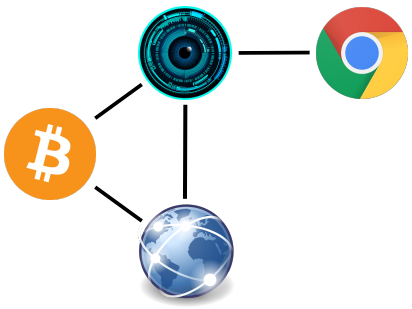


Olivier Ricou

Géopolitique de l'Internet

Version 3.1 du 24 septembre 2024

Table des matières

Introduction

De 1969 à 1982 IBM a vécu un long procès pour situation de monopole dans l'informatique. Probablement sous la pression de ce procès, IBM a délégué au début des années 80 la conception des processeurs à Intel et celle du système d'exploitation à Microsoft pour ses micro-ordinateurs IBM PC. Cette décision a permis à ces deux entreprises de devenir elles-mêmes des entreprises dominantes. Microsoft en particulier a pleinement profité du glissement de la valeur dans l'informatique du matériel vers le logiciel au point de se retrouver en quasi situation de monopole avec Windows et sa suite de bureautique durant les années 90. Cependant avec l'arrivée d'Internet, la valeur de l'informatique a glissé du logiciel aux services. Ironiquement Microsoft a eu son procès pour position monopoliste pour avoir tenté d'imposer son navigateur Internet Explorer. Depuis de nouvelles puissances se sont imposées sur le devant de la scène, à savoir les GAFA (Google, Apple, Facebook et Amazon). Microsoft a raté le train de l'Internet ainsi que celui des ordiphones (mais qui se rattrape très bien dans les domaines du nuage (*cloud*) avec Azure et de l'intelligence artificielle via OpenAI).

Aujourd'hui le ministère américain de la justice poursuit Google pour position dominante dans les moteurs de recherche et la publicité en ligne.

Si le premier changement de valeur, du matériel vers les logiciels est dû à la démocratisation de l'informatique, le second est dû à son omniprésence dans nos vies. L'humain est devenu connecté, ses appareils informatiques étant autant d'extensions. Nous sommes devenus dépendants du réseau, de ses services, et cette dépendance nous la devons à Internet.

Il faut dire qu'en trente ans Internet est passé d'un outil confidentiel d'universitaires à un mass média doublé d'un outil de travail incontournable et d'un mode vie. Trente ans, c'est rapide à l'échelle d'une société. Internet a bouleversé nos habitudes à tel point que son avènement peut être comparé à celui de l'imprimerie en accéléré. Des secteurs entiers de notre société ont dû s'y adapter. Le monde des médias a dû intégrer ce nouveau venu qui lui retire l'exclusivité de l'information et décuple le pouvoir du bouche à oreille pour le meilleur et pour le pire. Les politiques, surpris par ce trublion qui supprime la notion de pouvoir pyramidal, ont dû et doivent encore adapter les lois. La bourse, star de notre époque, a salué l'arrivée de ce nouvel élément en y voyant un eldorado puis un gouffre financier pour finalement y trouver les premières entreprises dont la capitalisation a dépassé les 1000 milliards de dollars. Les ados mais aussi les adultes y ont trouvé un espace d'expression leur permettant de communiquer entre eux simplement et sans limites au point de générer de nouvelles maladies pour les plus accros. Les entreprises ont été conquises par cet outil tellement économique et pratique à une époque où tout se numérise. Et bien sûr, les malfaisants utilisent Internet pour arnaquer à distance les plus naïfs, pirater les entreprises voire les États, lesquels se défendent, tout en faisant la

cyber-guerre entre eux.

Si Internet a pu bouleverser à ce point notre société, c'est que sa technique développée depuis les années 60 a été assez souple pour s'adapter aux besoins et aux innovations tout en étant assez solide pour résister au passage à l'échelle qu'a été l'arrivée de cinq milliards d'internautes. Et si la technique a su être à la hauteur c'est grâce à une politique de consensus développée depuis les années 70 où chaque protagoniste pouvait, et peut, s'exprimer et s'informer librement en dehors de considérations commerciales. Ces aspects ont permis la création de protocoles ouverts et gratuits permettant à chacun de les appliquer et rendant l'usage d'Internet si fiable et si peu coûteux.

Ce livre à pour but de présenter les coulisses d'Internet : comment Internet est gouverné, quels sont les forces en présence, les luttes, les abus, les disruptions qu'il génère et en quoi tout cela impacte le monde physique. En explorant la faune d'Internet, dont une représentation partielle est donné figure 1, j'espère offrir au lecteur une vision approfondie de cet univers qui lui permette de mieux appréhender le potentiel, les bénéfices mais aussi les dangers d'Internet.

Comme pour toute histoire, ce livre se doit de commencer par planter le décor. Dans notre cas, nous regarderons les fondamentaux informatiques d'Internet et les bases de son fonctionnement sans entrer dans les détails trop techniques. Puis nous abordons le monde de la sécurité, si mal appréhendée et pourtant tellement importante dans notre monde intégralement connecté.

Une fois ces explications faites, on abordera l'histoire d'avant, lorsqu'Internet n'était qu'universitaire, pour arriver à l'histoire d'aujourd'hui et au poids d'Internet dans notre monde. Cela nous permettra de comprendre comment Internet est gouverné, d'où viennent les influences, quel est le poids des entreprises, ce que font les États et ce qu'il ne peuvent pas faire.

La seconde partie étudie deux domaines radicalement transformés par l'arrivée de l'Internet : la communication et la désinformation puis le commerce en ligne et les moyens de paiement. Cela sera l'occasion de découvrir le Bitcoin et les crypto-monnaies.

La dernière partie se focalise sur la politique. Internet a rapidement été utilisé comme outil de coordination par les contestataires, puis pour mener une révolution (on pense au Primptemps arabe). À l'inverse Internet est aussi un outil de contrôle de la population, de surveillance massive comme l'a révélé E. Snowden. Les niveaux suivants sont l'espionnage et la cyber-guerre, déjà bien intégrée dans les forces armées.

Enfin on termine sur une note d'espoir : celle de voir Internet sauver nos démocraties malades en permettant de nouvelles formes de démocratie. En attendant il permet déjà aux citoyens de mieux s'informer, de s'organiser et d'interagir avec les dirigeants.

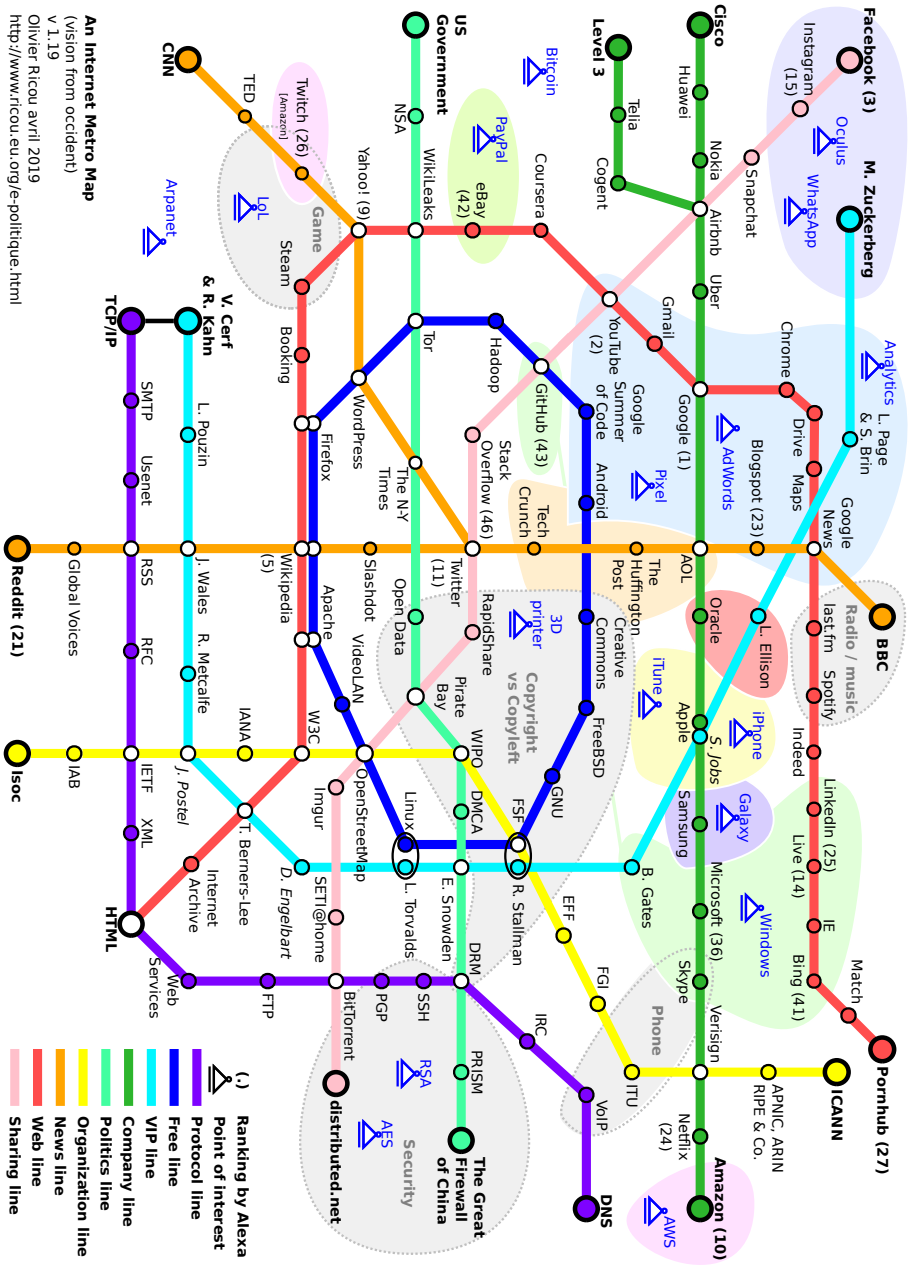


FIGURE 1 – Un plan du métro de l'Internet

Première partie

La chose

Chapitre 1

La mécanique d'Internet

Ce premier chapitre est le chapitre technique du livre. Il est divisé en deux parties. La première présente les bases du fonctionnement d'Internet avec ses spécificités techniques. La seconde partie parle de sécurité, des dangers mais introduit aussi quelques notions mathématiques afin de démystifier la cryptographie. Si on considère qu'Internet est un réseau physique avec des protocoles de communication, des logiciels et finalement des utilisateurs qui forment la couche sociale, ce chapitre se concentre sur les premiers niveaux.

1.1 Le réseau

La grande force d'Internet est de permettre aux machines de communiquer entre elles. Historiquement d'autres systèmes ont permis la même chose, mais Internet a gagné la compétition pour devenir l'objet indispensable qu'il est aujourd'hui.

Grâce à Internet et aux logiciels toujours plus conviviaux, des milliards de personnes peuvent communiquer sans ce soucier de la technique sous-jacente. Pourtant il est intéressant de regarder sous le capot pour comprendre les enjeux de pouvoir mais aussi pour mieux comprendre qui contrôle nos usages et comment.

Dans son principe, la mécanique d'Internet est simple. Elle est basée sur deux notions :

1. un empilement de protocoles de communication avec au milieu une *langue* commune composée des protocoles TCP et IP [1], voir l'encart page 16,
2. la connexion de machines en réseaux et l'interconnexion des réseaux (ce qui a donné le nom Inter-Net).

1. pour simplifier, il existe aussi UDP sur IP utilisé pour la vidéo par exemple et d'autres nettement moins utilisés.

Une langue commune

Le premier point souligne le fait que toutes les machines connectées à Internet parlent la langue informatique commune qu'est TCP/IP [2]. Outre l'aspect d'une langue commune, l'utilisation de TCP/IP impose une numérotation unique des machines, comme il existe une numérotation des téléphones. Cette numérotation est appelée l'adresse IP [3] et se présente sous la forme de 4 nombres inférieurs à 256 séparés par des points comme `134.157.1.12`.

Ainsi deux ordinateurs respectant le protocole TCP/IP peuvent se contacter et communiquer si il existe une liaison entre eux.

TCP/IP, le protocole d'Internet

Les informaticiens ont découpé les communications, entre deux machines ou entre deux programmes, en couches avec le principe que chaque couche communique seulement avec les deux couches l'encadrant. Le modèle de référence des informaticiens fait intervenir 7 couches allant de la couche physique, comment transmettre des 0 et des 1 avec du courant électrique ou des photons, à la couche applicative sur qui définit le protocole de communication d'un programme.

Internet réduit le nombre de couches mais le principe reste le même. Il impose seulement d'utiliser le tronc commun que sont la couche de transport, TCP ou UDP, et la couche réseau qu'est IP. C'est la raison pour laquelle on associe Internet au protocole TCP/IP.

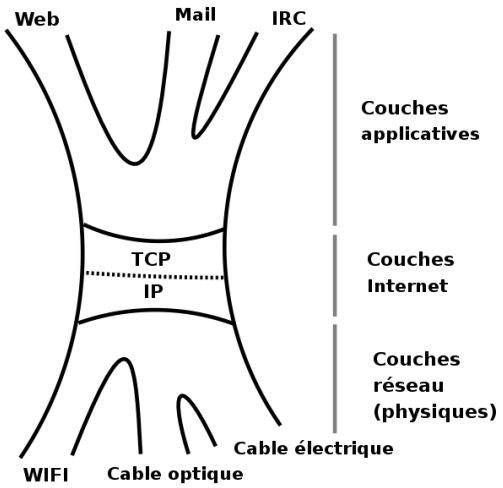


FIGURE 1.1 – TCP/IP au cœur du protocole de communication d'Internet

Ainsi les supports physiques et leur protocole peuvent varier sans avoir d'impact sur la compatibilité Internet. Ce modèle permet aussi de définir tous les protocoles applicatifs désirés tant qu'*in fine* leur couches applicatives peuvent se raccorder à la couche de transport. D'où la possibilité de créer toutes les applications imaginables.

2. en informatique on parle de *protocole*.
3. Ip version 4, la version encore la plus répandue. Pour une brève description de la version suivante, IP version 6, voir l'encart page 18.

Des machines connectées en réseau, des réseaux interconnectés

Le second point souligne la structure d'Internet : Internet est une interconnexion de réseaux indépendants, cf figure 1.2. Que vous soyez chez vous, au travail ou à l'hôtel, votre connexion à Internet passe par un premier réseau qui est le réseau local. Chez vous il est composé de vos appareils connectés et sa limite est la *box* qui vous relie au réseau de votre fournisseur d'accès. Sur le dessin votre réseau local peut être le Bleu et celui de votre fournisseur le Marron. Le réseau Vert étant relié au réseau Marron, vous pouvez vous y connecter depuis votre réseau local.

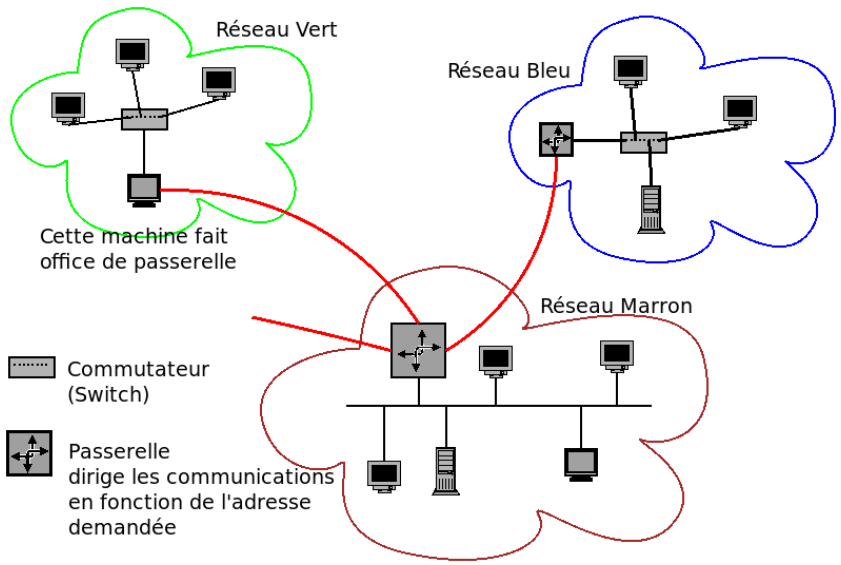


FIGURE 1.2 – Des réseaux interconnectés.

La connexion entre les réseaux passe par des machines spéciales très importantes puisque permettant l'accès aux autre réseaux donc à Internet. Il s'agit des passerelles qui sont le plus souvent des routeurs (une box est un routeur).

On retrouve ce même schéma avec des grosses organisations, les réseaux Bleu et Vert étant des réseaux de départements et le réseau Marron étant le réseau principal de l'organisation. Cette architecture permet au réseau principal de contrôler ce qu'il laisse passer vers Internet.

Cette notion de sous-réseaux apparaît aussi au niveau des adresses IP dans l'ordre des 4 nombres. Le premier nombre indique une zone, le second une sous-zone... comme `33 1 42 37 xx xx` indique que ce téléphone est en France, dans la région parisienne, à coté de la Croix de Berny (237 étant BER). Mais la comparaison se limite là car l'adressage IP est plus souple, les sous-réseaux n'ayant pas obligatoirement le même préfixe que le réseau auquel ils appartiennent et surtout l'adresse IP n'est pas géographique. D'ailleurs l'attribution des numéros de téléphone a aussi évolué et n'est plus basée sur la position géographique.

Le danger de l'analogie avec le téléphone

```
B1gron : jve te tracé ac ton ip
Nonoeil: Cool.
B1gron : tu va voir
Nonoeil: Oui. Je vais voir, comme tu dis.
B1gron : put1 sa marche pa!!! ta 1 brouyeur????
Nonoeil: Mais qu'est-ce qu'il dit l'autre ? Qu'est-ce qui ne marche pas ?
B1gron : sa sonne mm pa che toi
Nonoeil: ça sonne ? Je suis au boulot là, tu vas tomber sur le Central,
         si t'appelles, mon rigolo
B1gron : ok alor le central a 1 brouilleur
Nonoeil: le central a ce qu'il veut en même temps
B1gron : jvé tosser cher a coze de ses coneries
Nonoeil: Ouais ouais. Si tu le dis !
Myrdène: Mais attends... T'as composé son numéro IP sur ton portable, B1gron ?
B1gron : ui pk???
```

source : Les perles d'IRC, `www.danstonchat.com`

Ainsi une entreprise connue possède les adresses IP qui commencent par `129.42`[4]. Il est probable qu'elle a distribué à ses départements des sous-réseaux comme `129.42.2.xxx` pour le département Vert, `129.42.3.xxx` pour le Bleu etc...

Si le département Bleu s'achète une connexion directe vers Internet qui ne passe pas par le réseau Marron, alors cela lui offre deux façons de se connecter à Internet. Il est fort probable que les responsables du réseau n'apprécient guère car ils ne pourront plus filtrer toutes les communications entre l'entreprise et Internet, ce qui rendra d'autant plus difficile la protection du réseau.

IPv6

La nouvelle version d'IP est la version 6, déjà en activité même si l'ancienne version, la version 4, reste la plus courante. La version 6 a été créé afin principalement de répondre au manque d'adresse IPv4 pour tout le monde. Avec 128 bits par adresse, la version 6 offre $2^{128} = 3,4\ 10^{38}$ adresses ce qui fait 670 billiards d'adresses par millimètre carré sur la Terre.

Préfixe (48 bits)	Sous-réseau (16 bits)	Interface (64 bits)
`2001:0db8:0000:`	`85a3:`	`0000:0000:ac1f:8001`

TABLE 1.1 – Format des adresses d'IPv6

Une adresse s'écrit en hexadécimal (contrairement à IPv4). Ainsi par exemple on a `2001:0db8:0000:85a3:0000:0000:ac1f:8001` ce qui peut aussi être écrit en suprimant les zéros non significatifs `2001:db8:0:85a3:0:0:ac1f:8001` voire `2001:db8::85a3::ac1f:8001`.
On peut faire varier la taille du préfixe et du sous-réseau.

4. on peut trouver son nom avec la commande `whois 129.42.1.1`

Des adresses à usage privé

Comment a-t-on une adresse IP ? En la demandant à celui qui vous fournit la connexion à son réseau. Il vous donnera une adresse parmi celles qui lui ont été attribuées.

