sémaphore** · 318

*Sequenced Packet eXchange* · 200, 397

*Sequenced Packet eXchnage* · 251

*Serial access* · 12

*server* · 319

***Server Message Block*** · 248, 328, 397

**Serveur** · 319

Serveur de stockage réseau · 248

Serveur mandataire · 288, 319

Serveur privé virtuel · 373

**Serveur racine** · 320

**Service** · 68, 140, 148, 201, 236, 245, 250, 255, 281, 320, 334, 344, 392, 394, 395, 396, 397

*Service Advertising Protocol* · 251, 396

***Service Data Unit*** · 318, 396

***Service Oriented Architecture*** · 330, 397

***Service Set IDentifier*** · 334, 397

*Service-CSCF* · 187

services cachés · 354

**Session** · 187, 250, 264, 272, 321, 327, 395, 397

***Session Initiation Protocol*** · 327, 397

**SGML** · 321, 396

**SHA** · 232, 321, 396

**Shannon** · 158, 322

**Shannon (Théorème de)** · 322

***Shareware*** · 322

***Shellcode*** · 322

*Short Message Service* · 233, 328, 397

*Shortest Path First* · 22, 265, 266, 395

**SHTTP** · 323, 397

***Shunning*** · 323

**SI** · 115, 339

*Side channel attack* · 38

**SIEM** · 323, 397

*SIGINT* · 303

**Signal** · 48, 324

**Signal analogique** · 324

*Signal intelligence* · 303

**Signal numérique** · 324

*Signaling* · 324

*Signaling System 7* · 318, 334, 397

**Signalisation** · 324

**Signalisation hors bande** · 325

**Signature d'attaque** · 325

**Signature de virus** · 325

**Signature électronique** · 326

**Signet** · 326

SIM · 68, 326, 397

***Simple Mail Transfer Protocol*** · 93, 328, 397

***Simple Network Management Protocol*** · 329, 397

***Simple Object Access Protocol*** · 330, 397

*Single Carrier – Frequency Division Multiple Access* · 378

*Single Mode Fiber* · 151, 328, 397

***Single Sign-On*** · 335, 397

***Sinkholing*** · 327

**SIP** · 187, 327, 397

***Slacktivisme*** · 327

**SMB** · 248, 264, 328, 397

SMF · 151, 328, 397

*smishing* · 171

*SMS* · 171, 233, 328, 397

**SMTP** · 93, 235, 281, 328, 397

**SMURF (attaque)** · 329

***Snapshot*** · 329

*Sniffer* · 302

**SNMP** · 230, 234, 264, 281, 329, 394, 397

**SNORT** · 329

**SOA** · 330, 397

**SOAP** · 330, 397

**SOC** · 324, 330, 397

*Social engineering* · 191, 330

**Société de Service et d’Ingénierie Informatique** · 334, 397

*Society for Worlwide Interbank Financial Telecommunications* · 312

*Socket* · 89, 334, 397

socle d’application · 157

*soft QoS* · 293

*Software* · 221

**Sonde de détection d’attaque** · 331

Sous système d’exploitation et de maintenance · 266

Sous-système des stations de base · 61

**Spam** · 282, 331

***Spanning Tree*** · 331

*Spear Phishing* · 173

*Spearphishing* · 171

**Spectre électromagnétique** · 331

*SPF* · 265

SPIP · 81

*Spoofing* · 243

***Spread Spectrum*** · 333

*Spread Spectrum modulation* · 239

SPX · 200, 251, 264, 397

*Spyware* · 221

**SQL** · 191, 296, 333, 397

**SS7** · 252, 318, 334, 397

**SSH** · 264, 281, 334, 397

**SSID** · 334, 397

**SSII** · 140, 189, 334, 397

**SSL** · 158, 256, 334, 397

SSL *Handshake protocol* · 334

SSL *Record protocol* · 334

**SSO** · 335, 397

**STAD** · 335, 397

***Standard Generalized Markup Language*** · 321, 396

**Standards** · 335

Standards de cryptographie à clé publique · 276

*State of the art* · 140

**Station de base** · 335

***Statistical Data and MetaData eXchange*** · 318, 396

**Stéganographie** · 336

*Steganography* · 336

STIX · 67, 228, 336, 397

***Store and Forward*** · 336

***Streaming*** · 314, 337, 396

***Structured Query Lanquage*** · 333, 397

***Structured Threat Information eXpression*** · 336, 397

**Stuxnet** · 152, 153, 154, 316, 337, 338

*Subscriber Identity Mobile* · 68, 326, 397

**Suiveur** · 154, 338

**Suivre** · 338

supertrames · 179

***Supervisory Control And Data Acquisition*** · 316, 396

*Swap* · 272

SWIFT · 305, 312

*Switched virtual circuit* · 77

**Synchrone** · 339

***Synchronous Data Link Control*** · 318, 396

*System software* · 221

Système autonome · 43

**Système d'exploitation** · 339

Système d’arrêt d’urgence · 212

**Système d’information** · 339

**Système d’information industriel** · 340

**Système d’information sensible** · 340

Système de Détection d'Intrusion · 184

Système de géolocalisation mondial · 165

Système de gestion de contenu · 81

Système de gestion de réseau · 252

Système de gestion des clés XML · 384

Système de noms de domaine · 123

Système de prévention d’intrusion · 199

Système de télécommunication mobile universel · 363

**Système de Traitement Automatisé des Données** · 335

Système global de communication mobile · 167

T

**TA** · 343, 397

Table arc-en-ciel · 297

**Table de routage** · 343

*Tag* · 48, 344

***Tag Switching*** · 344

*Tahoe* · 345

*target* · 76, 393

**Tarpit** · 344

**Taux d'erreurs** · 344

**Taux d'erreurs Résiduelles** · 345

Taux d’échantillonnage fixe · 69

*TAXII* · 336

**TCP** · 22, 27, 34, 51, 93, 112, 158, 178, 181, 195, 264, 265, 345, 397

**TCP/IP (modèle)** · 347

**TD/CDMA** · 348, 397

**TDM** · 348, 397

**TDMA** · 12, 24, 348, 397

Technique d’évasion avancées · 19