Vous pouvez aussi utiliser, sans rien demander, des adresses réservées à usage interne et donc interdites sur Internet. Il s'agit pour la version 4 d'IP de :

- `10.xx.xx.xx` pour se faire un très gros réseau local (16 millions de machines),
- `172.16 à 31.xx.xx` pour un gros réseau (1 million de machines)
- `192.168.xx.xx` pour un réseau moyen (65 000 machines quand même),
- `127.0.0.1` pour désigner votre machine (chaque machine a au moins 2 adresses IP : celle ci qui ne sert qu'à usage interne, l'autre pour communiquer avec l'extérieur.)

Pour IP version 6, les adresses privées appartiennent à l'espace `fc00::/7` (cf RFC4193). En pratique cela revient à choisir comme préfixe `fd` puis à choisir de façon aléatoire l'identifiant global et l'identifiant de sous-réseaux. On a ainsi 2^{64} adresses pour soi et très peu de chances qu'une autre personne ait le même réseau privé.

Internet : des milliers de réseaux

D'un point de vue topologique, Internet n'est que la duplication en millions d'exemplaires de la figure 1.2. Pour avoir une image globale il faut détecter quels réseaux sont reliés à quels réseaux, ce qu'a fait sur une partie d'Internet CAIDA en 2001 en analysant 535 000 nœuds d'Internet et plus de 600 000 connexions, cf figure 1.3.

Un point, une adresse IP, est rattachée à un son réseau local et forme un premier groupe de point sur le dessin, une petite tache. Ce groupe du réseau local est le plus souvent rattaché à un groupe qui est celui de son fournisseur d'accès. Ce groupe appartient à un plus grand groupe qui est le réseau du cablo-opérateur [5]. Enfin les cablo-opérateurs ont des interconnexions entre eux.

On voit que le réseau n'est pas totalement distribué mais que chaque groupe a un nœud d'interconnexion qui relie le groupe au groupe père. Ceux qui contrôlent ces nœuds d'interconnexion peuvent limiter les communications, les bloquer ou les espionner. Bien sûr un État peut faire de même avec les nœuds qui sont sur son territoire.

Une autre représentation graphique d'Internet est proposée figure 1.4. Cette fois il s'agit d'une version où chaque point représente un réseau. La taille des points correspond à la taille du réseau et la taille des liens au débit entre les réseaux reliés. Les couleurs des points correspondent au type du réseau (commercial, académique, administratif...). Les auteurs de ce dessin on placé les réseaux les plus importants sur les nœuds d'un maillage grossier plus les nœuds moins important sur un maillage plus fin etc.

5. les cablo-opérateurs sont les entreprises qui posent les câbles d'Internet. Les grandes entreprises des télécommunications sont souvent des cablo-opérateurs, cf section [**?**].

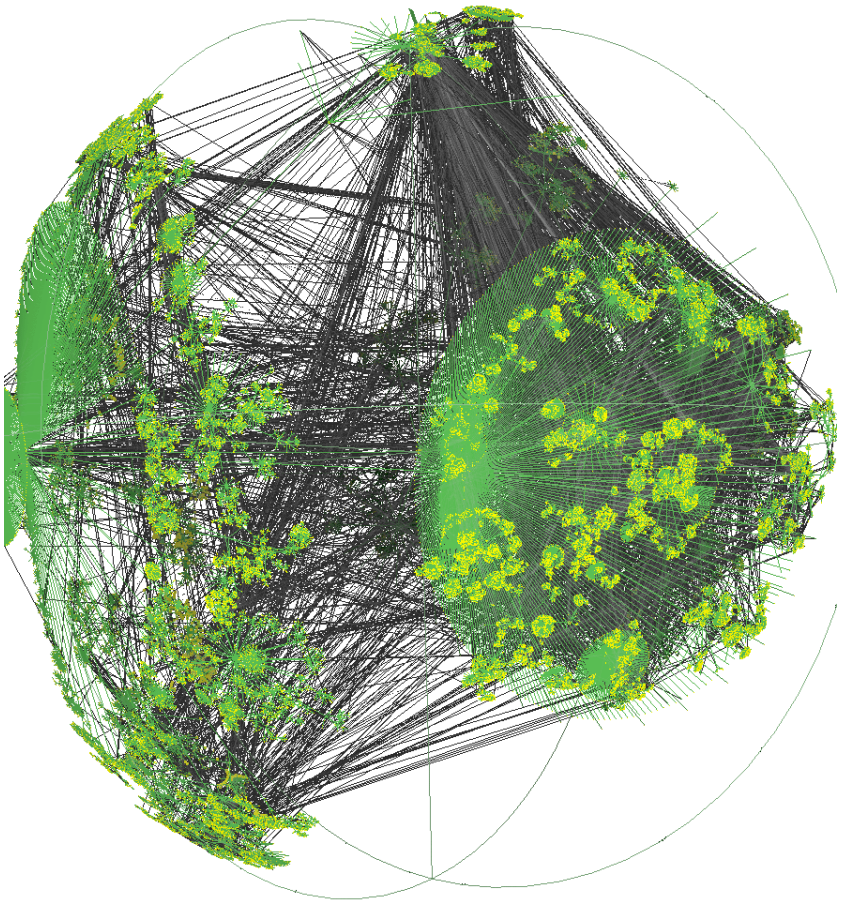


FIGURE 1.3 – Une partie d'Internet vue par le logiciel Walrus
source : CAIDA, mars 2001

1.1.1 L'information relayée de réseaux en réseaux

Que l'on envoie un mail à une machine distante ou que l'on récupère une page web, le principe est le même : l'information est découpée en paquets relayés de réseaux en réseaux.

Traceroute montre le chemin

La détection des réseaux et de leur interconnexion peut se faire simplement à l'aide de la commande `traceroute`, mais aussi par le Web à partir de machines qui offrent ce service, cf http://www.traceroute.org/. Ce programme permet de suivre la route d'un chemin entre deux machines d'Internet. Si l'affichage produit peut sembler abscons au premier abord, il est en fait relativement simple : chaque ligne représente une machine par laquelle passe le message. Ainsi on peut connaître son environnement et la qualité de sa connexion à Internet ou au moins aux nœuds d'Internet que l'on considère le plus important.

En agrégeant les résultats on peut présenter une vue partielle des réseaux d'Internet et de leurs connexions comme le font les figures 1.3 et 1.4.

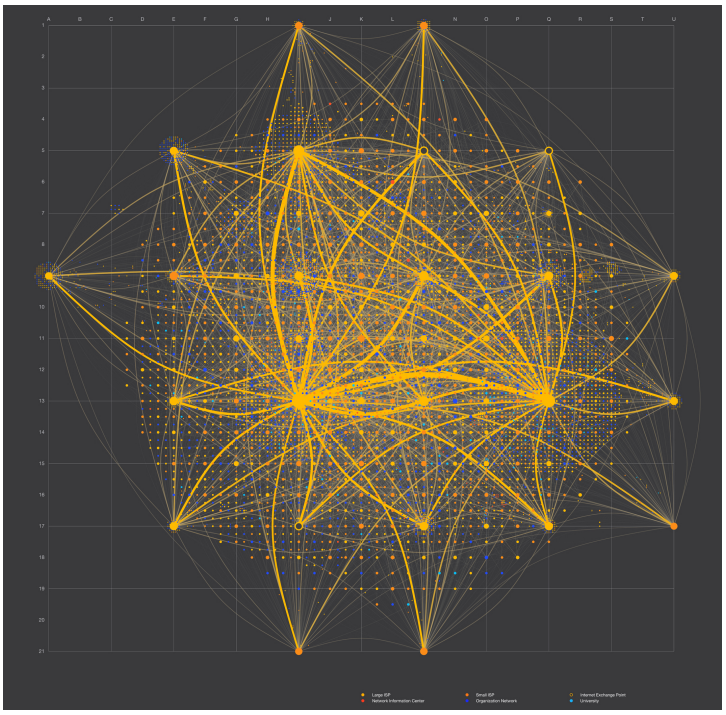


FIGURE 1.4 – L'interconnexion des réseaux (AS) d'Internet
source : Noosphe.re – 2011

Un exemple : la route entre deux universités

Dans l'exemple qui suit, la connexion entre Jussieu et le MIT n'utilise que des réseaux académiques :

```
(mendel)../home/ricou>traceroute www.mit.edu
traceroute to www.mit.edu (18.7.22.83), 30 hops max, 40 byte packets
 1  134.157.204.126 (134.157.204.126)
 2  cr-jussieu.rap.prd.fr (195.221.126.49)
 3  gw-rap.rap.prd.fr (195.221.126.78)
 4  jussieu-g0-1-165.cssi.renater.fr (193.51.181.102)
 5  nri-c-pos2-0.cssi.renater.fr (193.51.180.158)
 6  nri-d-g6-0-0.cssi.renater.fr (193.51.179.37)
 7  renater-10G.fr1.fr.geant.net (62.40.103.161)
 8  fr.uk1.uk.geant.net (62.40.96.90)
 9  uk.ny1.ny.geant.net (62.40.96.169)
10  esnet-gw.ny1.ny.geant.net (62.40.105.26)
11  198.124.216.158 (198.124.216.158)
12  nox230gw1-PO-9-1-NoX-NOX.nox.org (192.5.89.9)
13  nox230gw1-PEER-NoX-MIT-192-5-89-90.nox.org (192.5.89.90)
14  B24-RTR-3-BACKBONE.MIT.EDU (18.168.0.26)
15  WWW.MIT.EDU (18.7.22.83)
```

Un essai fait d'une machine chez un fournisseur d'accès commercial français vers une université française fera apparaître la machine passerelle `renater.par.franceix.net` qui sert de passerelle entre Renater et les réseaux commerciaux. Elle est située dans le GIX [6] nommé France-IX [7] (anciennement SFINX) qui permet à tous les opérateurs Internet de se relier entre eux suivant leurs accords, dit accords de peering.

Essayons de comprendre le chemin suivi par notre paquet IP entre Jussieu et le MIT. Le premier intermédiaire que notre message va rencontrer est la passerelle de notre réseau. Son adresse IP est 134.157.204.126 comme on le voit sur la ligne numérotée 1. De là on rejoint l'interconnexion entre Jussieu et le RAP, réseau académique parisien, en 2, pour entrer sur le réseau universitaire français, Renater, en 4, cf figure 1.5.

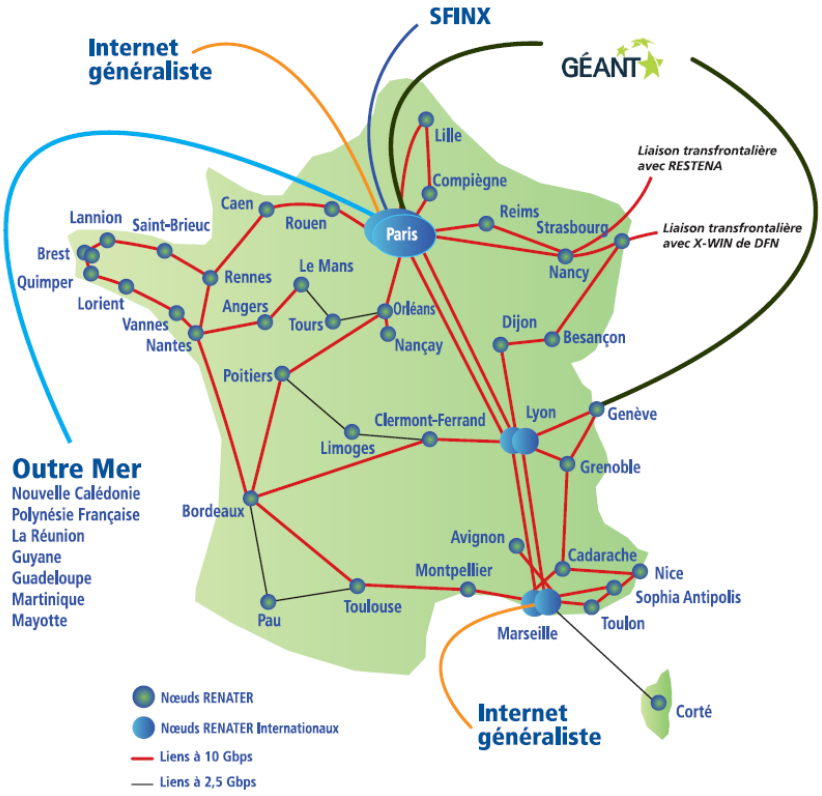


FIGURE 1.5 – Renater, le réseau universitaire français
source : Renater 2011

On passe de Renater à Géant, le réseau universitaire européen, en 7, qui nous envoie en Angleterre, en 8, d'où on va à New-York rejoindre le réseau académique d'Amérique du Nord, Internet 2, en 9 et 10, cf figures 1.6 et 1.7.

De là on passe sur NOX, le réseau de la Nouvelle Angleterre, en 12 et 13, pour atteindre le réseau du MIT, en 14, et enfin le serveur web `www.mit.edu`, en 15, cf figure 1.8.

6. Global Internet eXchange point ou IXP, Internet eXchange Point.
7. la liste de membres parisien de ce GIX est sur https://www.franceix.net/en/france-ix-paris/members-in-paris/

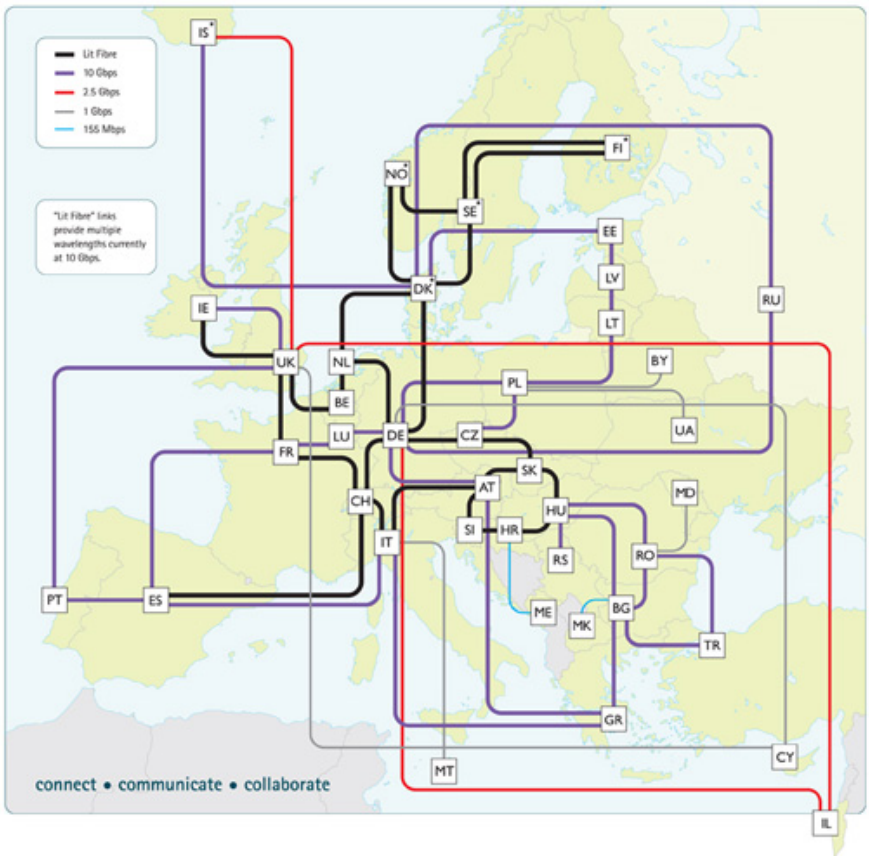


FIGURE 1.6 – Géant, le réseau universitaire européen
source : Géant, 2012

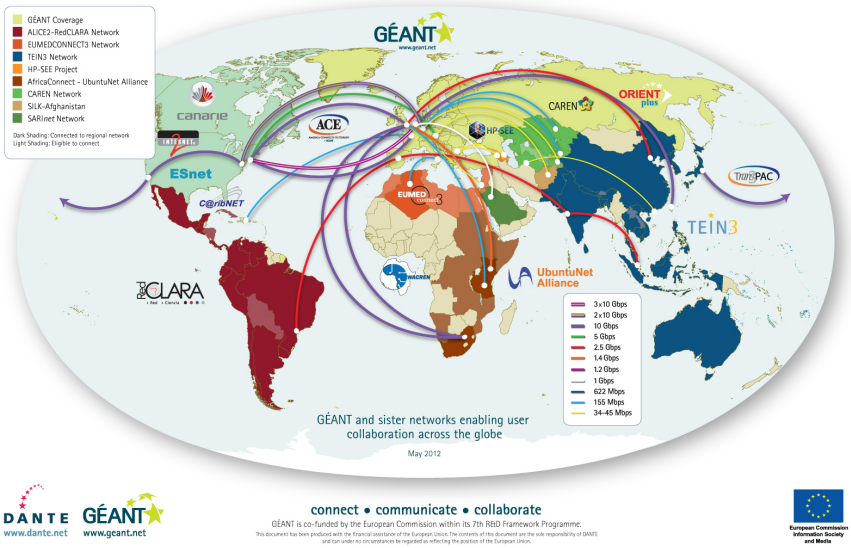


FIGURE 1.7 – Interconnection entre Géant et les autres réseaux académiques
source : Géant, 2012

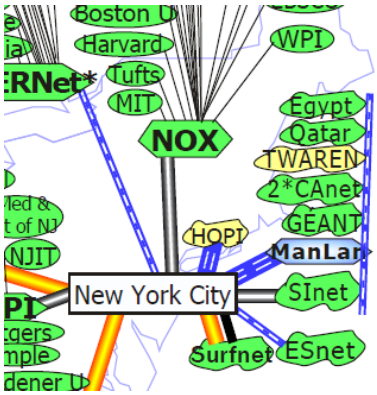


FIGURE 1.8 – Internet 2 et NOX pour arriver au MIT
source : Internet 2, 2005

Le calcul du débit

Sachant que le débit entre deux machines est celui du nœud le plus faible, si un réseau a un goulot d'étranglement en un point, cela se ressent directement. Aussi il est toujours bon de savoir quels seront vos partenaires principaux et de savoir par quels opérateurs vous devrez passer. En pratique il faut savoir quels accords d'interconnexion a votre hébergeur, avec quels opérateurs, à quel débit et quelle est l'occupation moyenne du réseau.

Certains opérateurs proposent de pouvoir suivre en direct la *météo* de leur réseau, malheureusement cette information est devenue rare en France. On peut néanmoins avoir quelques informations :

— L'état du réseau chez Free est visible sur http://www.free-reseau.fr/
— Le tableau de bord de Nerim permet de voir vers quels réseaux vont les données des clients de Nerim et le débit

Il est aussi possible de faire le travail à la main avec des outils comme `iperf3` qui mesurent le débit entre deux machines dont on a le contrôle ou entre sa machine et un serveur ouvert comme ceux indiqué sur https://iperf.cc/.

1.1.2 Des domaines et des noms

Des noms Au commencement les machines avaient des numéros et rapidement des noms tant pour faciliter la vie des humains que pour permettre de changer l'adresse numérique de la machine sans en changer son nom [8]. Dès 1973 la correspondance entre les noms et les adresses numériques des machines reposait sur un fichier avec les noms et adresses IP de toutes les machines d'Internet. Cela impliquait de télécharger ce fichier régulièrement pour connaitre les

8. L'adresse IP est liée au réseau ce qui implique de changer d'adresse IP lorsqu'on change une machine de réseau. Avoir un nom qui redirige vers une adresse IP permet de changer l'IP tout en garantissant la continuité des service basés sur le nom (mail, web...).

nouvelles machines reliées à Internet et les changements d'adresse. Puis le nombre de machine est devenu trop important et variait trop vite pour garder ce fichier à jour sur toutes les machines. Aussi en 1984 on a créé un service appelé Domain Name System, DNS, qu'on interroge pour connaître l'adresse IP d'une machine dont on connaît le nom.

L'archéologie des noms de machines

Un ami qui aime consulter les textes de référence de l'Internet que sont les RFC, Request For Comments, a fait cette constatation :

- RFC 1, avril 1969 : aucune mention des noms des machines, juste les adresses (sur 5 bits)
- RFC 33, février 1970 (remplace RFC 1) : toujours pas de noms, mais les adresses passent à 8 bits
- RFC 229, septembre 1971 : première mention des noms. Aucun mécanisme de résolution n'est envisagé (même pas un simple fichier de correspondances) mais il y a une table des noms officiels et de l'adresse correspondante.
- RFC 606, décembre 1973 : première mention d'un mécanisme de résolution, un fichier, avec une syntaxe formelle, placé à un endroit bien connu, le futur HOSTS.TXT

Le DNS tel qu'il est aujourd'hui arrivera seulement en 1984.

Des domaines Internet étant un ensemble de réseaux, il semble naturel que chaque réseau ait un nom de domaine dans lequel il peut ranger ses sous-réseaux et machines. Mais se pose alors la question de l'organisation globale et comment faire pour que chaque réseau connaisse les noms de tous les autres réseaux. La réponse retenue a été un système d'arborescence dont chacun connait la racine et qui permet de retrouver tout le monde à partir de la racine.

Regardons la figure 1.9 page 26. La terminaison la plus à droite est la machine `whois.eu.org.`. Pour comprendre ce nom il est plus simple de le lire de droite à gauche avec au début la racine que l'on nomme " . " [9]. En continuant de droite à gauche on trouve le domaine terminal [10] `org` et ensuite le domaine `eu.org` auquel appartient la machine `whois`.

On imagine bien qu'il ne serait pas gérable que chaque machine obtienne son nom d'une seule autorité tant pour des raisons de performance que de praticité (sans parler du contrôle absolu qu'aurait ainsi cette autorité sur Internet). Aussi le nommage d'Internet se base sur un système de délégation de zone. Ainsi `.org` à délégué la gestion de `.eu.org` ce qui fait que `.eu.org` est une zone indépendante de la zone `.org` et qu'elle peut faire ce qu'elle veut en "dessous" de `eu.org`.

La figure 1.10 montre que le domaine `eu.org` délègue les sous domaines `gr`, `dk` et `uk.eu.org` mais gère le sous domaine `fr.eu.org` et les machines `www` et `whois.eu.org`.

9. .org est un raccourci accepté pour .org. où le point final qui correspond à la racine est oublié.
10. *Top Level Domain* ou TLD

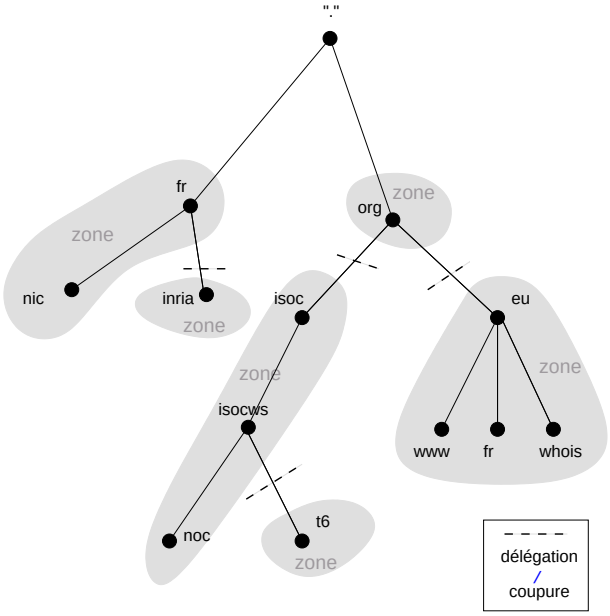


FIGURE 1.9 – Une toute petite partie de l'arborescence des noms de domaines

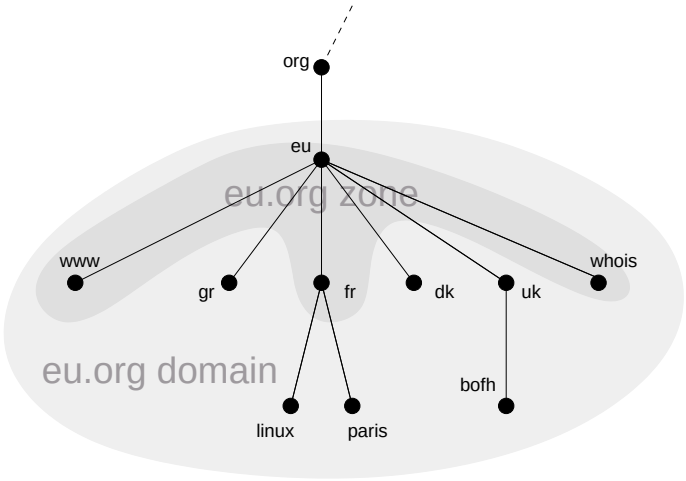


FIGURE 1.10 – La différence entre une zone et un domaine

Il existe donc :

— les *domaines* qui comprennent tout ce qui finit par le nom de domaine,
— les *zones* formées de l'ensemble des machines et sous-réseaux contrôlés par le propriétaire du nom de domaine.

On comprend ainsi pourquoi le propriétaire d'un domaine, comme `.fr`, ne peut être tenu responsable de ce qu'on trouve sur un serveur web hors de sa zone, comme `www.tf1.fr` par exemple.

Par contre, techniquement parlant, il peut toujours retirer la délégation de zone et donc fermer le domaine `tf1.fr`. De même le gestionnaire du point final peut fermer `.com` ou `.fr`.

Confessions d'un voleur ou l'argent des noms de domaines

par Laurent Chemla, co-fondateur de la société Gandi

Je vends des noms de domaines sur Internet.

Un peu d'histoire et de technique sont nécessaires pour comprendre à quel point je suis un voleur.

Un nom de domaine, c'est ce qui sert à identifier un ordinateur sur Internet. Quand on vous propose d'aller visiter www.machinchose.org on vous indique un nom d'ordinateur (www) qui se trouve dans le domaine « machinchose.org » et qui contient ces informations que vous pouvez consulter sur le Web.

Sans un nom de ce genre, un ordinateur ne peut être consulté qu'en utilisant un numéro, tel que par exemple 212.73.209.251. C'est nettement moins parlant et beaucoup plus difficile à mémoriser. Alors pour simplifier on donne des noms aux ordinateurs qui contiennent de l'information publique. Ce qui nécessite, bien sûr, une base de données qui soit capable de retrouver un numéro à partir d'un nom. Et que cette base soit unique et accessible de n'importe où.

Pendant des années, ce système a fonctionné grâce à un organisme de droit public financé par le gouvernement américain. L'Internic (c'était le nom de cet organisme) se chargeait de faire fonctionner la base de donnée, et chacun pouvait y ajouter le nom de domaine de son choix, gratuitement, selon la règle du « 1er arrivé 1er servi ».

Puis vint le temps de l'ouverture d'Internet au grand public (1994), et la fin des subventions gouvernementales au profit du seul marché. Et là, surprise : une agence publique (qui gérait gratuitement ce qu'il faut bien appeler une ressource mondiale unique) fut transformée en entreprise commerciale (Network Solutions Inc, ou NSI), sans que quiconque s'en émeuve particulièrement, et se mit à vendre 50$ par an (puis 35$ par an dans un fantastique élan de générosité) ce qui était totalement gratuit peu de temps avant. Et pour son seul profit.

Je dois vous livrer un chiffre qui, s'il n'est pas confidentiel, mérite cependant le détour : le coût réel de l'enregistrement d'un nom dans la base de données mondiale, y compris le coût de fonctionnement d'une telle base, a été évalué il y a deux ans à 0,30$.

Des chiffres comme ça, je pourrais en donner beaucoup. Je pourrais dire par exemple qu'en estimant le nombre de domaines enregistrés par NSI à une moyenne mensuelle de 40.000, son bénéfice sur les 5 dernières années tourne autour des 80 millions de dollars. Et encore ce chiffre est-il une estimation basse, quand on sait que NSI vient d'être racheté par une autre Net-Entreprise pour la modique somme de 21 milliards de dollars.

Et pourtant, NSI vend du vent, tout comme moi. En fait, nous vendons le même vent.

source : Extrait d'un article publié dans le journal Le Monde en avril 2000 et disponible dans son intégralité sur http://www.chemla.org/textes/voleur.html.

`eu.org`, des domaines gratuits

L'exemple `eu.org` est d'autant plus intéressant que ce domaine délègue gratuitement des sous domaines c.a.d. que si vous désirez avoir un sous domaine comme `ricou.eu.org`[a], il suffit de le demander sur le site web `www.eu.org`. Cela demande bien sûr de savoir gérer un sous domaine.

a. `ricou.eu.org` est déjà pris et pour longtemps puisque c'est gratuit.

Trouver l'adresse IP d'un nom, le fonctionnement du DNS

La recherche d'une adresse IP est l'opération initiale pour chaque connexion dès lors que l'on initie la connexion avec le nom de la machine et non son adresse IP. Pour faire la correspondance nom/adresse IP, vous devez avoir indiqué à votre machine l'adresse d'un "Serveur de nom", ou serveur DNS. Si tel n'est pas le cas vous ne pourrez plus vous connecter aux autres machines d'Internet, sauf en donnant directement leur adresse IP bien sûr.

Pour trouver l'adresse IP d'une machine à partir de son nom, votre serveur de nom va lire le nom de la machine de droite à gauche pour savoir à quel autre serveur de nom il pourra demander l'adresse IP s'il ne la connaît pas.

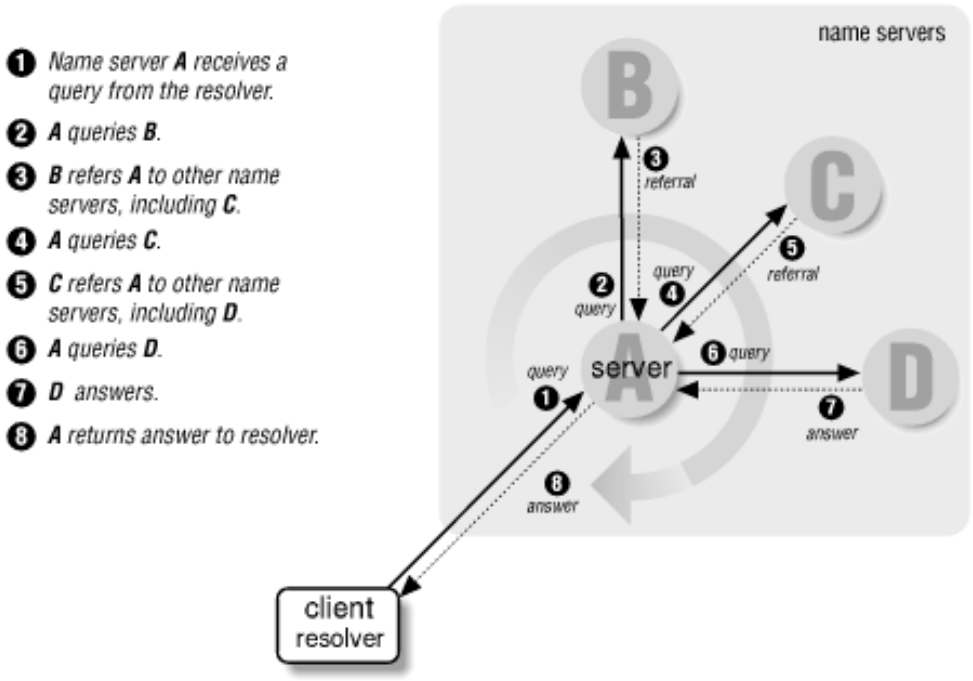


FIGURE 1.11 – Fonctionnement récursif du DNS
(illustration extraite du livre DNS & Bind chez O'Reilly)

Supposons que l'on cherche à se connecter sur le serveur web `www.jussieu.fr`. Notre serveur

de nom, A sur la figure 1.11, n'a rien en mémoire et donc pas l'adresse IP [11] de cette machine. Aussi il demande a un des serveur racine du DNS [12] dont l'adresse est stockée dans chaque serveur de nom. Le serveur racine, B sur la figure, qui ne connait que les TLD le renverra sur le serveur C qui gère `.fr.`, lequel renverra au serveur D qui gère `jussieu.fr.` et qui donnera l'adresse IP de son serveur web à savoir `134.157.250.59`.

1.2 La sécurité

Internet n'est pas sûr.

On voit que si un serveur DNS nous ment, on ira à une mauvaise adresse IP. Si on désirait consulter son compte bancaire, cela peut être très fâcheux car notre mot de passe va tomber entre de mauvaises mains. On a vu aussi qu'un message passe de réseau en réseau ce qui laisse entendre que les réseaux intermédiaires peuvent le lire voire le détourner. Mais ces failles structurelles ne sont qu'un petit morceau de possibilités d'agression sur Internet. En fait les possibilités sont immenses pour les agresseurs.

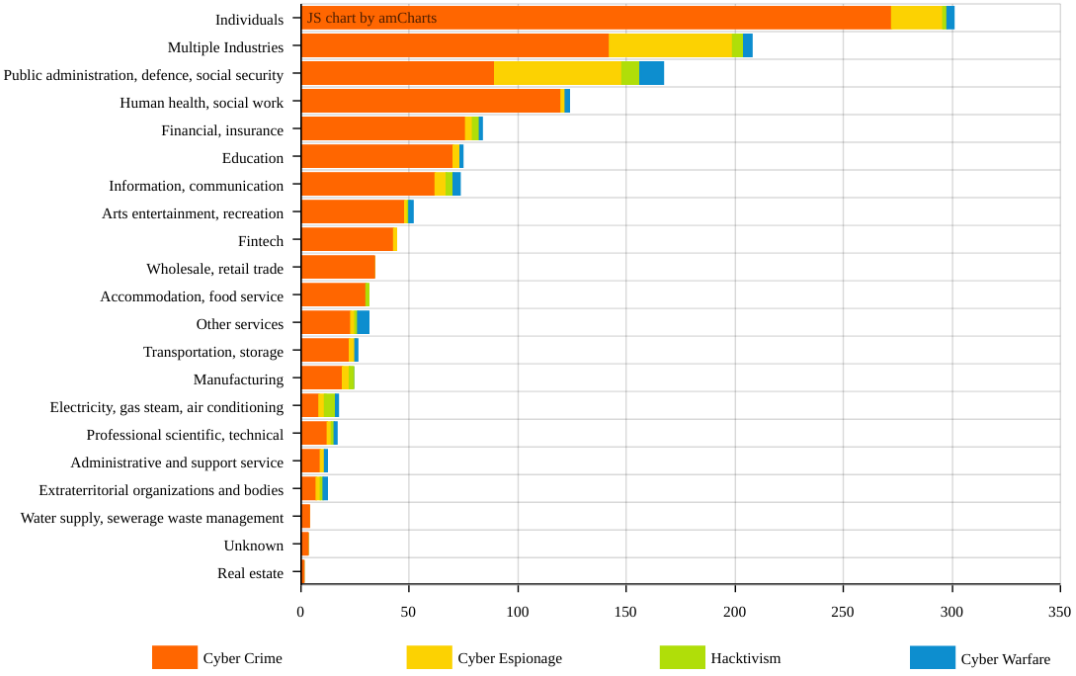


FIGURE 1.12 – Source des attaques sur Internet et leur cibles
source : Hackmageddon – 2018

À l'origine de l'Internet, club fermé, ce manque de sécurité n'était pas un problème. Mais maintenant qu'Internet est un outil économique et stratégique de première importance, il est

11. il la conservera un certain temps une fois la demande faite ce qui évite de réitérer le processus à chaque connexion.

12. ce serveur racine est tellement important qu'il est dupliqué en 13 exemplaires. Si ces 13 serveurs (plus en fait, cf la section 3.2.1) tombent tous en panne, Internet s'arrêtera doucement, le temps que les mémoires des serveurs de nom de la planète s'effacent.

naturellement devenu une cible privilégiée pour tout type d'agression, criminelle, politique, étatique... Comme de plus le risque est quasiment nul pour l'agresseur, on comprend que le cyber crime se porte bien. Si pour un individu le risque peut sembler lointain car virtuel, il est ne faut surtout pas le sous-estimer. Perdre ses économies, ses données ou son identité n'est pas une expérience agréable. La figure 1.12 montre que le cyber-crime est l'activité la plus importante dans les agressions sur Internet et que sa cible numéro 1 est les individus. Il s'agit de la population la plus fragile car peu de personnes ont des notions de sécurité informatique ou peuvent s'offrir un expert pour les protéger.

Aussi regardons les problèmes de sécurité sur Internet et comment les personnes mal intentionnées en profitent.

1.2.1 Les failles sur Internet

Pour simplifier, rangeons les sources de failles sur Internet en trois types :

— l'architecture d'Internet,
— les bugs logiciels,
— les utilisateurs (utilisateurs finaux mais aussi opérateurs du réseau).

En tant qu'utilisateur on est bien sûr responsable de nos bêtises mais on subit aussi celles des autres. Aussi il est important de prévenir et de se protéger.

Les failles architecturales d'Internet

D'un point de vue technique, Internet actuel a deux vulnérabilités fondamentales :

— les messages sont transmis sans protection sur le réseau
— l'identification de l'interlocuteur qu'il soit individu ou machine est peu fiable.

Ces failles date de la création d'Internet, ou d'IPv4, à une époque où le réseau était universitaire et sans que la sécurité soit considérée comme utile. Il était alors bien agréable de pouvoir savoir que tel collègue à l'autre bout du monde est connecté à telle machine et donc de pouvoir lui afficher une image sur son écran afin de travailler dessus ensemble. Tout cela utilisait des protocoles bloqués aujourd'hui pour des raisons de sécurité. Par exemple ce qui permettait d'afficher sur un écran distant une image permettait aussi de lire le clavier distant et donc de voir tout ce tapait le collègue, y compris ses mots de passe.

Donc Internet a été créé sans penser à la sécurité mais fort heureusement il est tout à fait possible d'ajouter une couche de sécurité. Aujourd'hui un utilisateur averti ne risque plus grand chose au quotidien à cause des protocoles mal sécurisés d'Internet. Il peut surfer en mode HTTPS, il peut chiffrer ses mails, se connecter à distance et transférer des fichiers via des canaux sécurisés.

Les communications en clair Le protocole de transport des données sur Internet, TCP/IP, ne prévoit pas de protéger les données transportées. Tous les paquets sont transmis en clair. Ainsi toute personne qui contrôle un des ordinateurs par lequel passent les données peut les lire. Par exemple lorsqu'on surfe sur le web, on utilise souvent le mode non sécurisé HTTP et non HTTPS [13], ce qui permet à notre fournisseur d'accès de voir toutes les pages qu'on regarde.

Autre exemple, au niveau d'un réseau local, à la maison, tous les paquets sortant vers Internet doivent passer par une passerelle. Le contrôle de cette machine permet la lecture de tout ce qui va et vient. Toujours sur un réseau local une personne qui est physiquement sur le même fil Ethernet qu'une autre [14] peut y détecter le courant qui y passe et donc lire les données.

Voici ce qu'un renifleur de paquets IP comme le programme `tcpdump` permet voir passer si on est sur le chemin [15] pour écouter :

```
18:12:23.988 IP (tos 0x0, ttl  64, id 24337, offset 0, flags [DF], proto:
TCP (6), length: 1019) po8.pmmh.espci.fr.3192 > mg-in-f147.google.com.www:
P 1:968(967) ack 1 win 1460 <nop,nop,timestamp 7090623 2265318920>
E...._.@.@.i..6Q..U...x.P.Yn....B....r......
.l1.....GET /search?hl=fr&q=piratage+i
```

On voit ici un paquet destiné à Google avec une demande de recherche contenant le mot "piratage".

Il est donc important de garder à l'esprit que les données ne sont pas protégées par le réseau et que le travail de protection doit être fait au niveau des applications [16] afin que les données ne quittent votre machine que chiffrées.

Ainsi depuis l'affaire Snowden et l'espionnage de plus en plus actif des États, les applications WhatsApp et Telegram ont intégré la cryptographie depuis l'émetteur jusqu'au destinataire. Cela veut aussi dire qu'avant 2014, les messages envoyés étaient lisibles par votre opérateur, l'État et tous les pirates sur le chemin.

Si l'application n'a pas de mode de chiffrement intégré, il est possible d'établir un canal sécurisé entre deux machines à l'aide d'un tunnel ou un VPN. Dans ce cas tout ce qui sort de la machine par ce canal est protégé jusqu'à l'autre machine. C'est une bonne solution pour relier son ordinateur portable à son serveur et pouvoir utiliser les réseaux wifi mis à disposition à l'hôtel ou en visite dans une entreprise sans être espionné par le propriétaire du wifi voire par toute personne connectée si le protocole du wifi est trop faible.