**Téléchargement** · 348

**Télécharger** · 348

***TELecommunication NETwork*** · 349

*Telephone over IP* · 349

**Téléphonie sur IP** · 349

**TELNET** · 349

Témoin de connexion · 91, 349

*Template* · 238

***Temporal Key Integrity Protocol*** · 352, 380, 397

**Temps de latence** · 349

**Temps de réponse** · 349

Temps Moyen Entre Panne · 242

**Terminal** · 142, 350

***Terrestrial Trunked Radio Access*** · 351

**Test d’intrusion** · 350

**TETRA** · 278, 351

TGS · 211

***The Onion Router*** · 354, 397

*Ticket Granting Service* · 211

**tiers de confiance** · 86, 87, 352

***Time Advance*** · 343, 397

***Time Division* / CDMA** · 348, 397

***Time Division Multiple Access*** · 12, 24, 348, 397

***Time Division Multiplexing*** · 348, 397

***Time Out*** · 352

*Time slot* · 94

***Time-To-Live*** · 359, 397

**TKIP** · 352, 380, 397

**TLD** · 124, 251, 253, 352, 357, 397

**TLS** · 133, 178, 256, 334, 335, 397

TMEP · 242

toile · 33, 72, 378, 381

**TOIP** · 349

*Token* · 208

***Token Ring*** · 214, 218, 352

**Tolérance aux pannes** · 353

***Top Level Domain*** · 124, 251, 352, 357, 397

**Topologie de réseau** · 353

Topologie en · 353

Topologie en anneau · 353

Topologie en bus · 353

Topologie en étoile · 353

Topologie maillée · 353

**TOR** · 26, 27, 354, 397

**Trace** · 354

Traduction d'adresse réseau · 248

**Trafic** · 69, 355

**Traitement automatique de données** · 355

**Traitement de données à caractère personnel** · 355

**Trame** · 355

***Transceiver*** · 335, 356, 390

**Transcodage** · 356

***Transcoding Rate and Adaptation Unit*** · 358, 397

**Transfert de paquets** · 356

**Transfert de zone** · 44, 205, 356

**Transfert de zone DNS** · 44

Transfert inter-cellulaire · 173

*Transhumanism* · 357

**Transhumanisme** · 357

***Transmission Control Protocol*** · 195, 345, 397

**TRANSPAC** · 357

*Transponder* · 304

**Transport** (couche) · 358

*Transport layer* · 358

**Transport Layer Security** · 335, 397

*transrating* · 356

**TRAU** · 358, 397

**Triple DES** · 358

*Trojan* · 73, 358

**Troll** · 358

*Trust* · 86

*Trusted Automated of Indicator information* · 336

*trusted third party* · 86, 352

**TTL** · 352, 359, 397

*TTP* · 86, 352

**Tunnel** · 359

TYPO3 · 81

***Typosquatting*** · 359

U

**UAC** · 245, 361, 362, 397

**UCS** · 362, 365

**UDP** · 249, 264, 296, 307, 346, 358, 362, 397

UIT · 153, 188, 205, 363, 397

UIT-T · 383

UML · 261, 363

**UMTS** · 142, 168, 177, 188, 225, 235, 363, 397

**UMTS -TDD** · 364, 397

**UNI** · 364, 398

**Unicast** · 311, 364

**Unicode** · 35, 365, 366

***Unicode Transformation Format*** · 366

***Unified Access Control*** · 361, 397

*Unified Modeling Language* · 261, 363

***Uniform Resource Identifier*** · 365, 398

***Uniform Resource Locator*** · 365, 398

*Uniform Ressource Locator* · 18

***Uniform Ressource Name*** · 365, 398

Union Internationale des Télécommunications · 153, 205, 363, 397

Unité de données service · 318

Unité de transcodage et d’adaptation du débit · 358

***Universal Character Set*** · 362, 365

***Universal Mobile Telecommunication System*** · 363, 397

***Universal Mobile Telecommunication System Time Division Duplex*** · 364, 397

***Universal Serial Bus*** · 366, 398

**UNIX user network** · 366, 398

*Upgrade* · 235

*Upload* · 348

**URI** · 365, 398

**URL** · 18, 165, 299, 365, 398

**URN** · 365, 398

**USB** · 79, 101, 152, 281, 316, 366, 398

**USENET** · 366, 398

***User Datagram Protocol*** · 296, 347, 362, 397

*User Generated Content* · 89

***User to Network Interface*** · 364, 398

**Usurpation d’adresse** · 366

Usurpation de cache ARP · 32

**UTF** · 366

V

*Valance* · 369

**Valence** · 369

*Value Added Network* · 305

*VAN* · 305

*variable bit rate* · 69, 369, 398

***Variable-Length Subnet Mask*** · 266, 372, 398

**VBR** · 69, 369, 398

VDS · 373

**Ver informatique** · 370

*Vertical Redundancy Check* · 271

***Very Small Aperture Terminal*** · 373, 398

Vidéo à la demande · 372

***Video On Demand*** · 372, 398

***Vine*** · 370

*Virtual* · 243, 306, 370, 371, 394, 398

*Virtual circuit* · 77

*Virtual Dedicated Server* · 373

***Virtual Local Area Network*** · 371, 398

***Virtual Private Network*** · 306, 373, 398

***Virtual Private Server*** · 373, 398

**Virtuel** · 243, 370

**Virus** · 370

**Virus polymorphe** · 371

*Virus signature* · 325

**Visitor Location Register** · 168, 371, 398

**VLAN** · 202, 214, 371, 398

**VLR** · 167, 175, 213, 256, 371, 398

**VLSM** · 265, 266, 372, 398

**VOD** · 372, 398

**Voie** · 372

*VoIP* · 234, 372

**Voix sur IP** · 372

**VPN** · 200, 241, 373, 398

**VPS** · 373, 398

*VRC* · 271

**VSAT** · 373, 398

**Vulnérabilité** · 374

*Vulnerability* · 98, 99, 374, 375

W

**W3C** · 178, 377, 398

**WAN** · 123, 157, 306, 377, 398

**WAP** · 377, 398

*watchdog* · 74

*water holing* · 39

*Watering hole* · 39

*Wave interférence* · 194

**WCDMA** · 177, 378, 398

**Web** · 72, 81, 114, 118, 192, 208, 249, 269, 292, 293, 319, 330, 377, 378, 381, 398

*webmail* · 93

*Well known discretionary* · 52

*well known mandatory* · 52

*well known ports* · 281