On regardera plus en détail les façons de se protéger dans la section sur la cryptographie.

13. C'est le serveur qui choisi le protocole. On peut voir dans l'URL si on utilise HTTPS. Les navigateurs mettent souvent un cadenas lorsqu'on est en mode sécurisé.
14. Toutes les personnes branchées sur un même *hub* sont sur le même fil Ethernet. Avec un *switch* il est plus difficile d'intercepter les communications mais cela reste possible (voir l'ARP Spoofing).
15. chemin que révèle `traceroute`
16. Cela demande à ce qu'il existe un protocole chiffré pour les applications concernées.

L'identité de l'interlocuteur Comme indiqué au début de cette section, le DNS peut mentir et donner la mauvaise adresse IP lorsqu'on lui demande `www.machin.com`. Lorsqu'on envoie un mail, là aussi le destinataire peut être différent de celui espéré. Le mail peut être intercepté en chemin. Inversement cela peut être le destinataire qui est trompé sur l'identité de l'émetteur ce qui a généré, par exemple, l'arnaque au faux virement qu'on verra.

Aussi il est important d'avoir la preuve qu'on communique avec la bonne machine ou la bonne personne et pour cela, là encore, la cryptographie apporte une solution et en particulier le système de certification [17].

Les bugs logiciels

Un bug logiciel est une erreur de programmation que le pirate peut exploiter pour obtenir un accès privilégié à une machine ou au moins pour y exécuter des commandes. Les bugs existent partout. Ils sont le plus souvent référencés car connus mais parfois ils sont nouveaux. Un bug nouveau qui permet de prendre le contrôle d'une machine à distance vaut très cher sur le marché noir.

Un exemple classique de bugs que peut utiliser un pirate consiste à donner à un programme une valeur à laquelle il ne s'attend pas.

Par exemple lorsqu'on envoie des données sur Internet, elles sont découpées en paquets. Chaque paquet a des méta-données qui décrivent le paquet dont une qui est la taille du paquet. Dans les années 90 on a découvert que si on indique que la taille du paquet est de -1 octet alors l'ordinateur qui reçoit le paquet se fige. Vous pouviez ainsi très facilement figer n'importe quel serveur sur Internet.

Un autre exemple s'appelle les injections SQL. Il s'agit d'introduire sa requête dans une base de données. De nombreux services dont des serveurs web s'appuient sur des bases de données. Cela permet par exemple de faire une requête pour avoir le prix d'un produit. En regardant comment le serveur web soumet sa requête à la base de donnée, on peut la modifier pour effectuer notre requête. Elle peut aussi bien être la destruction de la base de l'exportation d'information privée [18].

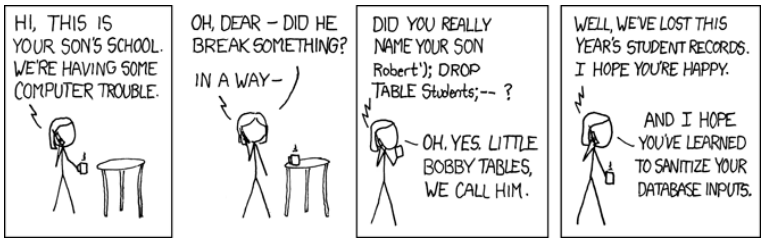


FIGURE 1.13 – Exploit [19] d'une mère
source : https://xkcd.com/327/

17. La machine produit un document signé par une autorité de certification que notre navigateur connait ce qui lui permet de vérifier que la signature est valide, cf section 1.3.3
18. il est heureusement facile de se protéger de ce type d'attaque mais il faut y penser.

Enfin regardons les débordements de mémoire. Sachant que les variables d'un programme sont contigües au code du programme dans la mémoire tampon, il est possible de donner une valeur à la variable qui, dans certains cas, va déborder de son espace alloué et modifier d'autres choses. Le plus souvent cela va casser le programme et l'arrêter mais un bon pirate pourra en profiter pour faire faire ce qu'il veut alors même que le programme tourne sur une machine distante.

Il existe bien sûr de nombreuses autres façons de profiter d'un bug ou d'une faiblesse de conception d'un programme. Pour l'instant il n'est malheureusement pas possible actuellement de garantir qu'un programme n'en contiennent pas [20].

La meilleure façon de lutter contre les bugs est de veiller à ce que sa machine soit régulièrement mise à jour pour y appliquer les correctifs.

L'erreur humaine

Quels que soient les outils de sécurité mis en place, il est difficile voire impossible de protéger un système si un utilisateur autorisé aide le pirate. Cette aide peut aller du mot de passe trop simple à l'installation sur sa machine d'un programme comprenant un logiciel malveillant (*malware*).

Une étude lors de la conférence DEFCON 2016 [21] indique que 84% des pirates utilisent les réseaux sociaux pour mener leurs attaques c.a.d. qu'ils cherchent la faille humaine. Et s'ils le font, c'est que ça marche...

Le premier type d'attaque consiste à profiter de la naïveté humaine ou simplement au manque de compréhension des bases de l'informatique. Les attaques de ce type sont innombrables et parfois très bêtes mais l'idée est qu'en l'envoyant à des millions de personnes, si 1% se fait avoir c'est gagné. Dans ce domaine deux types d'attaques ont fait leurs preuves : l'arnaque et l'hameçonnage ou filoutage (*phishing* en anglais). Le FBI a évalué le coût de ces attaques à plus de 10 milliards de dollars entre 2013 et 2018.

La seconde faille humaine consiste à pousser l'utilisateur à installer un programme malveillant sur sa machine. Cela peut être fait en mettant en libre téléchargement un logiciel merveilleux qui comprend le *malware* ou en l'incluant dans une pièce attachée à un mail.

Une troisième faille humaine est l'erreur de ceux qui sont au contrôle. Si un administrateur d'un système informatique configure mal un logiciel ou un appareil alors des pirates pourront en profiter. Ainsi des numéros de cartes bleues de clients de Tati étaient disponibles sur le web et référencés par Google simplement parce que Tati n'avait pas configuré correctement son serveur web [22].

19. L'exploitation d'un bug s'appelle un exploit.
20. C'est possible sur des tout petit programme comme celui qui contrôle une machine à café, mais pas sur les programmes usuels.
21. https://www.esecurityplanet.com/hackers/fully-84-percent-of-hackers-leverage-social-engineering-in-attacks.html
22. cf affaire Tati versus Kitetoa, http://www.kitetoa.com/Pages/Textes/Les_Dossiers/Tati_versus_Kitetoa/historique.shtml

Mais la liste des erreurs possibles n'est malheureusement pas fermée, l'imagination étant sa limite. En 2018 la Nasa s'est fait piratée car un employé a mis sur le réseau interne un petit ordinateur mal protégé qui a servi de cheval de Troie.

Les failles qui n'en sont pas

Un ordinateur, un composant du réseau peut tomber en panne. La justice peut demander l'accès à un ordinateur et à son contenu. On peut perdre son ordiphone. Un cambrioleur peut voler un ordinateur portable. Il existe bien des façons de perdre le contrôle ou l'accès à ses données, d'avoir un serveur coupé de l'Internet sans pour autant que l'on puisse parler de cyber-attaque. C'est évident lorsqu'on le dit mais c'est souvent une problématique sous-estimée.

Pour lutter contre ces désagréments aux conséquences vraiment graves parfois, il existe des stratégies qui ont fait leurs preuves :

— faire des sauvegardes dans des lieux différents [23],
— chiffrer ses données (voire tout le disque dur),
— installer un mouchard qui permet de reprendre le contrôle de sa machine, de son ordiphone, à distance,
— comprendre où sont stockées les données et comment elles sont stockées, voir l'encart FBI/CIA.

Enfin dans la liste des failles qui n'en sont pas mais qui pourraient en être, il y a les programmes écrits en JavaScript qui s'exécutent en arrière plan lorsque vous regardez une page web. Ils ne vont que consommer de l'énergie, par exemple pour miner des bitcoins à leur bénéfice, mais cela peut mettre un ordiphone à genoux rapidement. Notons que souvent le site web qui vous envoie le programme JavaScript ne le fait pas volontairement, il a été lui même piraté.

Le FBI lit les mails des maitresses du patron de la CIA

Même chez les espions on ne comprend pas toujours très bien que le mail n'est pas protégé s'il est hébergé par un fournisseur de service. L'affaire Petraeus (2012) en a été la preuve.

Paula, la maîtresse cachée du chef de la CIA, David Petraeus, est jalouse de Jill, une copine de ce dernier. Elle lui envoie donc des mails malveillants mais en se protégeant (faux compte Gmail, mails envoyés que depuis des lieux publics et hôtels avec wifi gratuit). Jill porte plainte contre X.

Le FBI récupère auprès de Google les adresses IP des machines qui ont envoyé les mails puis en regardant les registres des hôtels, il s'avère qu'une seule personne était dans ces différents hôtels à ces différents moments : la maîtresse secrète. Une fois Paula identifiée, le FBI obtient de Google l'accès à son compte Gmail officiel. Il y découvre la correspondance avec le chef de la CIA. Le FBI en profite pour regarder aussi le compte Gmail de Jill et découvre une relation avec un général.

Résultat, le patron de la CIA démissionne et le général perd le poste de chef de l'OTAN qui lui tendait les bras.

23. cela protège aussi du chantage aux données chiffrées (*ransomware*)

1.2.2 Les cyber-attaques

Maintenant que l'on a fait le tour des principales failles, regardons comment elles sont exploitées. La figure 1.14 présente la liste des cyber-attaques les plus utilisées en 2017 et 2018.

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	➲	1. Malware	➲	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	➲	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	➲	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	➲	9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	➲	10. Physical manipulation/ damage/ theft/loss	➲	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

Legend: Trends: ↓ Declining, ➲ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

FIGURE 1.14 – Évolution des agressions sur Internet
source : ENISA Threat Landscape Report 2018

On peut ranger ces agressions en fonction du type de faille :

Malware 🐞	Phishing 😐	Denial of Service 🌐
Web Based Attack 🐞	Insider Threat 😐	Spam 🌐
Web Application Attacks 🐞	Information Leakage 😐	
Data Breaches 🐞	Physical manipulation... 😐	
Cryptojacking 🐞		Botnets 🌐 🐞
Ransomware 🐞	Identity Theft 😐 🐞	Cyber Espionage 🌐 😐 🐞

TABLE 1.2 – Classement des agressions par type de faille
🐞 : Bug 😐 : Utilisateur 🌐 : Architecture d'Internet

m.à.j. sur http://www.ricou.eu.org/e-politique.html

Les États-Unis ont estimés le coût de ces attaques sur leur territoire entre 57 et 109 milliards de dollars en 2016. La marge d'erreur est liée à la difficulté d'estimer un coût comme une perte de réputation. La figure 1.15 présente les différents types de coûts avec leur incertitude et importance.

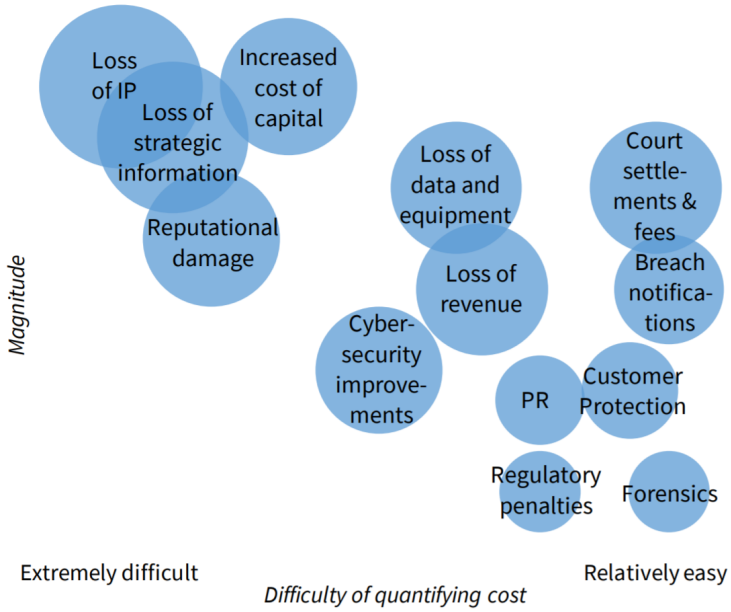


FIGURE 1.15 – Coûts possibles suites à une cyber-attaque
source : The Cost of Malicious Cyber Activity to the U.S. Economy – 2018

Regardons quelques unes des attaques les plus usuelles.

Les logiciels malveillants (*malwares*)

De nombreux programmes, programmes craqués, greffons et autres extensions sont librement téléchargeables et très attractifs mais malheureusement ils contiennent parfois des virus, cheval de Troie ou autre méchanceté qui agira seul ou permettra au pirate d'agir à distance sur la machine infectée, ordinateur ou ordiphone. La machine infectée peut aussi devenir un *zombie* que le pirate utilisera pour attaquer ailleurs ou envoyer du spam.

Lorsque le *malware* est inclus dans une pièces attachées on parle encore de *phishing*. Un exemple simple consiste à envoyer un fichier Excel ou Word en se faisant passer pour un collègue. Le simple fait d'ouvrir la pièce attachée peut suffire à infecter sa machine.

Parmi les plus célèbres de ces malwares citons :

— NotPetya le destructeur conçu pour affaiblir l'Ukraine. Ses dégâts ont été évalué à 10 G$. Si l'Ukraine a subit la majorité des dégats, d'autres ont aussi été touchés comme l'entreprise de transport danoise Maersk qui a déclaré 300 M€ de pertes ou Saint-Gobain en France qui a évalué ses dégats à 80 M€.

— ILOVEYOU qui a touché des dizaines de millions de machines sous Windows en se propageant par le mail. Son coût a été estimé entre 5 et 9 G$ de dommages et 15 G$ de correctifs pour s'en protéger.
— MyDoom qui, comme ILOVEYOU, s'est propagé par le mail sur les machines Windows. En 2004 entre 16 et 25% des mails étaient infectés par ce virus. Le but de ce virus semble avoir été de créer des zombies pour relayer du spam. Son coût global a été estimé à 38 G$,
— Stuxnet un virus israélo-américain conçu pour détruire du matériel du programme nucléaire iranien (cf chapitre sur la cyber-guerre).

Pour ce protéger de ces logiciels malveillants il faut développer une bonne hygiène informatique.

La première règle est de maintenir sa machine à jour en installant toutes les mises à jour au fur et à mesure qu'elles sortent. Même si ainsi la sécurité n'est pas totale, elle est souvent suffisante, les pirates allant vers les proies les plus faciles à savoir les machines pas à jour. Bien sûr lorsqu'un virus utilise une faille inconnue, tout le monde est nu jusqu'à l'arrivée du correctif.

La seconde règle consiste à faire attention aux logiciels qu'on installe et à supprimer ceux qu'on n'utilise plus. Ceci est particulièrement vrai sur les ordiphones. Ainsi il n'est pas normal qu'une application de type minuteur demande le droit d'accéder au carnet d'adresse, aux paramètres du réseau ou je ne sais quoi. Une telle application n'a besoin d'aucun droit spécifique. Si elle en demande il y a danger. Le danger ne peut être que commercial et toucher la vie privée de l'utilisateur mais il peut aussi être bien plus grave.

Il est aussi possible d'utiliser un système d'exploitation et des logiciels qui n'intéressent pas les cyber-criminels car trop peu utilisés. Ainsi un système comme Linux ou FreeBSD est bien moins attaqué que Windows ou MacOS. Pour de nombreux experts Linux et FreeBSD sont aussi intrinsèquement plus sûr car ouverts ce qui permet un audit permanent et une correction plus rapide des failles. L'agence de la sécurité française, l'ANSSI va dans ce sens et propose un système d'exploitation très sécurisé basé sur Linux : Clip OS.

Les demandes de rançon (*ransomware*)

Certain virus chiffrent tous les fichiers de la machine infectées et demande ensuite au propriétaire de payer une rançon pour que ses données soient déchiffrées.

L'un des plus connus, WannaCry, a touché plus de 300 000 ordinateurs en 2017. Il a utilisé la faille de sécurité de Windows en s'appuyant sur l'exploit EternalBlue développée par la NSA [24] pour son usage personnel mais qui a fuité ! Notons qu'il n'a touché que les machines pas à jour ou les vieux systèmes d'exploitation, comme Windows XP, que Microsoft ne maintenait plus. Des hôpitaux, des ministères, des villes, des entreprises ont été affectés par WannaCry.

Le principe de chiffrer les données pour demander une rançon ne nécessite pas obligatoirement l'utilisation d'un virus mais c'est quand même bien pratique.

24. L'agence de sécurité informatique américaine, cf chapitre sur la démocratie

Les attaques web

L'importance du Web est telle que pour certains Internet est le Web. Cela implique que toute organisation a un site web qui va d'une simple présentation à un site marchand qui est le cœur de l'entreprise. Aussi pouvoir pénétrer un serveur web intéresse de nombreuses personnes. Des activistes cassent des sites web d'ennemis ou les détournent pour y afficher leur message. Les Anonymous sont coutumiers du fait, ISIS a fait de même contre TV5Monde via des hackers russes a priori. Parfois ce sont des États qui vont bloquer des sites [25]. Le plus souvent ce sont des cyber-criminels qui attaquent pour faire payer les organisations victimes.

Les injections sont la méthode la plus utilisée pour casser un serveur web.

Vol de données (*data-breach*)

Nous laissons nos données partout, dans les banques, les hôtels, les transports, les réseaux sociaux, les sites spécialisés... et ces données ont de la valeur. Elles permettent d'utiliser une identité pour créer de faux vrais papiers, elles permettent aussi d'agir sur Internet en notre nom, elles permettent parfois d'accéder à des comptes bancaires pour se servir, de connaitre notre historique, nos relations pour faire du chantage...

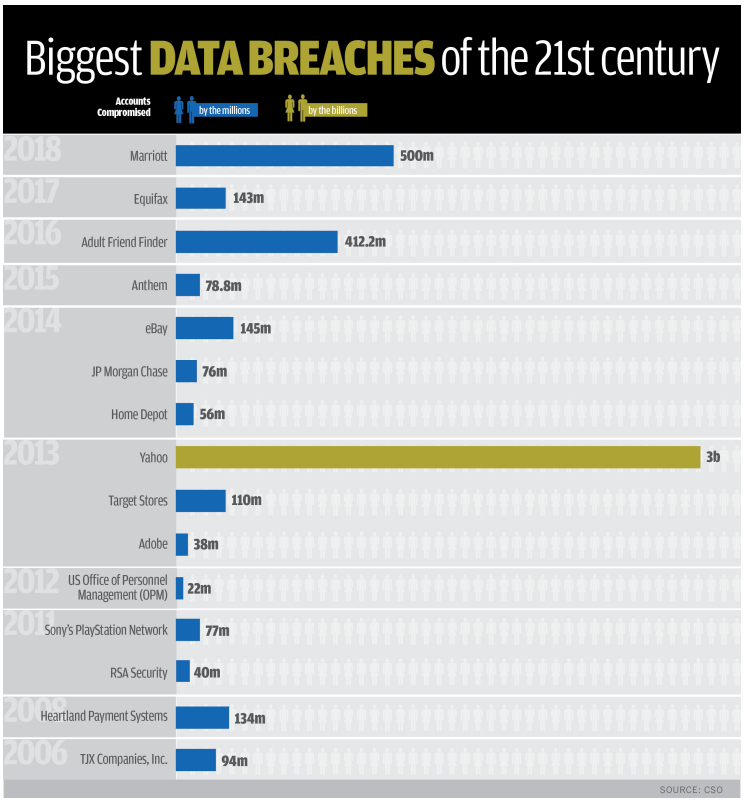


FIGURE 1.16 – Nombres connus de données volés entre 2006 et 2018

25. La Russie l'a fait en Estonie et en Géorgie.

La liste des vols les plus importants, figure 1.16, ne doit pas faire oublier les moins connus nettement plus nombreux.

Le premier de la liste concerne les hôtels Marriott. D'après la dernière annonce en 2019, 383 millions d'identité ont été volées avec 25 millions de numéros de passeport (dont 80% était chiffrés), 9 millions de carte de crédit chiffrées mais 385 000 cartes de crédit pas chiffrées. Ces chiffres sont à prendre avec précaution car l'intrusion dans le système informatique de Marriott date de 2014. Aussi pendant plus de 4 ans les pirates voyaient tout.

Le dénis de service

Il s'agit d'une attaque spéciale puisqu'elle ne nécessite pas de casser la sécurité d'un autre. Il s'agit simplement de faire une tentative de connexion à une autre machine et de la répéter. Cela peut être charger une page web et la recharger toutes les secondes. Bien sûr si seulement une personne fait cela, cela n'a aucun impact sur la machine visée, mais si des millions voire des milliards de requêtes ont lieu en même temps [26], la machine visée passe en surcharge et ne peut plus répondre. Elle devient inaccessible, coupée de l'Internet, ce qui est le but.

On comprend que le succès dépend du le nombre d'attaques simultanés. Aussi pour mettre toutes leurs chances de leur coté, les attaquants utilisent des machines zombies dont ils ont pris le contrôle par le passé (via des virus par exemple) afin d'avoir une force de frappe conséquente.

En 2016 des jeunes joueurs de Minecraft ont piratés des caméras IP et d'autres objets de l'Internet pour lancer des dénis de service distribués contre des serveurs Minecraft concurrents (attaque nomée Mirai). Le piratage a été très simple puisqu'ils ont simplement utilisé les login et mot de passe par défaut de ces objets de l'Internet [27]. Ainsi ils ont pu lancer des attaques d'1 Tbits/s contre le réseau d'OVH qui hébergeait des serveurs Minecraft concurents ainsi que sur d'autres réseaux. L'importance de l'attaque, nettement plus forte que le pic de l'attaque de 2007 contre l'Estonie [28], a laissé penser à une attaque étatique initialement.

Le filoutage (*Phishing*)

Le filoutage ou phishing consiste à récupérer des informations personnelles que l'attaquant pourra exploiter ensuite. Il peut s'agir d'un login/mot de passe, d'un numéro de carte bleue ou même des données a priori moins sensibles qui permettront une usurpation d'identité. Le processus consiste le plus souvent à envoyer un mail alarmant demandant au destinataire de suivre un lien pour se protéger. Cela peut être votre soi-disant banque qui vous demande de changer votre mot de passe mais le lien envoie sur une copie du site de la banque. En 2019, le directeur exécutif du groupe Orange a estimé qu'environ deux millions de français sont victimes chaque année du phishing.

26. on parle alors de DDOS pour Distributed Deny of Service
27. Comme quoi ne pas changer un mot de passe par défaut peut rendre complice d'une cyber-attaque...
28. cf chapitre sur la cyber-guerre

L'exemple qui suit demande aux propriétaires d'un nom de domaine chez Enom de se connecter sur leur compte pour valider les informations les concernant sous peine de perdre leur nom de domaine.

```
Date: Sat, 1 Nov 2008 10:56:39 +0100
From: eNomCentral Team <support@enom.com>
To: olivier@ricou.eu.org
Subject: Inaccurate whois information.

Dear user,

On Sat, 1 Nov 2008 10:56:39 +0100 we received a third party complaint of
invalid domain contact information in the Whois database for this domain.
Whenever we receive a complaint, we are required by ICANN regulations to
initiate an investigation as to whether the contact data displaying in the
Whois database is valid data or not. If we find that there is invalid or
missing data, we contact both the registrant and the account holder and
inform them to update the information.

...
PLEASE VERIFY YOUR CONTACT INFORMATION - http://www.enom.com.ssl48.mobi
LINK TO CHANGE INFORMATION - http://www.enom.com.ssl42.mobi

Thank you,
Domain Services
```

Bien sûr, le lien donné est un faux qui ne renvoit pas chez Enom, `www.enom.com`, mais sur `www.enom.com.ssl48.mobi`, site qui appartient à celui qui contrôle `ss148.info`. Si l'on suit ce faux lien, on tombe sur une page identique d'aspect à la page d'authentification du site d'Enom et si l'on entre son login/mot de passe, on s'est fait avoir. Ainsi le pirate récupère le contrôle du nom de domaine ce qui lui permet d'intercepter de l'information et rediriger des requêtes. S'il le fait discrètement, le propriétaire du domaine ne s'en rendra pas compte.

Lorsqu'on craint d'être la victime d'une telle attaque, il est conseillé de contacter directement et par la voie usuelle l'entreprise concernée. Ainsi, dans notre cas, en allant sur la page d'accueil d'Enom, la véritable : `www.enom.com`, on sait immédiatement à quoi s'en tenir, le message suivant confirmant l'arnaque :

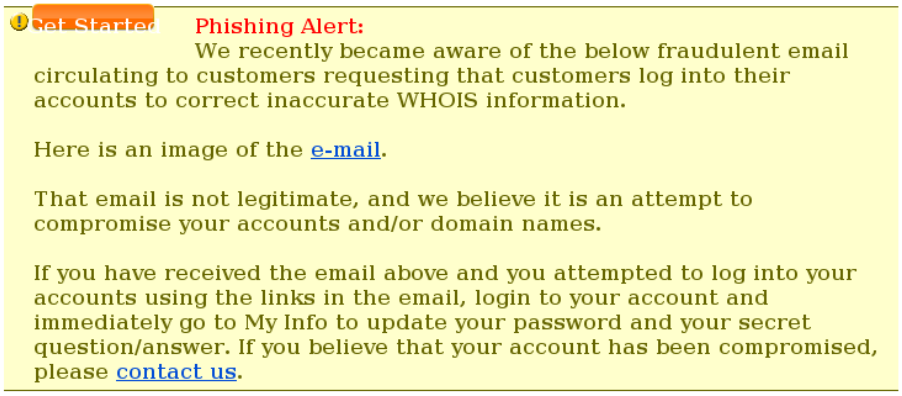


FIGURE 1.17 – Message d'avertissement d'Enom contre une arnaque

La règle numéro 1 pour se protéger du filoutage est de ne jamais cliquer sur un lien compris dans un mail. Si on veut quand même cliquer, c'est de vérifier précautionneusement l'URL de la page web une fois qu'on a cliqué.

L'arnaque

Si cette attaque n'est pas dans la liste elle n'en est pas moins un type d'attaque très utilisé. Il s'agit de convaincre la victime de verser de l'argent à l'arnaqueur.

L'arnaque nigériane a été et reste un grand classique. Elle consiste le plus souvent à demander de l'aide pour sortir des sommes considérables de son pays en échange d'un pourcentage conséquent. Pour cela il va falloir ouvrir un compte bancaire au Nigéria, y déposer une somme minimale puis d'autres excuses permettront de demander d'autres sommes supplémentaires. Les quelques personnes arnaquées qui ont été sur place pour réclamer leurs biens ont souvent fini à la morgue. Notons que parfois c'est le gros lot pour l'arnaqueur puisque le FBI avait arrêté la comptable d'un cabinet d'avocats américains qui avait versé plus d'un millions à ses arnaqueurs.

Mais les arnaques ne se font pas que par mail. De nombreuses personnes ont perdu des sommes importantes en pensant avoir rencontré l'amour de leur vie sur des sites de rencontre puis en les aidant financièrement à sortir d'une mauvaise passe pour les rejoindre. Ce type d'arnaque effectué le plus souvent par des étrangers (c'est moins dangereux) s'est sophistiqué avec temps et aujourd'hui l'arnacœur dira vivre dans une ville française dont il sait tout grâce à Internet. Mais il aura toujours des problèmes qui coûtent bien cher.

Les réseaux sociaux sont aussi des endroits parfait pour les arnaqueurs. Enfin d'autres types d'arnaques existent, cf figure 1.18.

Les particuliers ne sont pas les seules victimes des arnaqueurs. Les entreprises subissent depuis quelques années l'arnaque au faux virement. Elle consiste à envoyer un faux mail au nom du patron avec une demande de virement urgente pour conclure une affaire. Bien sûr de nombreux comptables ont fait le virement sans vérifier l'authenticité de l'émetteur du message.

Investment	$8,648	Fake Invoice	$441
Romance	$6,003	Credit Repair/Debt Relief	$388
Moving	$3,993	Online Purchase	$365
Cryptocurrency*	$3,147	Fake Check/Money Order	$341
Home Improvement	$2,895	Tech Support	$255
Nigerian/Foreign Money Exchange	$2,133	Credit Card	$231
Business Email Compromise	$1,717	Government Grant	$218
Family/Friend Emergency	$1,219	Health Care/Medicaid/Medicare	$170
Counterfeit Product	$1,210	Scholarship	$155
Travel/Vacation	$887	Utility	$106
Advance Fee Loan	$716	Debt Collection	$98
Charity	$708	Yellow Pages/Directory	$91
Identity Theft	$683	Phishing	$44
Rental	$662	Tax Collection	$31
Employment	$598		
Sweepstakes/Lottery/Prize	$547	Other	$746

*Denotes a category first tracked in 2018

FIGURE 1.18 – Somme perdue en moyenne par type d'arnaque
source : BBB Scam Tracker – 2015-2018

Notons que souvent l'affaire est bien préparée avec une bonne connaissance de l'entreprise de la part des arnaqueurs, et pour cause, les sommes en jeu sont nettement plus importantes. Le préjudice a été estimé à 485 M€ entre 2010 et 2018 pour les entreprises françaises et 2.3 G$ pour les États-Unis [29].

Pour éviter les arnaques il faut prendre le temps de la réflexion (la moindre chose bizarre dans le message est un indice d'arnaque possible), en parler à des proches et regarder des sites qui référencent les arnaques comme https://info.signal-arnaques.com/.

1.3 La cryptographie

La cryptographie protège les communications dès lors que votre machine n'est pas infectée, que votre logiciel n'a pas de bug, que vous ne donnez pas vos clés ou mot de passe au pirate...

29. https://www.lesechos.fr/idees-debats/cercle/les-arnaques-au-virement-concernent-toutes-les-entreprises-130970

Elle permet

— de chiffrer les données,
— d'en garantir l'intégrité,
— de signer le message.

Le premier point implique

— la confidentialité des communications (transactions bancaires, connexions à distance, téléphone, mail...),
— la protection de données informatique stockées (secrets militaires, industriels, commerciaux, médicaux, personnels...)

Le second point, la garantie de l'intégrité, offre la certitude qu'un document est complet (contrat, mail, logiciel...) et que personne n'a pu le modifier.

Enfin le dernier point, la signature, permet

— de savoir avec certitude qui est l'origine d'un document item et inversement de prouver qu'on est l'auteur du document
— la non-répudiation,
— de protéger des systèmes informatiques contre les intrusions en vérifiant l'identité des machines et utilisateurs,
— de vérifier l'authenticité d'un site Web

Avec la combinaison des trois, on peut envoyer un mail en étant certain que personne d'autre que mon destinataire ne pourra le lire (chiffrage). Le destinataire aura la certitude que mail vient bien de l'émetteur grâce à la signature et qu'il n'a pas été modifié (intégrité). Ainsi l'émetteur ne pourra pas contester le fait d'avoir écrit le message (non-répudiation).

Avant de regarder l'utilisation de la cryptographie pour se protéger sur Internet, essayons de comprendre les principes de la cryptographie.

1.3.1 La théorie

Les clés symétriques ou secrètes

La façon la plus simple de chiffrer un message est de lui appliquer une fonction mathématique. Ainsi Jules César chiffrait ses messages en décalant les lettres de N, ainsi avec N=3, le A devient D. Pour le déchiffrer il suffit d'appliquer la fonction inverse avec la même clé. Bien sûr un bon système de cryptographie propose une fonction inverse assez compliqué pour qu'on ne puisse pas deviner le message sans la clé (N dans le cas de Jules César). Ce système est celui de la clé symétrique.

ATTAQUEZ GERGOVIE	DWWDTXHC JHUJRYLH
↓ +3	↓ -3
DWWDTXHC JHUJRYLH	ATTAQUEZ GERGOVIE

FIGURE 1.19 – Un message secret de Jules César

Pour communiquer entre 2 ou 3 personnes il suffit d'avoir une clé commune pour pouvoir communiquer de façon protégée par la suite. Bien sûr plus il y a de personnes qui partagent la clé, plus les risque de fuite sont importants. Pour éviter cela, on peut choisir de créer une clé par paire de personnes, soit $N^2/2$ clés pour un groupe de N personnes ce qui est rapidement ingérable.

Aussi pour un grand groupe on peut préférer le système dit de tiers de confiance, TDC, (Trusted Third Party en anglais, ou TTP) qui propose de définir une seule clé K_i pour chaque utilisateur qui lui permet de communiquer avec le tiers de confiance.

Lorsque deux personnes, i et j, veulent communiquer, le TDC génère une clé de session k qu'il transmet chiffrée à i avec la clé K_i et à j avec la clé K_j. Puis les utilisateurs utilisent la clé de session k pour communiquer, cf figure 1.20.

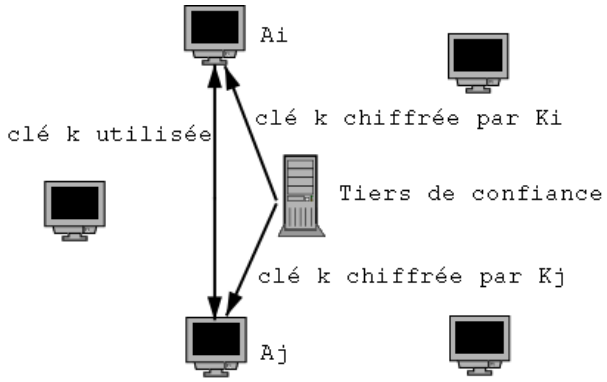


FIGURE 1.20 – Tiers de confiance pour chiffrement symétrique

Ce système de clés symétriques a les avantages suivants :

— il est facile d'ajouter un nouvel entrant dans le réseau,
— chaque individu ne stocke que sa clé de communication avec le TDC,
— le chiffrement et déchiffrement sont rapides.

Les inconvénients sont :

— le besoin du TDC pour initier toute communication,
— le TDC peut lire tous les messages.

On comprend que la présence du tiers de confiance peut être jugée problématique.

Les clés asymétriques ou publiques

Le système de cryptographie par clé symétrique a été le seul disponible jusqu'après la seconde guerre mondiale, ce qui veut dire que durant la seconde guerre mondiale les clés utilisées devaient être transmises physiquement à travers les théâtres d'opération avec tous les risques d'interception possibles lorsqu'on doit traverser les lignes ennemies. Lorsqu'on veut renouveler les clés régulièrement au cas où l'ennemi aurait réussi à les avoir, on en veut à la technologie qui impose cet exercice délicat.

La clé asymétrique corrige ce défaut en permettant de transmettre une clé publiquement pour chiffrer tout en gardant une clé privée pour déchiffrer. Les messages qu'on reçoit et que tout le monde peut intercepter, sont chiffrés avec la clé diffusée publiquement mais seule la clé privée peut les déchiffrer.

En pratique un utilisateur génère sa clé privée d_i et publique e_i puis diffuse cette dernière ce qui permet à quiconque de lui envoyer un message sans risque d'interception. On peut imaginer un répertoire public où chacun dépose sa clé publique. Ainsi le message m est chiffré par la fonction E qui utilise la clé publique du destinataire, puis déchiffré par la fonction D à l'aide de la clé privée du destinataire, cf figure 1.21.

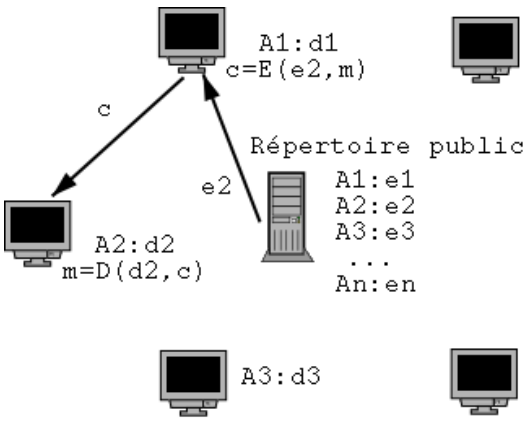


FIGURE 1.21 – Utilisation de clés asymétriques

Les avantages de la méthode sont

— l'absence d'intermédiaire, pas de TDC,
— le fichier des clés publiques peut être largement diffusé.

Les inconvénients sont :

— un pirate peut diffuser une fausse clé publique (cf ci-dessous),
— le chiffrement est plus lent qu'avec une clé symétrique.

L'attaque de l'homme au milieu L'attaque la plus simple contre ce système est de substituer la clé publique d'un utilisateur par celle du pirate et d'intercepter tous les messages. Une

fois le message intercepté, le pirate, l'homme au milieu, le déchiffre, le note, puis le chiffre avec la véritable clé publique du destinataire pour lui envoyer afin qu'il ne détecte pas l'interception.

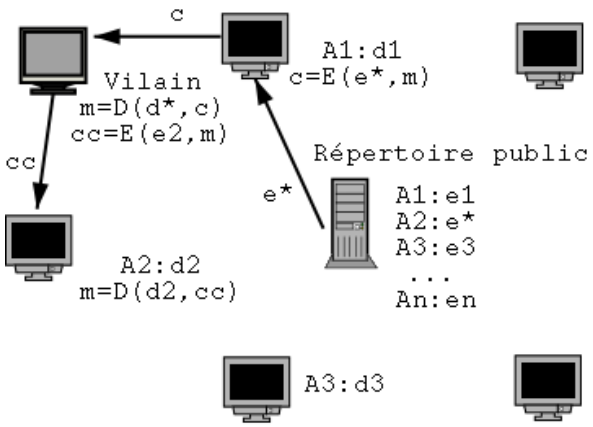


FIGURE 1.22 – Attaque de l'homme au milieu

La parade, pour ne pas voir son message intercepté, réside dans la fiabilité de la clé publique de son destinataire. Une clé publique est sûre, soit parce que le destinataire vous l'a remise en main propre, soit parce qu'une personne en qui vous avez entièrement confiance vous garantit cette clé publique. Cette personne de confiance peut être une autorité de certification (cf section 1.3.3) ou une personne dont vous êtes sûr car elle est dans votre liste des personnes de confiance. Dans ce dernier cas on parle de toile de confiance ou *Web of trust* [30].

Différents algorithmes de cryptographie

Sans remonter jusqu'à Jules César, il existe de nombreux algorithmes de cryptographie. Certain sont plus connus que d'autres et leur célébrité est la garantie de leur fiabilité. En effet il est difficile de créer un algorithme de cryptographie solide et seule sa vérification par le plus grand nombre possible de mathématiciens et d'utilisateurs peut offrir une garantie de sécurité.

La cryptographie symétrique : DES, Triple DES, RC, AES et ChaCha20 Historiquement DES, Data Encryption Standard, est le premier standard officiel des États-Unis à destination des entreprises. Il s'agit d'un algorithme de chiffrement à clé symétrique développé par IBM dans les années 70. DES utilise une clé de 56 bits qui, de nos jours, est bien trop faible pour résister aux attaques. Aussi DES ne doit plus être utilisé.

Son premier remplaçant a été Triple DES qui n'est que l'application de DES trois fois avec des clés différentes. Cela permet en effet d'amener la sécurité à un niveau correct mais pour un coût élevé en temps de calcul.

30. cf https://fr.wikipedia.org/wiki/Toile_de_confiance

Au MIT, Ronald Rivest a conçu de nombreux algorithmes de chiffrements symétriques dit à la volée ("stream cipher" – RC4) et par bloc ("block cipher" – RC2 / RC5 / RC6). Parmis ces algorithmes, RC4 a eu un véritable succès, mais aujourd'hui RC4 est obsolète et ne doit plus être utilisé, des attaques ont été trouvées pour le casser.

Aussi à la fin des années 90, le gouvernement américain à lancé un concours pour trouver le remplaçant idéal, sûr et peu gourmand en CPU afin de pouvoir l'exécuter sur le processeur d'une carte à puce. En 2001 le vainqueur a été déclaré, l'algorithme symétrique Rijndael [31] a été choisi pour être l'Advanced Encryption Standard (AES).

Enfin en 2008, ChaCha20 propose un algorithme performant et sécurisé pour les environnements mobiles.

La cryptographie asymétrique : RSA, DSA et les ECC L'heure de gloire [32] pour Rivest, Shamir est Alderman est arrivée avec RSA [33]. Cet algorithme conçut en 1977 est le premier algorithme à clé publique/clé privée (ou asymétrique) publié (l'armée anglaise avait trouvé quelques années auparavant un algorithme asymétrique mais bien sûr, elle s'était bien gardée de l'annoncer). Il est toujours très utilisé. Son principe mathématique est expliqué dans l'encart page 48.