*well known services* · 320

**WEP** · 378, 398

*White list* · 219, 378

*whitehat* · 72

*Wide Area Network* · 306, 377, 398

***Wideband Code Division Multiple Access*** · 177, 378, 398

**Wi-Fi** · 140, 173, 278, 379, 380, 398

***Wi-Fi Protected Access*** · 380, 398

***Wiki*** · 379

*wikileaks* · 158

**WiMAX** · 379, 380

***Wired Equivalent Privacy*** · 378, 398

***Wireless Application Protocol*** · 377, 398

***Wireless Fidelity*** · 379

***Wireless Local Area Network*** · 380, 398

*Wireless Markup Language* · 378

*Wireless Personal Network* · 270

***Wireless Personnal Area Network*** · 380, 398

*Wiring* · 65

**WL** · 378

**WLAN** · 380, 398

WML · 378

*workflow* · 81

***World Wide Web*** · 57, 178, 381, 398

***World Wide Web Consortium*** · 377, 398

***Worldwide Interoperability for Microwave Access*** · 379

*Worm* · 370

**WPA** · 380, 398

WPA2 · 380

WPAN · 270, 380, 398

**WWW** · 381, 398

X

**X** · 51, 163, 215, 218, 253, 255, 256, 312, 332, 334, 357, 383, 384

***x Digital Subscriber Line*** · 384

**X.25** · 253, 358, 383, 384

X.500 · 383

X.501 · 383

X.509 · 383

X.518 · 383

X.519 · 383

X.525 · 383

xDSL · 128, 384

*Xerox Network Specification* · 184

XKISS · 384

**XKMS** · 384, 398

XKRSS · 384

**XLL** · 384, 398

**XML** · 178, 207, 209, 384, 398

XML *Key Information Service Specification* · 384

***XML key management system*** · 384, 398

XML *Key Registration Service Specification* · 384

XMPP · 207

XNS · 184

**XOR** · 385

***XSS*** · 95

Z

**Zéro-day** · 387

**Zombie** · 7, 387

Zone d’amorce · 231

Zone de localisation · 213

Zone démilitarisée · 123

*Zone transfer* · 356

# Remerciements

Ce dictionnaire n’a pu voir le jour qu’avec la contribution active de plusieurs personnes issues de différents horizons et de spécialités multiples. Je tiens ici à particulièrement remercier William Dupuy, pour sa patiente relecture et son regard d’homme de l’art, Pierre D., qui a su allier à l’exac­titude des termes l’ouverture aux moins experts et rendre ainsi certaines définitions un peu moins austères. Les remerciements ne seraient pas complets sans y ajouter ceux avec qui j’ai l’occasion d’échanger régulièrement sur les questions de cyberdéfense ou de sécurité des systèmes d’information dont particulièrement François, Stéphane, Axel, etc.

1. Un glossaire est disponible sur le site internet de L’ANSSI à l’adresse suivante : http://www.ssi.gouv.fr/administration/glossaire/ [↑](#footnote-ref-2)
2. Journal Officiel du 1er septembre 2000. [↑](#footnote-ref-3)
3. Journal Officiel du 22 septembre 2000. [↑](#footnote-ref-4)
4. Journal Officiel du 26 mars 2006. [↑](#footnote-ref-5)
5. Journal Officiel du 22 septembre 2000. [↑](#footnote-ref-6)
6. Glossaire interarmées de terminologie opérationnelle, DC-04\_GIATO(2013) amendé au 1er juin 2015. [↑](#footnote-ref-7)
7. Glossaire interarmées de terminologie opérationnelle, DC-04\_GIATO(2013) amendé au 1er juin 2015. [↑](#footnote-ref-8)
8. Glossaire interarmées de terminologie opérationnelle, DC-04\_GIATO(2013) amendé au 1er juin 2015. [↑](#footnote-ref-9)
9. Concept interarmées d’influence, CIA-3.10-INFLUENCE (2012) [↑](#footnote-ref-10)
10. *Ibidem.* [↑](#footnote-ref-11)
11. Journal Officiel du 16 mars 1999. [↑](#footnote-ref-12)
12. Journal Officiel du 22 septembre 2000. [↑](#footnote-ref-13)
13. Voir site de l’AFNIC : https://www.sandbox.afnic.fr/fr/l-afnic-en-bref/presentation/missions-de-l-afnic-et-axes-strategiques-2012-2015-1.html [↑](#footnote-ref-14)
14. Journal Officiel du 22 septembre 2000. [↑](#footnote-ref-15)
15. ## Voir l’analyse de Bruce Schneier sur son blog : *«* *How the NSA Attacks Tor/Firefox Users With QUANTUM and FOXACID »* post du 7 octobre 2013 disponible à l’adresse :

    ## https://www.schneier.com/blog/archives/2013/10/how\_the\_nsa\_att.html.

    [↑](#footnote-ref-16)
16. Guy Fawkes était un catholique anglais membre d’un groupe lié à la Conspiration des poudres de 1605. Cette conspiration visait à assassiner le roi Jacques Ier et restaurer une monarchie catholique sur le trône d’Angleterre. L’échec de cette conspiration est aujourd’hui fêtée le 5 novembre en Angleterre. [↑](#footnote-ref-17)
17. Voir le site à l’adresse https://anonops.com [↑](#footnote-ref-18)
18. APT1 : *Exposing one of China’s Cyber Espionnage Units,* disponible à l’adresse http://intelreport.mandiant.com/ [↑](#footnote-ref-19)
19. Cedreic Pernet, APT sécurité et espionnage informatique, Ellipse 2014. [↑](#footnote-ref-20)
20. # Voir Scott j Roberts, APT is a Who not a What... And Why it doesn't Matter. <https://sroberts.github.io/2015/02/16/apt-is-a-who-not-a-what/> et également O. Kempf, APT, non pas quoi mais qui. <http://www.egeablog.net/index.php?post/2015/02/19/APT-%3A-non-pas-quoi-mais-qui>

    [↑](#footnote-ref-21)
21. Au mois de juillet 1961, Leonard Kleinrock, étudiant au MIT, publie sa thèse de doctorat « *information flow in large communication nets*» qui pose les bases de la théorie de la commutation de paquets sur laquelle se fonde l’Internet. Il est, à ce titre, considéré comme l’un des pères fondateurs d’Internet.