Mais RSA sera périmé avec l'arrivée des ordinateurs quantiques pour lesquels la décomposition en nombre premier est simple. Aussi une nouvelle famille de cryptographique asymétrique basée sur les courbes elliptiques (*Elliptic Curve Cryptography* ou ECC en anglais.) a été créée pour y résister.

Une alternative à RSA pour la signature est DSA (Digital Signature Algorithm) qui repose sur la difficulté a résoudre le problème de l'algorithme discret. Mais là encore les ordinateurs quantiques changent la donne car ils peuvent aussi résoudre ce problème simplement. Aussi il existe des versions basées sur les courbes elliptique : ECDSA et EdDSA utilisés pour les signatures dans des environnements comme SSL/TLS.

Les condensats ou empreintes de hachage : MD5, SHA-1, SHA-3 Un condensat (*hash* en anglais) permet de garantir l'intégrité d'un document. Il s'agit du résultat d'une fonction à sens unique, dite de hachage, qui résume un document en une ligne. Cette fonction est telle que si l'on modifie quoi que ce soit dans le document, alors le condensat devient totalement différent.

```
md5("Le condensat garantit l'intégrité") = 9fb6e5c02fd664892271ca02e0266457
md5("Le condensat garantit l'intégrite") = d80c680cf92d64cb7830c86fbb2350f7
```

Seul le é final a changé mais le condensat est totalement différent.

FIGURE 1.23 – Utilisation d'un condensat

31. cf la BD qui présente Rijndael, http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html
32. Prix Turing 2002, le Nobel des informaticiens
33. Les initiales de ses inventeurs

Les mathématiques de RSA

L'algorithme RSA est un algorithme de chiffrement asymétrique.

L'idée d'un algorithme asymétrique a été proposée par Whitfield Diffie et Martin Hellman dans un article en 1975 et mise en pratique en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman. James Ellis et Clifford Cocks des services de communication de l'armée anglaise, avaient trouvé cet algorithme quelques années plus tôt mais ne purent le dévoiler pour cause de secret militaire (cf l'histoire présentée par Ellis).

Son principe est relativement simple mais totalement révolutionnaire. On n'imaginait pas jusque là qu'il puisse être possible de décoder un message sans avoir la clé ayant permis de l'encoder.

Pour cela chaque utilisateur a

- une clé publique (e, n)
- une clé privée (d, n)

avec les nombre e, d et n construits ainsi :

		Exemple
1	Choisir 2 nombres premiers distincts p et q. Plus ils sont grands et meilleure sera la sécurité.	Prenons $p = 11$ et $q = 19$.
2	Soit $n = p\,q$.	$n = 11 \times 19 = 209$
3	Choisir un nombre d premier avec $(p-1)\,(q-1)$.	Dans notre cas $(p-1)\,(q-1) = 180 = 2^2 \times 3^2 \times 5$ donc $d = 7$ marche.
4	Choisir e tel que $(e\,d)\,\%\,((p-1)(q-1)) = 1$.	$e = 103$ vérifie $7e\,\%\,180 = 1$ puique $7 \times 103 = 721 = 4 \times 180 + 1$.

Ces choix impliquent que $e\,d\ \%\,J(n) = 1$ où $J(n)$ est l'indicatrice d'Euler sachant que $J(n) = (p-1)(q-1)$ lorsque p et q sont premiers. C'est la propriété magique qui permet à RSA de fonctionner.

Chiffrer un message On chiffre le message M à l'aide de la clé publique (e, n) du destinataire ainsi (tout n'est que 0 et 1 sur un ordinateur donc tout message est un nombre) :

	Exemple avec $M = 123$
$M' = M^e\,\%\,n$	$M' = 123^{103}\,\%\,209 = 63$

Message chiffré qu'il peut déchiffrer avec sa clé privée (d, n) car

$M'^d\,\%\,n = (M^e\,\%\,n)^d\,\%\,n$ $= M^{ed}\,\%\,n = M^{ed\,\%\,J(n)} = M$	$M'^d\,\%\,n = 63^7\,\%\,209 = 123 = M$

Prouver son identité L'émetteur chiffre le condensat $C(M)$ d'un message M avec sa clé privée (d, n) et l'envoie avec le message :

$$C' = C(M)^d\,\%\,n$$

Pour être certain que le message vient bien de l'émetteur il suffit de comparer $C(M)$ et $C'^e\,\%\,n$ avec (e, n) la clé publique de l'émetteur. S'ils sont égaux c'est bon.

Casser RSA Si on peut décomposer n en p et q alors trouver d est simple sachant que l'on connait e. Heureusement décomposer un très grand nombre en nombres premiers est une opération très lourde qui peut prendre des siècles pour un n de bonne taille (sauf pour les futurs ordinateurs quantiques).

Les condensats MD5 et SHA-1 ayant été cassés, ce qui rend possible la génération d'un autre document qui produit le même condensat, seule la famille des SHA-2 restait sûre avec en particulier SHA-256. Aussi le concours SHA-3, a été lancé pour définir une nouvelle fonction de hachage plus sûre et rapide.

En 2012 l'algorithme Keccak a été choisi pour être le SHA-3. Il est donc la nouvelle norme du NIST. Notons que l'un des auteurs de Kaccak, Joan Daemen, est aussi l'auteur de Rijndael qui a été retenu par le NIST pour être l'AES.

1.3.2 Utilisation de la cryptographie

Protéger son courrier avec GPG

Comme on l'a vu, le courrier est particulièrement vulnérable et la seule façon de le protéger nécessite l'usage de la cryptographie. Actuellement il existe deux principaux logiciels pour chiffrer les mails : GPG, GNU Privacy Guard, et S/Mime. Tous les deux utilisent différents algorithmes de cryptographie pour remplir toutes les conditions nécessaires à la protection du courrier :

— un algorithme de chiffrement symétrique de type AES pour chiffrer la session,
— un algorithme de chiffrement asymétrique de type RSA ou un ECC avec la courbe elliptique par défaut (mieux) pour chiffrer la clé de session et signer,
— un condensat comme SHA-256 ou SHA-3 pour vérifier l'intégrité.

Pour des raisons de performance, les messages sont donc chiffrés à l'aide d'un système à clé symétrique dite clé de session. Cette clé est elle-même chiffrée avec la clé publique du destinataire, ainsi lui seul pourra la récupérer avec sa clé privée et donc lire le message.

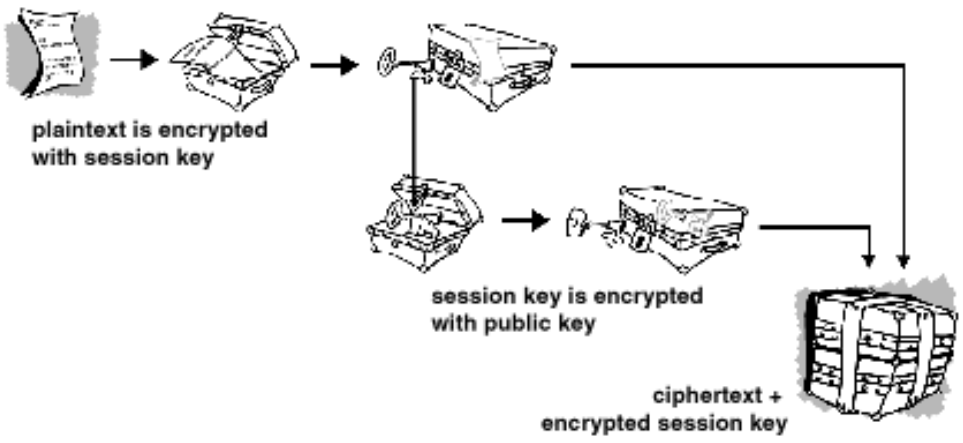


FIGURE 1.24 – Encodage d'un message à l'aide de GPG

La carte bleue cassée

Le 4 mars 2000, le texte suivant tombait dans le forum Usenet `fr.misc.cryptologie` :

```
Petite feuille Maple

> pub:=2^320+convert(`90b8aaa8de358e7782e81c7723653be644f7dcc6f816daf46e532b91e84f`,
                     decimal,hex);
pub := 213598703592091008239502270499962879705109534182641740644252416500858395774644508 84...

> facteur1:=convert(`c31f7084b75c502caa4d19eb137482aa4cd57aab`, decimal, hex);
facteur1 := 1113954325148827987925490175477024844070922844843

> facteur2:=convert(`14fdeda70ce801d9a43289fb8b2e3b447fa4e08ed`, decimal, hex);
facteur2 := 191748170252450443937578626823086218069693418 9293

> produit:=facteur1*facteur2;
produit := 213598703592091008239502270499962879705109534182641740644252416500858395774644 5...

> exposant_public:=3;
exposant_public := 3

> modulo_div_eucl:=(facteur1-1)*(facteur2-1);
modulo_div_eucl := 213598703592091008239502270499962879705109534182338597041485083258128 26...

> essai_rate_exposant_prive:=expand((1+modulo_div_eucl)/3);
essai_rate_exposant_prive := 213598703592091008239502270499962879705109534182338597041485 0...

> exposant_prive:=expand((1+2*modulo_div_eucl)/3);
exposant_prive := 142399135728060672159668180333308586470073022788225731360990055505418845...

> testnb:=1234;
testnb := 1234

> testsignnb:=testnb &^ exposant_prive mod produit;
testsignnb := 223593814777518377564104232545040455789953214462648171523669429097480691923 4...

> testverifsignnb:=testsignnb &^exposant_public mod produit;
testverifsignnb := 1234
```

On y trouve les nombres premiers p et q, ici `facteur 1` et `facteur 2` qui permettent de connaître le module n, ici `produit`. On voit que l'exposant publique, e, est 3 et après un premier test raté on trouve l'exposant privé d. Pour être sûr que tous ces chiffres sont bons, on chiffre 1234 et on le déchiffre. Ça marche.

Ce jour là le grand public voyait en clair la clé RSA à 320 bits qui permet de vérifier l'authenticité d'une carte bleue (voir l'article de Louis Guillou) . Cela indique seulement qu'une carte est authentique et non que l'on connaît le code secret de l'utilisateur, mais cela permet de faire des fausses cartes [a] qui tromperont un lecteur non relié aux banques comme celui qu'on présentait souvent dans les restaurants.

C'est cette faiblesse connue des milieux de la cryptographie qu'a utilisé Serge Humpich [b]. La trouvaille n'est pas extraordinaire car casser une clé de 320 bits n'était plus un exploit depuis le début des années 90. L'exploit réside surtout dans la légèreté du groupement des cartes bleues qui a pris 10 ans pour corriger une faille connue.

a. faire une fausse carte bleue est assimilé à faire de la fausse monnaie. Le tarif est 30 ans de prison.
b. cf http://fr.wikipedia.org/wiki/Serge_Humpich

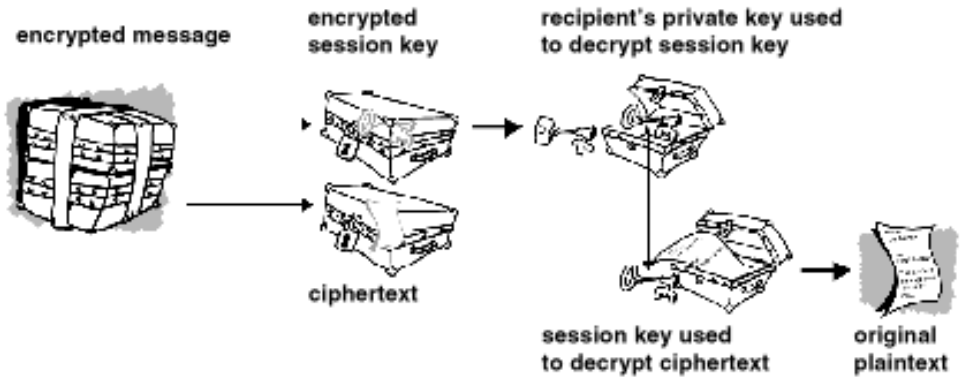


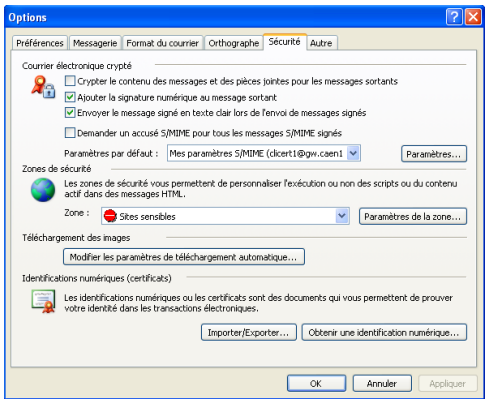
FIGURE 1.25 – Décodage d'un message à l'aide de GPG

Pour signer et vérifier l'intégrité du courrier, l'émetteur fait un condensat du courrier et le chiffre avec sa clé publique. Ainsi le destinataire peut générer le condensat du courrier déchiffré et le comparer avec le condensat que lui a envoyé l'émetteur après l'avoir déchiffré avec la clé publique de l'émetteur.

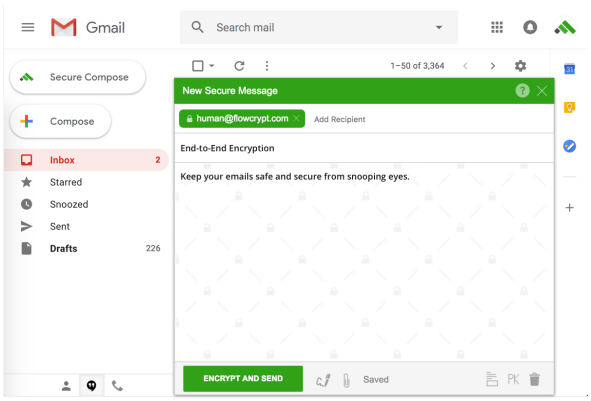
Lorsque GPG est inclus dans votre logiciel de mail, son utilisation est transparente. Son initialisation peut faire peur pour celui qui ne connait rien à la cryptographie puisque qu'on va lui demander de protéger sa clé privée avec un mot de passe et de publier sa clé publique. La publication de la clé publique est la partie la plus sensible puisque mal faite, elle peut permettre l'attaque de l'"homme au milieu", cf page 45. Il est donc soit nécessaire de la transmettre main dans la main [34], soit de la faire signer par une connaissance dont on a déjà la clé publique de façon sûre et ainsi agrandir sont réseau de confiance. On pourrait envisager de faire signer sa clé par une autorité de certification mais je ne l'ai jamais vu faire (trop lourd, trop cher ?).

En pratique S/MIME ou GPG sont de plus en plus intégrés dans les lecteurs de courrier mais il peut être quand même nécessaire de créer ses clefs soi même, cf ce site d'autodéfense courriel. Pour les webmails [35] c'est plus rare mais il existe des greffons pour Gmail comme FlowCrypt ou Mailvelope. Notez que le mode confidentiel de Gmail (*Gmail Confidential Mode*) n'est pas une protection acceptable car elle ne protège pas contre Google ni contre les états qui ont autorité sur Google ou d'un piratage des serveurs de Gmail [36].

34. transmettre le condensat de la clé publique est souvent plus simple et permet ensuite de récupérer la clé sur Internet puis de vérifier qu'elle est la bonne.
35. Le mail qu'on lit avec son navigateur.
36. lire aussi la réaction de l'EFF à ce sujet



Outlook et S/MIME



Gmail et FlowCrypt

FIGURE 1.26 – Lecteurs de mail et leur outil de cryptographie

Le Web sécurisé

Le Web est protégé par l'algorithme de chiffrage SSL [37] qui est présent sur les navigateurs les plus courants. Par contre, comme pour tout algorithme de chiffrage, son efficacité est directement liée à son utilisation et à la taille de la clé de codage utilisée.

Ainsi la majorité des pages web ne sont pas chiffrées et donc passent en clair sur le réseau avant d'arriver sur votre ordinateur. Cela veut dire que toute personne qui contrôle les machines intermédiaires peut savoir quelles sont les pages web que vous regardez.

Lorsque vous arrivez sur une page sécurisée, ce qui est visible par une icône en forme de clé ou de cadenas ainsi que dans l'URL qui commence par `https`, personne ne peut intercepter le contenu si la clé de chiffrement utilisée est dite forte, à savoir contient 256 bits [38]. Si par contre la clé est trop courte, comme 40 bits largement utilisé dans les années 90, alors la sécurité est illusoire car trop faible pour résister aux attaques brutales, type d'attaques qui essayent toutes les clés possibles. Avec un niveau de sécurité entre les deux comme 128 bits, encore très utilisé en 2018, vos communication sont protégées pour quelques années à savoir il faudra des années pour déchiffre le message. Si vous ne changez votre mot de passe pour vous connecter à votre banque que tous les 10 ans, vous prenez peut-être des risques.

Aussi n'hésitez pas à cliquer sur le petit cadenas pour vérifier si la protection utilisée est SSL 256 ou 128 bits (si vous trouvez du 40 bits, veuillez me l'indiquer svp !).

Il existe aussi un autre risque qui est celui de ne pas être connecté au véritable serveur mais à une copie comme dans le cas d'hameçonnage. Aussi il existe un système d'authentification du site web visité.

37. renomé TLS depuis 2001
38. un bit est 0 ou 1, 1001 est un nombre binaire à 4 bits qui vaut 9 en décimal.

1.3.3 Authentification et autorité de certification

L'authentification consiste à vérifier l'identité du correspondant.

Dans le cas d'un mail le champs `From` n'est pas suffisant car facilement falsifiable. Aussi il est nécessaire que le courrier soit signé par la clé privée de votre correspondant et que vous ayez sa clé publique. Bien sûr il faut être certain qu'il s'agit de sa clé publique et non pas d'une fausse. Comme il n'est pas toujours aisé de donner main dans la main cette clé ou son condensat, un autre système a été conçu : la certification.

La certification consiste à demander à un organisme reconnu d'offrir la garantie que le document [39] récupéré sur Internet est bien celui de notre correspondant. Pour cela l'organisme ajoute au document sa signature à l'aide de sa clé privée. Ainsi toute personne qui a la clé publique de l'organisme peut vérifier que la signature est bonne. On voit qu'on a seulement repoussé le problème puisque maintenant pour savoir si un document est le bon, il faut récupérer la clé publique de l'organisme.

La bonne nouvelle est que les autorités de certification sont des organismes reconnus aussi leur clés publiques sont présentes par défaut dans tous les ordinateurs. Ainsi la personne qui désire falsifier une clé publique doit maintenant commencer par trafiquer le système d'exploitation ou le navigateur utilisé pour y mettre de fausses clés publiques d'autorité de certification. La tâche est nettement plus ardue.

Ce système est surtout utilisé pour le Web afin de garantir qu'un site appartient bien à celui qu'il déclare être. Dans ce cas il existe différents niveaux de certification. L'autorité peut vérifier seulement que le domaine appartient bien à celui qui demande le certificat ou aller plus loin en demandant des documents officiels. Cela se retrouve graphiquement dans certains navigateurs :

FIGURE 1.27 – Certificat basé sur le nom de domaine et certificat basé sur des papiers officiels

Les autorités de certification commerciales

De nombreuses entreprises sont des autorités de certification [40]. Elles bénéficient d'un marché très lucratif puisque signer la clé d'une personne est une opération dont le seul coût est la vérification de son identité. On retrouve l'une des nombreuses "poules aux œufs d'or" qui se promènent sur Internet [41]. Cela étant un trublion en la personne de Let's Encrypt perturbe sérieusement le marché depuis 2016 en offrant des certificats gratuits.

L'autorité de certification la plus importante a longtemps été Vérisign, la même entreprise que celle qui gère les `.com` et `.net`. Elle a acheté de nombreux concurrents comme Thawte

39. clé publique, certificats SSL ou autre
40. Pour se décréter autorité de certification, il suffit d'avoir une clé publique et de se faire connaitre
41. Dans la même veine que la gestion des noms de domaine.

et GeoTrust avant de céder en 2010 sa partie autorité de certification à Symantec [42] pour 1,28 milliards de dollars. Depuis c'est le déclin et plus aucune autorité n'a pu dépasser les 50% de part de marché.