    Voir <http://www.historyofthings.com/history-of-the-internet>. Consulté le 5 avril 2014. [↑](#footnote-ref-22)
22. Instruction interministérielle n° 910/SGDSN/ANSSI du 22 octobre 2013 relative aux articles contrôlés de la sécurité des systèmes d’information (ACSSI). [↑](#footnote-ref-23)
23. Glossaire interarmées de terminologie opérationnelle, DC-04\_GIATO(2013) amendé au 1er juin 2015. [↑](#footnote-ref-24)
24. Guy Pujolle, Cours réseaux et télécoms, Eyrolles, 2008. [↑](#footnote-ref-25)
25. Voir Comprendre et anticiper les attaques DDOS [↑](#footnote-ref-26)
26. Voir description de l’attaque par point d’eau sur le site de l’ANSSI. http://www.ssi.gouv.fr/administration/principales-menaces/lespionnage/lattaque-par-point-deau-watering-hole/ [↑](#footnote-ref-27)
27. Prestataires d’audit de la sécurité des systèmes d’information, Référentiel d’exigences, V2 14février 2013. http://www.ssi.gouv.fr/IMG/pdf/RGS\_v-2-0\_C.pdf [↑](#footnote-ref-28)
28. Prestataires d’audit de la sécurité des systèmes d’information, Référentiel d’exigences, V2 14février 2013. http://www.ssi.gouv.fr/IMG/pdf/RGS\_v-2-0\_C.pdf [↑](#footnote-ref-29)
29. Journal Officiel du 1er septembre 2000. [↑](#footnote-ref-30)
30. Journal Officiel du 22 septembre 2000. [↑](#footnote-ref-31)
31. Voir norme internationale ISO / CEI 60050. [↑](#footnote-ref-32)
32. Journal Officiel du 22 septembre 2000. [↑](#footnote-ref-33)
33. La défense en profondeur appliquée aux systèmes d’information, Mémento, 19 juillet 2004. http://circulaire.legifrance.gouv.fr/pdf/2009/04/cir\_2014.pdf [↑](#footnote-ref-34)
34. IBM ne retiens que « 4V » (Volume, Variété, Vitesse, Véracité) et Gartner [↑](#footnote-ref-35)
35. Rapport d’information du Sénat N°767 Les enjeux liés au développement du Bitcoin et des autres monnaies virtuelles. 23 juillet 2014. Consultable à l’adresse : http://www.senat.fr/rap/r13-767/r13-7671.pdf. [↑](#footnote-ref-36)
36. Journal Officiel du 20 mai 2005. [↑](#footnote-ref-37)
37. Code de postes et des télécommunications électroniques, modifié par la Loi n°2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle. [↑](#footnote-ref-38)
38. Règlement (CE) nº 2887/2000. [↑](#footnote-ref-39)
39. Journal Officiel du 26 mars 2006. [↑](#footnote-ref-40)
40. D’après « Terminologie d’usage au CERTA, 2006 » disponible à l’adresse http://www.cert.ssi.gouv.fr/ [↑](#footnote-ref-41)
41. Journal Officiel du 22 septembre 2000. [↑](#footnote-ref-42)
42. *Ibidem.* [↑](#footnote-ref-43)
43. Journal Officiel du 26 mars 2002. [↑](#footnote-ref-44)
44. Ibidem. [↑](#footnote-ref-45)
45. Glossaire de l’ANSSI, disponible à l’adresse : http://www.ssi.gouv.fr/administration/glossaire/ [↑](#footnote-ref-46)
46. Glossaire de l’ANSSI, disponible à l’adresse : http://www.ssi.gouv.fr/administration/glossaire/ [↑](#footnote-ref-47)
47. Journal Officiel du 22 septembre 2000. [↑](#footnote-ref-48)
48. Journal Officiel du 22 septembre 2000. [↑](#footnote-ref-49)
49. Idem. [↑](#footnote-ref-50)
50. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022309303 [↑](#footnote-ref-51)
51. Site de la CNIL, http://www.cnil.fr/ [↑](#footnote-ref-52)
52. Journal Officiel du 22 septembre 2000. [↑](#footnote-ref-53)
53. D’après définition du dictionnaire Larousse. [↑](#footnote-ref-54)
54. Instruction générale interministérielle n°1300 http://www.ssi.gouv.fr/archive/fr/reglementation/igi1300.pdf [↑](#footnote-ref-55)
55. Voir la présentation sur le site : http://www.fntc.org. [↑](#footnote-ref-56)
56. http://www.ssi.gouv.fr/archive/fr/reglementation/igi1300.pdf [↑](#footnote-ref-57)
57. Journal Officiel du 1er septembre 2000. [↑](#footnote-ref-58)
58. Prestataires d’audit de la sécurité des systèmes d’information, Référentiel d’exigences, V2 14février 2013. http://www.ssi.gouv.fr/IMG/pdf/RGS\_v-2-0\_C.pdf [↑](#footnote-ref-59)
59. Glossaire de l’ANSSI disponible à l’adresse : http://www.ssi.gouv.fr/administration/glossaire/c/ [↑](#footnote-ref-60)
60. Prestataires d’audit de la sécurité des systèmes d’information, Référentiel d’exigences, V2 14février 2013. http://www.ssi.gouv.fr/IMG/pdf/RGS\_v-2-0\_C.pdf [↑](#footnote-ref-61)
61. Le modèle OSI divise en couches fonctionnelles les architectures de communication entre machines. Ce modèle ne décrit pas les protocoles à utiliser. Il est généralement organisé en sept niveaux: couche physique (1), liaison de données (2), réseau (3), transport (4), session (5), présentation (6), application (7). [↑](#footnote-ref-62)
62. [http://cpe.mitre.org](http://cpe.mitre.org/) [↑](#footnote-ref-63)
63. Voir site de l’association http://creativecommons.fr/. [↑](#footnote-ref-64)
64. Journal Officiel du 22 septembre 2000. [↑](#footnote-ref-65)
65. Prestataires d’audit de la sécurité des systèmes d’information, Référentiel d’exigences, V2 14février 2013. http://www.ssi.gouv.fr/IMG/pdf/RGS\_v-2-0\_C.pdf [↑](#footnote-ref-66)
66. Glossaire de l’ANSSI disponible à l’adresse : http://www.ssi.gouv.fr/administration/glossaire/c/ [↑](#footnote-ref-67)
67. D’après *Le financement participatif en 5 chiffres clés,* disponible à l’adresse :

    http://www.toutsurlesplacements.com/crowdfunding-le-financement-participatif-en-5-chiffres-cles.html [↑](#footnote-ref-68)
68. La loi oblige les parlementaire a fournir une déclaration de patrimoine dans le cadre de la transparence de la vie politique. Les déclarations (manuscrites) sont consultables sur le site de la Haute Autorité pour la Transparence de la Vie Politique : http://www.hatvp.fr/index.html. [↑](#footnote-ref-69)
69. Défense et sécurité des systèmes d’information stratégie de la France, ANSSI, 2011 [↑](#footnote-ref-70)
70. Défense et sécurité des systèmes d’information stratégie de la France, ANSSI, 2011 [↑](#footnote-ref-71)
71. Disponible à l’adresse : http://www.cvedetails.com [↑](#footnote-ref-72)
72. Le calculateur est disponible à l’adresse https://nvd.nist.gov/cvss.cfm?calculator&adv&version=2 [↑](#footnote-ref-73)
73. Norber Wiener, *Cybernetics, or Control and Communication in the Animal and the Machine,* Librairie Hermann & Cie (Paris), The MIT Press (Cambridge, Mass.) et Wiley (New York) 1948. [↑](#footnote-ref-74)
74. Article 323-1 du Code Pénal français. [↑](#footnote-ref-75)
75. DIA 3.40 (2014) [↑](#footnote-ref-76)
76. Défense et sécurité des systèmes d’information stratégie de la France, ANSSI, 2011. [↑](#footnote-ref-77)
77. *Ibidem.* [↑](#footnote-ref-78)
78. PIA-7.2.6-3\_GIAT-0(2012) *Glossaire interarmées de terminologie opérationnelle.* [↑](#footnote-ref-79)
79. DIA 3.40 (2014). [↑](#footnote-ref-80)
80. Défense et sécurité des systèmes d’information stratégie de la France, ANSSI, 2011. [↑](#footnote-ref-81)
81. Concept Cyberdéfense, CICDE, 2011. [↑](#footnote-ref-82)
82. DIA 3.40 (2014) [↑](#footnote-ref-83)
83. *Ibidem.* [↑](#footnote-ref-84)
84. Défense et sécurité des systèmes d’information stratégie de la France, ANSSI, 2011. [↑](#footnote-ref-85)
85. Voir définition du data mining pour le marketing : http://www.definitions-marketing.com/Definition-Datamining [↑](#footnote-ref-86)
86. D’après la définition présentée dans le document de terminologie opérationnelle du ministère français de la Défense. PIA 00.401 du 8 mars 2007. [↑](#footnote-ref-87)
87. CERTA-2012-INF-002, les défigurations de site Web, 2 mars 2012; consultable à l’adresse <http://www.certa.ssi.gouv.fr/site/CERTA-2012-INF-002/CERTA-2012-INF-002.html> [↑](#footnote-ref-88)
88. La défense en profondeur appliquée aux systèmes d’information, Mémento, 19 juillet 2004. http://circulaire.legifrance.gouv.fr/pdf/2009/04/cir\_2014.pdf [↑](#footnote-ref-89)
89. Journal Officiel du 14 juin 2003. [↑](#footnote-ref-90)
90. Glossaire de l’ANSSI, disponible à l’adresse : http://www.ssi.gouv.fr/administration/glossaire [↑](#footnote-ref-91)
91. PIA 00.401 du 8 mars 2007 [↑](#footnote-ref-92)
92. Journal Officiel du 22 septembre 2000. [↑](#footnote-ref-93)
93. Journal Officiel du 3 mai 2014. [↑](#footnote-ref-94)
94. Loi du 6 janvier 1978 relative à l’informatique aux fichiers et aux libertés, modifiée. http://www.cnil.fr/fileadmin/documents/approfondir/textes/CNIL-78-17\_definitive-annotee.pdf [↑](#footnote-ref-95)
95. *Ibidem.* [↑](#footnote-ref-96)
96. Le document Microsoft Word piégé exploite la faille répertoriée le 13 novembre 2011 sous l’appellation MS11-087. [↑](#footnote-ref-97)
97. Duqu: A Stuxnet-like malware found in the wild, v0.93, 14 october 2011, technical report by the Laboratory of Cryptography and system security (CrySyS).

    <http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf> consulté le 1er juin 2013. [↑](#footnote-ref-98)
98. Rapport Symantec, W32.Duqu, The precursor to the next Stuxnet, Version 1.4, November 23, 2011.