Nom	Nombre de certificats	Part de marché (%)	Variation mensuelle (%)
COMODO CA Limited	1 158 223	31,65	0,85
DigiCert	541 108	14,79	0,60
Let's Encrypt	510 360	13,95	27,51
GlobalSign nv-sa	278 362	7,61	-1,79
GoDaddy,com Inc,	271 728	7,42	-1,00
cPanel, Inc	91 346	2,50	3,68
Unknown	84 514	2,31	-5,84
Amazon	69 770	1,91	-2,17
Google Trust Services	51 826	1,42	3,36
Starfield Technologies, Inc,	35 063	0,96	2,58
GeoTrust Inc,	34 682	0,95	-44,28

TABLE 1.3 – Classement des autorités de certification
source : Security space – nov. 2018

Les autorités de certification gouvernementales

La signature électronique étant reconnue par la loi en France, il semblerait normal que l'État certifie les signatures des citoyens après les avoir duement vérifiées comme il le fait pour les cartes d'identité. Malheureusement ce n'est pas le cas. L'État délaisse l'identité numérique au secteur privé et il n'est pas possible d'aller au commissariat de police avec sa clé publique et demander qu'elle soit certifiée.

Cela mène à des situations problématiques. Ainsi l'État a demandé aux entreprises de payer la TVA par Internet. Pour cela il leur demandait de justifier leur identité en présentant leur certificat numérique certifié par une autorité de certification. Et pour être bien clair, le ministère des finances indiquait dans sa FAQ sur la TéléTVA que

> *Les autorités de certification font autorité pour certifier les identités et principales caractéristiques des personnes à qui elles délivrent des certificats numériques. Elles jouent un peu le même rôle que les mairies lorsque vous faites une demande de passeport.*

et ajoute

> *(le) Ministère de l'Economie, des Finances et de l'Industrie qui en les référençant, reconnaît la qualité des procédures mises en œuvre dans l'identification des demandeurs, l'enregistrement et la délivrance des certificats. C'est la raison pour laquelle elles sont amenées à vous demander de nombreux justificatifs.*

42. L'entreprise d'anti-virus

Qui certifie ce site web ?

L'équivalent du champs `From:` pour identifier les sites web est leur adresse ou URL. On imagine que `www.lcl.fr` appartient à au Crédit Lyonnais (presque vrai, à sa maison mère) mais là encore il s'agit d'une information qui peut être trompeuse. Ainsi que penser de `www.lcl.net` ou `particuliers.secure-lcl.fr` ? Aussi le web dispose avec SSL d'un outil qui permet ce certifier qui est derrière un site web.

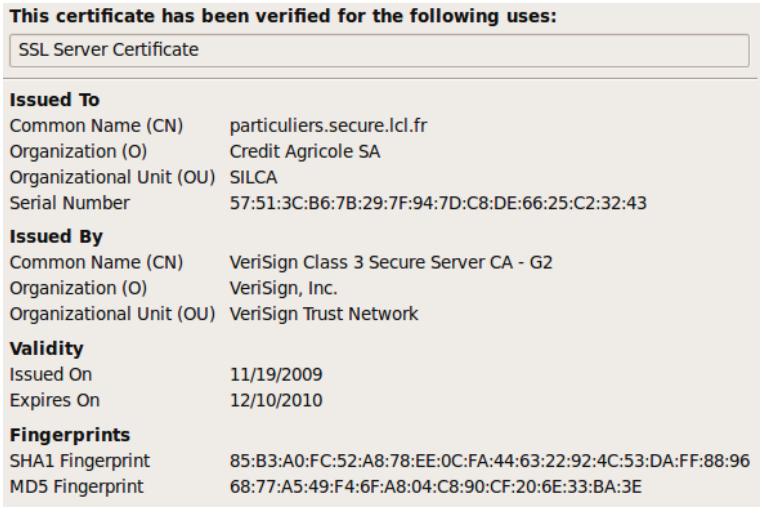


FIGURE 1.28 – Le certificat de `particuliers.secure.lcl.fr`

Là encore on se base sur la signature de la clé publique par une autorité de certification supérieure. Ainsi on peut voir dans le certificat du site du Crédit Lyonnais (lcl) qu'il est certifié par le Crédit Agricole, sa maison mère, qui elle-même est certifiée par Vérisign *Class 3 Secure Server* laquelle est certifiée par Vérisign *Class 3 Primary*. Enfin cette dernière est certifiée par elle-même, il faut bien s'arrêter quelque part.

```
% openssl s_client -connect particuliers.secure.lcl.fr:443
CONNECTED(00000003)
depth=2 /C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority
verify error:num=19:self signed certificate in certificate chain
verify return:0
---
Certificate chain
 0 s:/C=FR/ST=Hauts de Seine/L=La Defense/O=Credit Agricole SA/OU=SILCA/\
     CN=particuliers.secure.lcl.fr
   i:/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=Terms of use at\
     https://www.verisign.com/rpa (c)05/CN=VeriSign Class 3 Secure Server CA
 1 s:/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=Terms of use at\
     https://www.verisign.com/rpa (c)05/CN=VeriSign Class 3 Secure Server CA
   i:/C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority
 2 s:/C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority
   i:/C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority
---
```

On voit que dans ces deux cas où l'internaute veut ou doit justifier son identité, il ne peut le faire qu'en passant par une entreprise privée *qui sera amenée à demander de nombreux justificatifs*, justificatifs qu'un citoyen n'a peut-être pas envie de donner à une entreprise privée. Ce point est d'autant plus triste que la carte d'identité électronique nationale serait très utile sur Internet pour réduire les risques d'arnaques, diminuer le nombre de spam, communiquer avec l'administration, vérifier l'âge des Internautes et peut-être un jour faire des débats en ligne à visage ouvert ou inventer une nouvelle forme de démocratie.

L'auto certification

Puisque la certification est nécessaire pour avoir un site web chiffré et que les autorités de certification étaient payantes avant l'arrivée de Let's Encrypt en 2015, de nombreuses personnes s'auto-certifiaient à savoir qu'elles signaient leur propre clé privée via leur autorité de certification crée pour l'occasion. Dans ce cas la clé ne sera pas reconnue puisque l'autorité n'est pas référencée mais cela permet néanmoins de chiffrer la communication entre le serveur et le navigateur. Malheureusement (ou heureusement) lorsque que le navigateur arrive sur une page web chiffrée par une clé auto-certifiée, il va bloquer la connexion tant que l'utilisateur ne lui indique pas explicitement de passer outre.

Le risque du certificat auto-certifié est qu'il est simple de lui appliquer l'attaque de l'homme au milieu. Ainsi votre FAI pourrait tout à fait générer un certificat auto-certifié qu'il vous présente chaque fois que vous vous connecté sur un site auto-certifié. Il pourra ainsi intercepter vos communications y compris si vous remplissez des formulaires et ce malgré le protocole HTTPS rassurant.

1.3.4 La sûreté de la cryptographie

Pour finir ce chapitre, regardons comment on casse un algorithme de cryptographie :

- il existe une faille mathématique ou une découverte mathématique casse l'algorithme,
- il existe une faille de programmation [43],
- la clé est trop courte et il est possible de tester toutes les clés possibles en un temps raisonnable,
- une faille ou découverte mathématique permet d'éliminer assez de clés pour que l'on puisse tester toutes les autres en un temps raisonnable.

Il y a donc deux catégories : les failles et la force brute qui teste toutes les clés possibles.

La force brute

La longueur d'une clé est la seule protection contre cette attaque. Ainsi suivant les caractères que vous utilisez, l'alphabet, et la longueur de votre mot de passe, tester toutes les clés possibles

43. Il est très difficile de programmer un logiciel de cryptographie même si l'algorithme est simple. Il est plus prudent d'utiliser une bibliothèque qui comprend les algorithmes dont on a besoin.

est raisonnable ou non. Le tableau ci-dessous en donne une idée :

Alphabet	4 caractères	8 caractères	12 caractères
Lettres minuscules	$26^4 = 456\,976$	208×10^9	954×10^{15}
Lettres minuscules et chiffres	$36^4 = 1,6 \times 10^6$	2×10^{12}	4×10^{18}
Minuscules, majuscules et chiffres	$62^4 = 14 \times 10^6$	218×10^{12}	3×10^{21}

TABLE 1.4 – Nombre de clés possibles suivant l'alphabet et la longueur

Si on suppose qu'on a un ou des ordinateurs qui peuvent tester un million de clés par seconde (chiffre très raisonnable) alors on voit qu'une clé de 4 caractères résiste au mieux 14 secondes. Par contre la clé de 12 caractères avec minuscules, majuscules et chiffres résistera un million de siècles...

La destruction de DES DES a une clé de 56 bits [44]. Il a été l'une des premières victimes cassées par la force brute :

— **En juin 97** Rocke Verser de Loveland, Colorado, le casse avec des machines d'autres internautes en 90 jours.
— **En janv 98** `distributed.net` le casse en 39 jours avec 10 000 ordinateurs et une moyenne de 28.1 milliards de clés testées par jour.
— **En juillet 98** `Electronic Frontier Foundation, EFF` le casse en 3 jours avec une machine à 250 000 $ fabriquée pour,
— **En janvier 99** DES est cassé en 22 heures par la machine de l'EFF couplée aux 100 000 machines réunies par le `distributed.net`.

Dans le dernier cas, près de mille milliards de clés étaient testées par secondes. A ce rythme, la clé de 12 caractères avec minuscules, majuscules et chiffres n'aurait tenu qu'un siècle. Sachant que la puissance des ordinateurs double tous les deux ans [45], cela veut dire que dix ans plus tard, la même clé ne résisterait plus que 3 ans.

Cela étant, tester une clé de type DES peut prendre moins de temps que de tester une clé de taille égale d'un autre algorithme, aussi il est important de faire attention aux comparaisons.

Le calcul distribué La force brute est une méthode qui se répartie très bien sur un ensemble d'ordinateurs, chacun testant une partie des clés. Aussi des internautes ont créé l'organisation distributed.net [46] afin de répartir le travail parmi les ordinateurs mis à leur disposition.

Avec cette méthode, le RC5 a été régulièrement cassé avec des clés de plus en plus longues :

— **En octobre 1997, RC5-56** est cassé en 212 jours de travail. Le pourcentage de clés vérifiées est de 47,03%, vitesse moyenne : 5,3 G clés/s. Au rythme final, il aurait fallu 83

44. il faut 6 bits pour stocker un caractère qui soit une minuscule ou une majuscule ou un chiffre, donc par rapport au tableau ci-dessus, 56 bits représente moins de 10 caractères.
45. Loi de Moore interprétée assez librement
46. depuis son dernier succès sur le RC5-64, ce site ne travaille plus sur les algorithmes de cryptographie.

jours pour vérifier l'ensemble des clés restantes.

— **En juillet 2002, RC5-64** trouvé en

```
1 757 jours de calcul, environ 4 ans et 10 mois
331 252 participants
15 769 938 165 961 326 592, 15 milliards de milliards de clés testées
  soit 81% des clés possibles

vitesse maximale : 270 147 024 000 clés/seconde
  - soit 32 000 de Apple PowerBook G4 800MHz ou
    46 000 PC AMD Athlon XP 2Ghz travaillant en parallèle
  - à cette vitesse il suffirait de 790 jours pour tester
    l'ensemble des clés
```

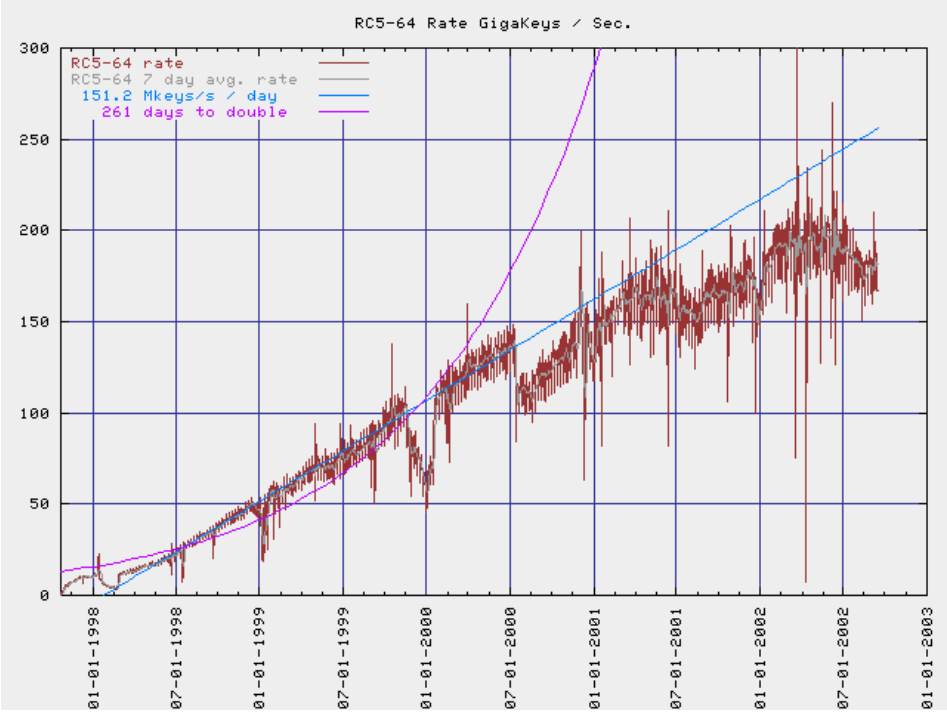


FIGURE 1.29 – Vitesse de test des clés RC5-64 durant le calcul

Casser le Web L'algorithme de cryptographie du Web est SSL. Dans les années 90 et encore au début des années 2000, il se conjuguait en 3 variantes de longueur de clés différentes : SSL 40 bits, SSL 56 bits et SSL 128 bits. Dès l'été 1995, SSL 40 bits a été cassé en 32 heures à l'INRIA et en 3h30 durant l'été 1997 à Berkeley et pourtant des banques l'utilisaient toujours en 2000. Aujourd'hui quelques quelques secondes suffiraient aussi il est indispensable d'utiliser la méthode SSL 128 voire 256 bits.

L'intelligence contre la cryptographie

Il existe peu de cas où des avancées mathématiques cassent des algorithmes de cryptographie, en voici néanmoins deux exemples.

RSA mis à l'épreuve Afin d'avoir une estimation de la sécurité de RSA, l'entreprise RSA Security organise un concours ouvert dont le but est de casser un message chiffré avec l'algorithme RSA d'une longeur de clef déterminée. Le but est de trouver les deux nombres premiers p et q qui génèrent le module de l'algorithme de RSA ce qui permet d'avoir la clé privée. Pour venir à bout de ce défi, la méthode mathématique utilisée est celle du "crible algébrique" qui permet de ramener le problème à un calcul matriciel dont la résolution nécessite un super ordinateur [47]. Ainsi

- **En février 1999, RSA-140 chiffres** a été cassé. Le crible a nécessité environ 125 stations SGI et Sun à 175 MHz et environ 60 PCs à 300 MHz pendant 1 mois. Le système matriciel a demandé 100 heures CPU et 810 MO de mémoire vive sur un Cray C916.
- **En août 1999,RSA-155 (512 bits)** tombe. Le crible a nécessité 160 stations SGI et Sun à 175-400 MHz, 8 SGI Origin 2000 processeurs à 250MHz, 120 Pentium II PCs à 300-450 MHz et 4 500 Digital 500 Mhz pendant **3**.7 mois. La matrice à résoudre avait 6 699 191 lignes et 6 711 336 colonnes pleines à 62.27%. Il a fallu 224 heures CPU et 3.2 GO de mémoire vive sur le même Cray pour résoudre le système.
- **En novembre 2005, RSA 640 bits** est tombé après 5 mois de calcul.
- **En décembre 2009, RSA 768 bits** est le dernier défi tombé.

Depuis 2010 RSA 1024 bits n'est plus considéré comme sûr. En 2017 RSA Security a indiqué que les clefs de 2048 bits devraient tenir jusqu'en 2030. L'organisme NIST suggère d'utiliser des clefs de 3072 bits si on désire que la sécurité dépasse 2030.

MD5 cassé affaiblit le Web Depuis 2004 on sait qu'il est possible de faire deux messages qui ont le même condensat MD5. En 2008, une équipe de chercheurs [48] a appliqué cette possibilité théorique à un cas bien pratique : la génération de faux certificats Web.

En temps normal un site web sécurisé envoie au navigateur un certificat qui prouve qu'il est bien le site web qu'il prétend être, cf figure 1.30. Le navigateur vérifie l'identité du site Web en vérifiant que le certificat qu'on lui envoie est bien signé par une autorité de certification connue (c.a.d. dont la clé publique est dans le navigateur). Si c'est le cas, il ne reste plus qu'à vérifier que les données écrites sur le certificat, comme l'URL, correspondent à celles du site web qu'on est en train de visiter. Tout ce travail est invisible pour l'utilisateur si tout se passe bien.

47. Une présentation sur la factorisation et donc sur la façon de casser RSA est présentée sur ce site : http://pauillac.inria.fr/algo/banderier/Facto/

48. Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, Benne de Weger, cf http://www.win.tue.nl/hashclash/rogue-ca/

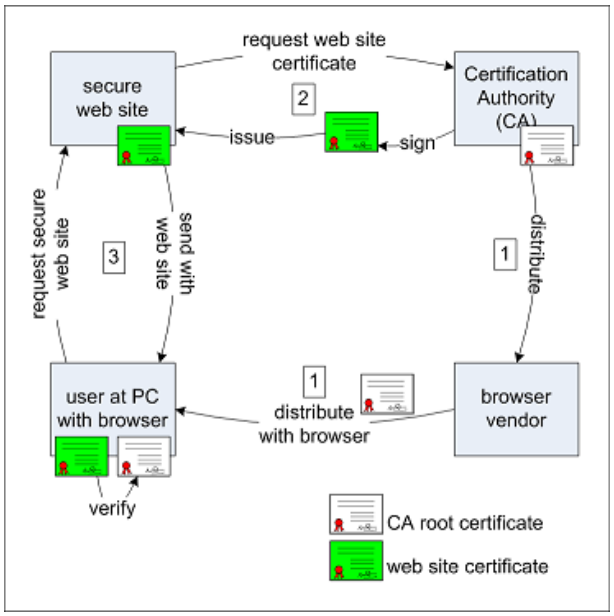


FIGURE 1.30 – Signature et utilisation normale des certificats SSL

Dans le cas normal, l'utilisateur (en bas à gauche) vérifie le certificat du site web (en haut à gauche) avec la clé publique de l'autorité de certification (en haut à droit) qui lui a été fournie avec son navigateur (en bas à droite).

L'attaque, cf figure 1.31, consiste à demander à l'autorité de certification de nous signer un certificat (le bleu). La signature étant faite sur le condensat MD5 du certificat, elle sera aussi valable si elle est attachée à un autre document qui a le même condensat que le certificat qu'on a envoyé. Cet autre est ici la clé publique de notre fausse autorité de certification (la noire). Avec cette fausse autorité, on peut signer le certificat de notre faux site web (le rouge). Maintenant il ne reste plus qu'à intercepter les requêtes vers le site web d'origine (en haut à gauche) et à lui présenter le certificat rouge du faux site accompagné de celui de la fausse autorité de certification (le noir). Ainsi le navigateur constate que le site a un certificat (le rouge), que ce certificat est signé par le noir lequel est signé par le certificat officiel de l'autorité de certification (puisque le noir a le même condensat que le bleu). Donc tout va bien et aucun avertissement ne sera envoyé à l'utilisateur qui se connectera au faux site web en toute confiance puisque la connexion est sûre grâce à SSL.

Depuis l'annonce de cette faille, les autorités de certification sérieuses n'utilisent plus le condensat MD5. Cela peut être vérifié en regardant l'algorithme de signature utilisé dans la description du certificat.