    <https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf> consulté le 1er juin 2013. [↑](#footnote-ref-99)
99. Présentation EBIOS sur le site de l’ANSSI. http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/outils-methodologiques/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite.html [↑](#footnote-ref-100)
100. EBIOS, Méthode de gestion des risques, ANSSI, 25 janvier 2010. http://www.ssi.gouv.fr/IMG/pdf/EBIOS-1-GuideMethodologique-2010-01-25.pdf [↑](#footnote-ref-101)
101. Journal Officiel du 14 décembre 2004. [↑](#footnote-ref-102)
102. Présentation sur le site de l’ENISA disponible à l’adresse suivante : https://www.enisa.europa.eu/media/enisa-en-francais/ [↑](#footnote-ref-103)
103. En application de l’article 226-22 du Code Pénal, en cas d’installation, à l’insu des salariés, l’employeur est passible de 5 ans d’emprisonnent et d’une amende de 300 000€. [↑](#footnote-ref-104)
104. Journal Officiel du 28 décembre 2006. [↑](#footnote-ref-105)
105. Prestataires d’audit de la sécurité des systèmes d’information, Référentiel d’exigences, V2 14février 2013. http://www.ssi.gouv.fr/IMG/pdf/RGS\_v-2-0\_C.pdf [↑](#footnote-ref-106)
106. Voir la présentation à l’adresse : http://www.etsi.org/standards [↑](#footnote-ref-107)
107. Journal Officiel du 14 juin 2003. [↑](#footnote-ref-108)
108. Jean-Pierre Mendiburu, « Fading ou évanouissement, radiocommunication », *Encyclopedia Universalis [en ligne],* consulté le 25 avril 2015, URL : http://www.universalis.fr/encyclopedie/fading-evanouissement/ [↑](#footnote-ref-109)
109. Prestataires de détection des incidents de sécurité, Référentiel d’exigences, ANSSI, 17 décembre 2014. http://www.ssi.gouv.fr/IMG/pdf/PDIS\_\_referentiel\_v0-9-1.pdf [↑](#footnote-ref-110)
110. Journal Officiel du 14 juin 2003. [↑](#footnote-ref-111)
111. ANSSI, Guide de l’infogérnace. http://www.ssi.gouv.fr/IMG/pdf/2010-12-03\_Guide\_externalisation.pdf [↑](#footnote-ref-112)
112. Défense et sécurité des systèmes d’information, stratégie de la France, ANSSI, 2011. [↑](#footnote-ref-113)
113. Voir le site de la FFDN, Fédération qui regroupe les fournisseurs d’accès associatifs : http://www.ffdn.org/ [↑](#footnote-ref-114)
114. Yves Eudes, « Flame, virus espion d’Etat », Le Monde 20 juin 2012. L’ordre de grandeur exposé ici découle de la taille du code. 20 Mo pour Flame contre 1 Mo pour Stuxnet. <http://www.lemonde.fr/technologies/article/2012/06/20/flame-un-virus-espion-d-etat_1721182_651865.html> consulté le 29 juillet 2013. [↑](#footnote-ref-115)
115. ANSSI, Référentiel Général de Sécurité (RGS) V.2. http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/ [↑](#footnote-ref-116)
116. Journal Officiel du 27 février 2003. [↑](#footnote-ref-117)
117. Journal Officiel 22 septembre 2000. [↑](#footnote-ref-118)
118. Journal Officiel 22 septembre 2000. [↑](#footnote-ref-119)
119. Journal Officiel du 16 mars 1999. [↑](#footnote-ref-120)
120. Philippe Godlewski, Sami Tabbane, Xavier Lagrange, Réseaux GSM, Hermés. [↑](#footnote-ref-121)
121. Journal Officiel du 26 octobre 2006. [↑](#footnote-ref-122)
122. La défense en profondeur appliquée aux systèmes d’information, Mémento, 19 juillet 2004. http://circulaire.legifrance.gouv.fr/pdf/2009/04/cir\_2014.pdf [↑](#footnote-ref-123)
123. Présentation des menaces sur le site de l’ANSSI, disponible à l’adresse suivante : http://www.ssi.gouv.fr/administration/principales-menaces/lespionnage/lattaque-par-hameconnage-cible-spearphishing/ [↑](#footnote-ref-124)
124. ISO 3309, 4335,7448,8471. [↑](#footnote-ref-125)
125. Journal Officiel 22 septembre 2000. [↑](#footnote-ref-126)
126. Glossaire de l’ANSSI. http://www.ssi.gouv.fr/administration/glossaire/c/ [↑](#footnote-ref-127)
127. ANSSI, Guide de l’homologation. http://www.ssi.gouv.fr/IMG/pdf/guide\_homologation\_de\_securite\_en\_9\_etapes.pdf [↑](#footnote-ref-128)
128. Journal Officiel du 10 octobre 1998. [↑](#footnote-ref-129)
129. Site officiel de l’IANA http://www.internetassignednumbersauthority.com/about [↑](#footnote-ref-130)
130. Source : <http://www.icann.org/tr/french.html>. [↑](#footnote-ref-131)
131. ANSSI, Référentiel Général de Sécurité V.2. http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/ [↑](#footnote-ref-132)
132. Journal Officiel du 20 avril 2007. [↑](#footnote-ref-133)
133. Journal Officiel du 26 mars 2006. [↑](#footnote-ref-134)
134. Voir le site 3GPP : http://www.3gpp.org/technologies/keywords-acronyms/109-ims [↑](#footnote-ref-135)
135. Voir les spécifications techniques http://www.etsi.org/deliver/etsi\_ts/123000\_123099/123003/10.05.00\_60/ts\_123003v100500p.pdf [↑](#footnote-ref-136)
136. Voir la recommandation http://www.itu.int/dms\_pubrec/itu-r/rec/m/R-REC-M.1457-9-201005-S!!PDF-E.pdf [↑](#footnote-ref-137)
137. ANSSI, Guide de l’infogérance. [↑](#footnote-ref-138)
138. Glossaire de l’ANSSI disponible à l’adresse: http://www.ssi.gouv.fr/administration/glossaire/i/ [↑](#footnote-ref-139)
139. Glossaire de l’ANSSI disponible à l’adresse: http://www.ssi.gouv.fr/administration/glossaire/i/ [↑](#footnote-ref-140)
140. Instruction Générale Interministérielle 1300. http://www.ssi.gouv.fr/archive/fr/reglementation/igi1300.pdf [↑](#footnote-ref-141)
141. Journal Officiel du 22 septembre 2000. [↑](#footnote-ref-142)
142. Journal Officiel du 16 mars 1999. [↑](#footnote-ref-143)
143. Benghozi, P., Bureau, S., & Massit-Folléa, F. 2009. L’Internet des objets : Quels enjeux pour l’Europe. Paris : Éditions de la Maison des sciences de l’homme. Tiré de http://books.openedition.org/editionsmsh/78. [↑](#footnote-ref-144)
144. Journal Officiel du 22 septembre 2000. [↑](#footnote-ref-145)
145. *Ibidem*. [↑](#footnote-ref-146)
146. Voir, *Mise en œuvre IS-IS pour IPV6 (CISCO)*, Centre Interuniversitaire de ressources informatiques de Lorraine, IPV6-ADIRE, octobre 2005. [↑](#footnote-ref-147)
147. Voir présentation de l’ISO sur http://www.iso.org/iso/fr/home/about.htm. [↑](#footnote-ref-148)
148. Voir le site de l’ISOC France : http://www.isoc.fr/ [↑](#footnote-ref-149)
149. Mission de l’ISOC : http://www.isoc.fr/missions [↑](#footnote-ref-150)
150. Voir la présentation globale : http://www.qrpinternational.fr/index/itil/what-is-itil [↑](#footnote-ref-151)
151. D’après la définition du CERT-FR. [↑](#footnote-ref-152)
152. Définition proposée par la Commission Electrotechnique Internationale. http://www.electropedia.org/iev/iev.nsf/display?openform&ievref=714-01-08 [↑](#footnote-ref-153)
153. Journal Officiel du 28 décelbre 2006. [↑](#footnote-ref-154)
154. Journal Officiel du 28 décembre 2006. [↑](#footnote-ref-155)
155. La défense en profondeur appliquée aux systèmes d’information, Mémento, 19 juillet 2004. http://circulaire.legifrance.gouv.fr/pdf/2009/04/cir\_2014.pdf [↑](#footnote-ref-156)
156. Livre blanc sur les logs, OSSIR, groupe de travail, 06 novembre 3006. http://www.ossir.org/uploads/media/OSSIR\_Livre-blanc\_Logs\_v1.pdf [↑](#footnote-ref-157)
157. Journal Officiel 20 mai 2005. [↑](#footnote-ref-158)
158. Système d’exploitation pour terminaux mobiles. [↑](#footnote-ref-159)
159. Mobile Report G-DATA, https://www.gdata.fr/espace-presse/communiques/article/mobile-report-plus-de-4500-nouveaux-fichiers-malveillants-chaque-jour-sur-android [↑](#footnote-ref-160)
160. Voir la présentation complète : <https://www.gdata.fr/security-labs/informations/categories-de-logiciels-malveillants>, consulté le 1er juillet 2015. [↑](#footnote-ref-161)
161. Glossaire de l’ANSSI disponible à l’adresse : http://www.ssi.gouv.fr/administration/glossaire/m/ [↑](#footnote-ref-162)
162. Glossaire de l’ANSSI disponible à l’adresse : http://www.ssi.gouv.fr/administration/glossaire/h/ [↑](#footnote-ref-163)
163. Journal Officiel du 16 mars 1999. [↑](#footnote-ref-164)
164. Journal Officiel du 20 avril 2007. [↑](#footnote-ref-165)
165. Journal Officiel du 20 mai 2005. [↑](#footnote-ref-166)
166. Journal Officiel du 26 mars 2006. [↑](#footnote-ref-167)
167. Journal Officiel du 14 juin 2003. [↑](#footnote-ref-168)
168. Voir http://www.labo-microsoft.org/articles/win/NAP/0/#1 [↑](#footnote-ref-169)
169. Voir la définition de l’autorité de régulation des télécommunications : http://dico.developpez.com/html/1209-Telecom-NAS-Network-Access-Server.php [↑](#footnote-ref-170)
170. D’après « *Netware, Operating system documentation project*» disponible à l’adresse http://www.operating-system.org/betriebssystem/\_french/bs-netware.htm. [↑](#footnote-ref-171)
171. D’après la définition proposée dans le cadre des marchés publics. Voir http://www.marche-public.fr/Marches-publics/Definitions/Entrees/NRA-Noeud-Raccordement-Abonne.htm [↑](#footnote-ref-172)
172. D’après la définition de *Mozilla Developer Network*. https://developer.mozilla.org/fr/docs/NSS [↑](#footnote-ref-173)
173. Concept Inter Armées 3.10 [↑](#footnote-ref-174)
174. D’après la documentation CISCO, http://cisco.goffinet.org/s3/ospf1-introduction#.VJUwuBTKM [↑](#footnote-ref-175)
175. Hacking, sécurité et tests d’intrusion Metasploit. [↑](#footnote-ref-176)
176. Prestataires d’audit de la sécurité des systèmes d’information, Référentiel d’exigences, V2 14février 2013. http://www.ssi.gouv.fr/IMG/pdf/RGS\_v-2-0\_C.pdf [↑](#footnote-ref-177)
177. Journal Officiel du 10 octobre 1998. [↑](#footnote-ref-178)
178. Journal Officiel du 1er septembre 2000. [↑](#footnote-ref-179)
179. Le règlement n° 97-02 du Comité de la réglementation bancaire et financière du 21 février 1997 relatif au contrôle interne des établissements de crédit et des entreprises d’investissement [↑](#footnote-ref-180)
180. Site de l’Agence Nationale des Fréquences. http://www.anfr.fr/fr/autorisations-certificats/reseaux-independants/les-reseaux-mobiles-professionnels-pmr/definition-et-contexte.html [↑](#footnote-ref-181)
181. D’après « Sécurisation active des réseaux : notions de base » http://www.securite-informatique.gouv.fr/autoformations/securite\_reseaux/co/secu\_reseaux\_1\_ch01\_uc06.html [↑](#footnote-ref-182)
182. Journal Officiel du 22 septembre 2000. [↑](#footnote-ref-183)
183. D’après le Guide pour l’élaboration d’une politique de sécurité des systèmes d’information. PSSI, section I, Introduction, Premier Ministre, 3 mars 2004. http://www.ssi.gouv.fr/IMG/pdf/pssi-section1-introduction-2004-03-03.pdf [↑](#footnote-ref-184)
184. Glossaire de l’ANSSI disponible à l’adresse : http://www.ssi.gouv.fr/administration/glossaire/p/ [↑](#footnote-ref-185)
185. D’après RFC 1661 disponible à l’adresse suivante : http://abcdrfc.free.fr/rfc-vf/pdf/rfc1661.pdf [↑](#footnote-ref-186)
186. D’après « Comprendre Point-to-Point Tunneling Protocol », à l’adresse http://technet.microsoft.com/fr-fr/library/dd379317.aspx [↑](#footnote-ref-187)
187. Prestataires d’audit de la sécurité des systèmes d’information, Référentiel d’exigences, V2 14février 2013. http://www.ssi.gouv.fr/IMG/pdf/RGS\_v-2-0\_C.pdf [↑](#footnote-ref-188)
188. Prestataires d’audit de la sécurité des systèmes d’information, Référentiel d’exigences, V2 14février 2013. http://www.ssi.gouv.fr/IMG/pdf/RGS\_v-2-0\_C.pdf [↑](#footnote-ref-189)
189. D’après le Guide pour l’élaboration d’une politique de sécurité des systèmes d’information. PSSI, section I, Introduction, Premier Ministre, 3 mars 2004. http://www.ssi.gouv.fr/IMG/pdf/pssi-section1-introduction-2004-03-03.pdf [↑](#footnote-ref-190)
190. **Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.** [↑](#footnote-ref-191)
191. Journal Officiel du 22 septembre 2000. [↑](#footnote-ref-192)
192. Journal Officiel du 22 septembre 2000. [↑](#footnote-ref-193)
193. Claude Servin, *Réseaux et télécoms*

     *,* Dunod, 2009. [↑](#footnote-ref-194)
194. Article L111-1 du Code de la propriété intellectuelle [↑](#footnote-ref-195)
195. Journal Officiel du 22 septembre 2000. [↑](#footnote-ref-196)
196. Glossaire de l’ANSSI disponible à l’adresse : http://www.ssi.gouv.fr/administration/glossaire/q/ [↑](#footnote-ref-197)
197. Portail Web de l’ANSSI. http://www.ssi.gouv.fr/fr/certification-qualification/qualification-d-un-produit-de-securite/presentation-281.html [↑](#footnote-ref-198)
198. Décision n°2008-1362 du 4 décembre 2008. [↑](#footnote-ref-199)
199. Directive 2002/22/CE du 7 mars 2002. [↑](#footnote-ref-200)
200. Les ports 1645 et 1646 sont aussi parfois utilisés. [↑](#footnote-ref-201)
201. D’après « Protocole RADIUS » MSDN Library http://msdn.microsoft.com/fr-fr/library/cc781821%28v=ws.10%29.aspx [↑](#footnote-ref-202)
202. Journal Officiel du 10 octobre 1998. [↑](#footnote-ref-203)
203. Ordonnance téléservice 2005, art 2. [↑](#footnote-ref-204)
204. Prestataires de détection des incidents de sécurité, Référentiel d’exigences, ANSSI, 17 décembre 2014. http://www.ssi.gouv.fr/IMG/pdf/PDIS\_\_referentiel\_v0-9-1.pdf [↑](#footnote-ref-205)
205. Journal Officiel du 26 mars 2006. [↑](#footnote-ref-206)
206. ITIL, http://www.knowledgetransfer.net/dictionary/ITIL/en/Remediation.html [↑](#footnote-ref-207)
207. Glossaire de l’ANSSI disponible à l’adresse : http://www.ssi.gouv.fr/administration/glossaire/r/ [↑](#footnote-ref-208)
208. Pour une présentation plus détaillée voir du même auteur : Le renseignement pour le cyberespace dans  *Cybertactique, conduire la guerre numérique*, Nuvis 2014. [↑](#footnote-ref-209)
209. Sans être exhaustif on parle ici des données issus du *deep web*, des réseaux sociaux (contenus comme comportement), les systèmes de sauvegarde partagée, les serveurs privés, les supports amovibles, la téléphonie mobile, les réseaux métier… [↑](#footnote-ref-210)
210. Journal Officiel du 22 septembre 2000. [↑](#footnote-ref-211)
211. Journal Officiel du 14 juin 2003. [↑](#footnote-ref-212)
212. Code des postes et des communications électroniques modifié par la loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle [↑](#footnote-ref-213)
213. Journal Officiel du 9 septembre 2006. [↑](#footnote-ref-214)
214. Journal Officiel du 20 mai 2005. [↑](#footnote-ref-215)
215. Journal Officiel du 2 mars 2002. [↑](#footnote-ref-216)
216. Glossaire de l’ANSSI disponible à l’adresse : http://www.ssi.gouv.fr/administration/glossaire/o/ [↑](#footnote-ref-217)
217. Prestataires de détection des incidents de sécurité, Référentiel d’exigences, ANSSI, 17 décembre 2014. http://www.ssi.gouv.fr/IMG/pdf/PDIS\_\_referentiel\_v0-9-1.pdf [↑](#footnote-ref-218)
218. Tobias Engel a présenté ses travaux lors du CCC de Hambourg le 27 décembre 2014. [↑](#footnote-ref-219)
219. Journal Officiel du 20 avril 2007. [↑](#footnote-ref-220)
220. Journal Officiel du 16 mars 1999. [↑](#footnote-ref-221)
221. Voir également le glossaire de l’ANSSI à l’adresse : http://www.ssi.gouv.fr/administration/glossaire/s/ [↑](#footnote-ref-222)
222. Journal Officiel de la République Française, JORF n°73 du 26 mars 2006, texte n° 34 **Vocabulaire des télécommunications (liste de termes, expressions et définitions adoptés).** [↑](#footnote-ref-223)
223. Hacking, sécurité et tests d’intrusion avec Metasploit. [↑](#footnote-ref-224)
224. Journal Officiel du 22 septembre 2000. [↑](#footnote-ref-225)
225. Journal Officiel du 20 mai 2005. [↑](#footnote-ref-226)
226. Code civil, art.1316-4 al.2. [↑](#footnote-ref-227)
227. Voir Bulletin d’actualité CERTFR-2014-ACT-052 du 26 décembre 2014. [↑](#footnote-ref-228)
228. Cédric Lorens, Laurent Levier, Denis Valois, Benjamin Morin, *Tableau de bord de la sécurité réseau*, Eyrolles. [↑](#footnote-ref-229)
229. Journal Officiel du 22 septembre 2000. [↑](#footnote-ref-230)
230. Ivanka Barzashka est chercheuse associée au *Centre for Science and Security Studies* du *Department of War Studies*, King’s College London. [↑](#footnote-ref-231)
231. Ivanka Barzashka (2013): Are Cyber-Weapons Effective?, The RUSI Journal, 158:2, 48-56 [↑](#footnote-ref-232)
232. **Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.** [↑](#footnote-ref-233)
233. D’après le guide « Maitriser la SSI pour les systèmes industriels », ANSSI, V1.0 Juin 2012, disponible à l’adresse http://www.ssi.gouv.fr/uploads/IMG/pdf/Guide\_securite\_industrielle\_Version\_finale.pdf. [↑](#footnote-ref-234)
234. Instruction interministérielle relative à la protection des systèmes d’information sensibles, n°901/SGDSN/ANSSI. [↑](#footnote-ref-235)
235. Journal Officiel du 22 septembre 2000. [↑](#footnote-ref-236)
236. Prestataires d’audit de la sécurité des systèmes d’information, référentiel d’exigences, V2.0 14 février 2013,ANSSI. [↑](#footnote-ref-237)
237. **La loi « pour la confiance dans l’économie numérique » du 21 juin 2004 (n° 2004-575)** a déplacé et modifié **la loi dite «**Godfrain **» du 5 Janvier 1988 (n° 88-19)** qui avait introduit dans le code pénal un texte, désormais présent à l’article 323-1 du code pénal, lequel dispose que « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende. » [↑](#footnote-ref-238)
238. Journal Officiel du 22 septembre 2000. [↑](#footnote-ref-239)
239. Journal Officiel du 22 septembre 2000. [↑](#footnote-ref-240)
240. Voir « Guide de la sécurité des données personnelles », CNIL, 2010. http://www.cnil.fr/fileadmin/documents/Guides\_pratiques/Guide\_securite-VD.pdf [↑](#footnote-ref-241)
241. Voir https://www.dgdr.cnrs.fr/bo/2007/02-07/431-bo0207-vocabulaire1.htm [↑](#footnote-ref-242)
242. D’après Guy Pujolle, Cours réseaux et télécoms, Eyrolles, 3ème édition, 2007. [↑](#footnote-ref-243)
243. Glossaire de l’ANSSI disponible à l’adresse : http://www.ssi.gouv.fr/administration/glossaire/f/ [↑](#footnote-ref-244)
244. Présentation de UAC par Juniper voir : http://www.juniper.net/fr/fr/products-services/security/uac/ [↑](#footnote-ref-245)
245. Une architecture série est préférable aux architectures parallèles dans un contexte haut débit car en parallèle, les bits arrivent avec des décalages qui provoquent des erreurs. En série, les hautes fréquences sont mieux tolérées. [↑](#footnote-ref-246)
246. Glossaire de l’ANSSI disponible à l’adresse : http://www.ssi.gouv.fr/administration/glossaire/u/ [↑](#footnote-ref-247)
247. Voir glossaire de l’ANSSI disponible à l’adresse : http://www.ssi.gouv.fr/administration/glossaire/v/ [↑](#footnote-ref-248)
248. Voir « Terminologie d’usage au CERTA – 2006 » à l’adresse http://www.cert.ssi.gouv.fr/site/CERTA-2006-INF-002/ [↑](#footnote-ref-249)
249. Source : Secunia Vulnerability Review 2014. https://secunia.com/?action=fetch&filename=secunia\_vulnerability\_review\_2014.pdf [↑](#footnote-ref-250)