La bêtise contre la cryptographie

SSH cassé par ignorance En mai 2008 la distribution Debian de Linux doit annoncer que toute la sécurité basée sur OpenSSL est compromise. Quelques années auparavant, une personne en charge de faire marcher le logiciel OpenSSL sur Debian a retiré du code source des

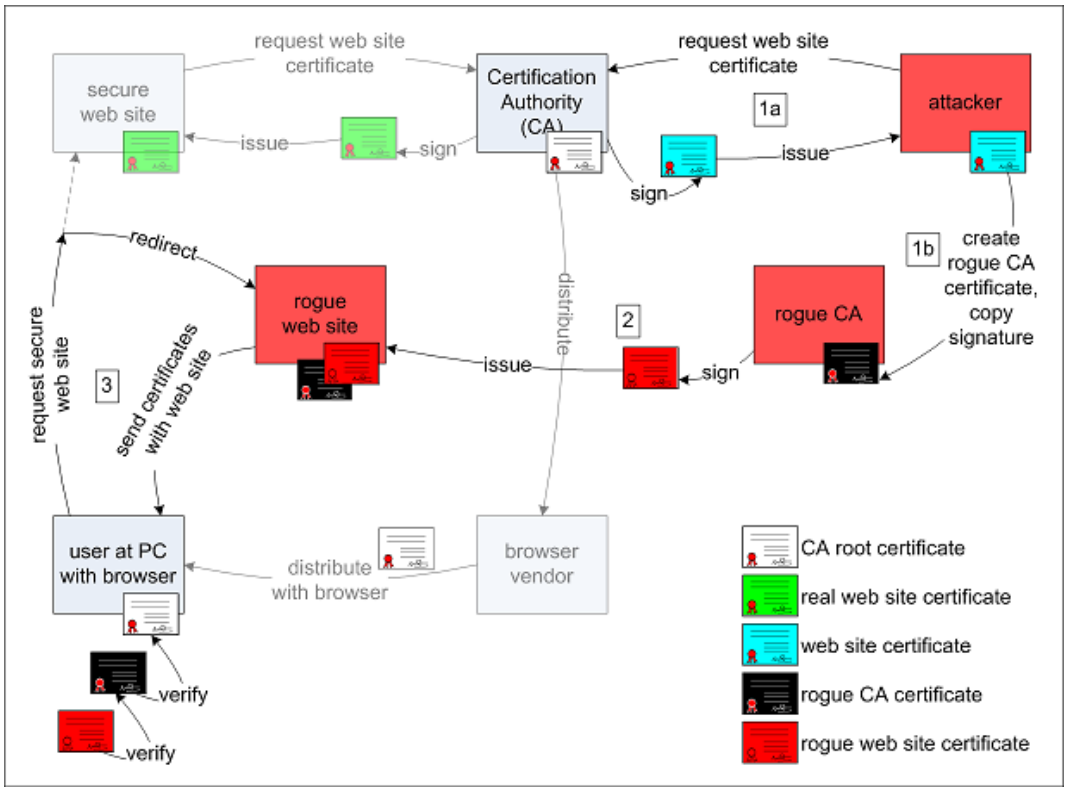


FIGURE 1.31 – Introduction d'un faux certificat SSL

lignes qui semblaient ne servir à rien. Et si le fait de retirer ces lignes n'a rien modifié au fonctionnement du logiciel, cela a détruit la fonction aléatoire en charge de fournir les nombres de base pour générer les clés. Or si on peut deviner ces nombres de base, on peut aussi deviner les clés, donc toute la sécurité s'effondre.

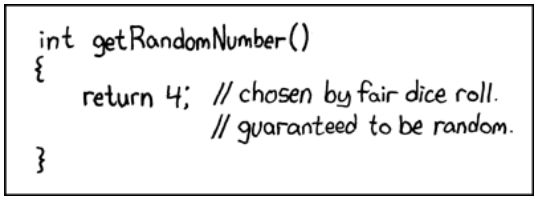


FIGURE 1.32 – XKCD se moque

Moralité : la programmation de la cryptographie est réservée aux spécialistes. Il est illusoire d'espérer programmer un algorithme de cryptographie sans générer des failles de sécurité si on n'a pas une longue expérience dans le domaine.

1.4 Plus

CircleID réunit des articles sur le fonctionnement de l'Internet, ce qui couvre plus que ce

simple chapitre.

À propos de l'architecture d'Internet

- Quesques articles de l'encyclopédie Wikipédia :
  - le protocole d'Internet : http://fr.wikipedia.org/wiki/Internet_Protocol,
  - le DNS : http://fr.wikipedia.org/wiki/DNS
- Architectural Principles of the Internet, RFC 1958 par B. Carpenter, IAB, Juin 1996, https://www.rfc-editor.org/info/rfc1958

À propos de la sécurité

Pour lutter contre la faille humaine, une grande faiblesse de la sécurité informatique :

- Signal Arnaque, https://info.signal-arnaques.com/ lorsqu'on sent l'arnaque possible,
- INFO ESCROQUERIES au 0805 805 817 ou https://www.internet-signalement.gouv.fr/ pour signaler un mail ou site qui semble être une tentative d'escroquerie.
- Cybermalveillance https://www.cybermalveillance.gouv.fr, tant pour les victimes que pour se prévenir des cyber-attaques.

Pour les informaticiens ou passionnés, quelques sources hétéroclites :

- l'observatoire de la sécurité des systèmes, http://www.ossir.org/,
- le blog de Bruce Schneier, http://www.schneier.com/
- Black Hat, https://www.blackhat.com/, l'une des plus grande conférence sur la sécurité,
- le site de l'ANSSI, en charge de la cyber-sécurite en France, https://www.ssi.gouv.fr/
- l'ENISA, en charge de la cyber-sécurité en Europe, https://www.enisa.europa.eu/

À propos de la cryptographie

En ce qui concerne la cryptographie, on pourra aussi consulter les ouvrages suivants : *The Codebreakers* de David Kahn et l'*Histoire des codes secrets* de Simon Sing.

Certains manuels (livres) sont disponibles en ligne dont *The Handbook of Applied Cryptography* et les *Frequently Asked Questions About Today's Cryptography* des RSA Labs.

Enfin voici quelques sites sur le sujet :

- le cours de crypto de la Khan Academy pour débuter en cryptographie
- Learn cryptography présente de nombreux algorithmes et des informations générales
- la section crypto de Reddit
- le blog de Matthiew Green avec ses pensées sur l'actualité de la crypto mais aussi des liens vers d'autres ressources et ses cours.

Chapitre 2

D'hier à aujourd'hui

L'histoire d'Internet est peut-être encore un peu trop jeune pour mériter le nom d'histoire au sens classique du terme, mais à l'échelle de l'informatique, Internet est préhistorique. Internet existait bien avant le premier ordinateur personnel. Lorsque le premier IBM PC est sorti en 1981, Internet avait déjà 12 ans.

Aujourd'hui Internet a cinq milliards d'utilisateurs et est au cœur de nos économies. Les États sont fortement impliqués dans sa stabilité tout en y préparant la guerre. Le cyber-monde a bien changé depuis l'outil académique géré par les chercheurs.

Cette évolution, de l'outil scientifique à l'outil indispensable pour tous peut se résumer en quatre périodes :

- Les années 60 sont celles de la recherche, des premiers articles sur les réseaux informatiques.
- Les années 70 ont permis de tester ces idées sur un réseau reliant quelques universités et de développer des applications dont le courrier électronique qui reste aujourd'hui l'application la plus utilisée.
- Les années 80 sont l'entrée dans l'Internet moderne, tant au niveau de l'informatique que de l'agrandissement du réseau. Durant ces années Internet est devenu un réseau universitaire mondial.
- Les années 90 ont vu l'apparition du Web et du grand public. Le réseau n'est plus un outil de chercheurs mais un mass média et un outil prisé tant par les citoyens du monde que par l'économie.
  Depuis Internet se développe. On a vu l'explosion des réseaux sociaux, l'arrivée des objets connectés, le télétravail (forcé ou désiré). Le monde virtuel est de plus en plus concret.

2.1 1958–1969 La recherche

Si la connexion d'ordinateurs en réseau semblait naturelle, deux aspects extérieurs à l'informatique ont guidé les recherches qui ont abouti à ce qui deviendra Internet :

— le réseau doit être résistant aux pannes, l'arrêt d'un nœud ne doit pas pouvoir bloquer le reste du réseau. Cet aspect est d'autant plus important si le réseau est un réseau militaire.
— les ordinateurs, des années 60, étant des machines excessivement chères, il faut trouver une façon de les partager entre les chercheurs des différents centres de recherche.

La chronologie

Puisque le premier réseau s'appelle Arpanet du nom de l'organisme qui a financé son développement, on aime à commencer l'histoire d'Internet à la création de l'ARPA, l'Advanced Research Projects Agency. Et puisque l'ARPA a été créée en réaction au lancement de Spoutnik, on commence notre chronologie en 1957.

Légende

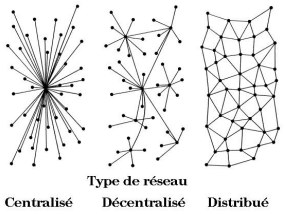
La chronologie utilise les symboles suivants :

 ordinateur ou machine

 terminal Minitel

 internaute

Pour les sigles, veuillez vous référer au glossaire.

Date	Généralités	Chiffres	Hors Internet
1957			Spoutnik est lancé
1958			Les États-Unis vexés créent l'ARPA, l'Advanced Research Projects Agency, pour ne plus être dépassés technologiquement.
1961	Leonard Kleinrock (MIT) publie ses premiers travaux sur la commutation de paquets.		
1964	Paul Barran (RAND) publie On Distributed Communications Networks sur les réseaux à commutation de paquets distribués.		
1965	L'ARPA finance une étude sur un réseau d'ordinateurs en temps partagé.	Débit : 1200 bps [1]	

1. bps : bits par secondes

Date	Généralités	Chiffres	Hors Internet
	Lawrence Roberts et Thomas Merrill relient deux ordinateurs par le téléphone à 1200bps, l'un au MIT, l'autre à Santa Monica (Californie).		Doug Englebart développe les concepts de la souris et de l'hypertexte.
1966	Premier projet d'Arpanet publié par Lawrence Roberts		
1968	Appel d'offres Arpanet. BBN (Bolt, Beranek & Newman) est choisi pour construire les équipements.		
1969	Les premières RFC[2], la 1 et la 4 décrivent l'interface d'Arpanet avec les ordinateurs, et sa mise en service.		

2.2 1969–1982 Le développement technique

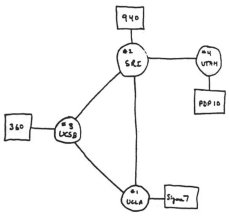
Alors que les États-Unis mettaient en place le réseau Arpanet, l'Angleterre et la France travaillaient aussi sur des projets similaires (en France il s'agit du projet Cyclades mené par Louis Pouzin). Les expériences de chacun ont ainsi permis d'améliorer les procédures pour arriver finalement au protocole retenu pour Internet à savoir la version 4 de TCP/IP.

En même temps le réseau a été le terreau sur lequel se sont développées les premières applications. Parmi elles, le mail et les listes de diffusion qui ont rapidement suivi, les forums de discussion (USENET), le téléchargement (FTP). Avec l'augmentation des débits, d'autres applications suivront.

C'est aussi durant ces années que le système d'exploitation UNIX[3] sera développé. Il a été pendant toutes les années 80 le système d'exploitation utilisé sur Internet. Il reste encore le système de référence dans le monde de la recherche et se propage en dehors de la recherche *via* Linux et Mac OS X.

2. Request For Comment, les articles technique de référence de l'Internet
3. on devrait dire *les* car il existe de nombreuses déclinaisons d'UNIX, chaque constructeur ayant la sienne.

La chronologie

Date	Généralités	Chiffres	Hors Internet
1969	Mise en service d'Arpanet *via* des lignes ATT à 50 kbps, les quatre premiers nœuds sont — le 30/08, l'Université de Californie, Los Angeles — le 01/10, l'Institut de Recherche de Stanford — le 01/11, l'Université de Californie, Santa Barbara — en décembre, l'Université d'Utah	Débit : 50Kbps Arpanet : 4 sites 	 *One small step for a man, one giant leap for mankind.*
1971		Arpanet : 15 sites, 23 machines	 Premier processeur d'Intel, le 4004 Xerox développe la première imprimante laser.
1972	Débuts du courrier électronique sur Arpanet. Le @ est utilisé pour les adresses. première démonstration du réseau Cyclades/Cigale, dirigé par Louis Pouzin. Des idées essentielles développées pour Cyclades seront reprises dans TCP/IP.		 Steve Jobs et Steve Wozniak lancent Apple. 
1973	Arpanet devient international en reliant l'University College (Londres) et le Royal Radar Establishment (Norvège). Premiers problèmes de sécurité sur Arpanet (RFC 602).	Arparnet : 2000	Bob Metcalfe (Xerox) invente Ethernet : le réseau local. 
1974	Cyclades est opérationnel.		Roland Moreno invente la Carte à puce.

Date	Généralités	Chiffres	Hors Internet
	Vinton Cerf et Robert Kahn publient leurs premiers travaux sur TCP/IP.		
1975	Premières listes de discussion sur Arpanet. La plus populaire : SF-Lovers, non officielle. Nouvelle version de TCP/IP : séparation de TCP et IP, ajout de UDP.		
1976			Premier super-ordinateur de Cray.
1977		Arpanet : 100	
1978	Version 4 de TCP/IP : base technique de l'Internet moderne. faute d'appui, arrêt de Cyclades qui relie à l'époque 20 ordinateurs à travers la France. MUD (multi-user dungeon), l'ancêtre de WoW Premier spam	 *source : La Recherche*	ouverture opérationnelle du réseau Transpac de France Telecom.
1979	Usenet, le forum décentralisé sur tous les sujets		
1981	Le système Unix 4.2 BSD (Berkeley) inclut TCP/IP	Arpanet : 200  B.Gates & P.Allen	IBM Lancement de l'ordinateur personnel : l'IBM PC Microsoft sort son premier système d'exploitation : MS DOS Télétel et le Minitel font leur apparition, utilisant l'infrastructure Transpac. Création de BITNET (protocoles IBM)

Date	Généralités	Chiffres	Hors Internet
1982	ARPA commence à préparer la conversion d'Arpanet à TCP/IP.	Ethernet 10 Mbps	TCP/IP devient standard du ministère de la Défense des États-Unis ce qui contraint les fournisseurs à ajouter TCP/IP aux ordinateurs vendus à ce ministère. Premiers systèmes TCP/IP commercialisés (Sun sous Unix BSD).

2.3 1983–1993 L'Internet moderne

En 10 ans Internet se propage, dans le monde universitaire, plus vite qu'un virus. On passe de quelques centaines à plus d'un million de machines, d'un réseau limité aux États-Unis et quelques proches à un réseau mondial, quoi que essentiellement présent dans les pays occidentaux.

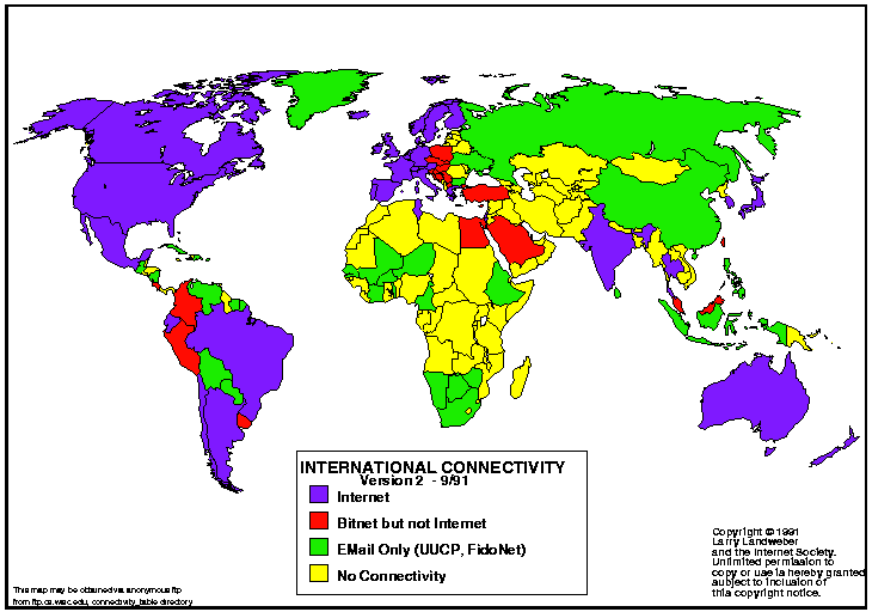


FIGURE 2.1 – Réseau informatique principal des pays en 1991

Durant cette même période, d'autres réseaux se sont développés comme le Minitel en France, cf ci-dessous, et BITNET, véritable concurrent de l'Internet [4]. Au début des années 90, BITNET sera à son apogée, étant même le principal réseau dans de nombreux pays, mais sans dépasser Internet, cf figures 2.1 et 2.2. BITNET disparaitra durant les années 90 devant Internet. Le troisième protagoniste, le "réseau" UUCP [5], est une collection de programmes permettant de se connecter par intermitence à Internet et d'échanger les données stockées en attendant la connexion. UUCP est essentiellement utilisé pour le courrier et les forums de discussion.

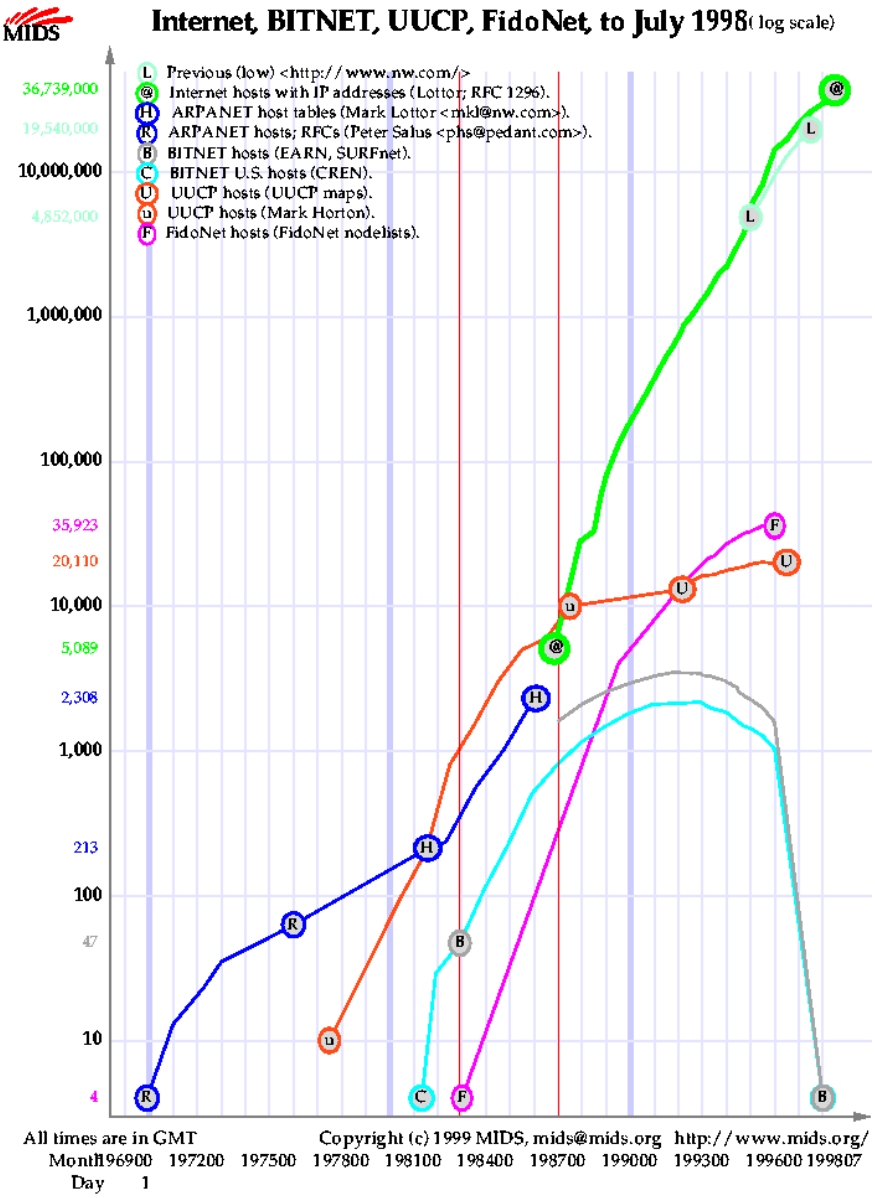


FIGURE 2.2 – Nombre de machines des différents réseaux entre 1969 et 1998

4. ce qui n'empéchait pas les deux réseaux d'être interconnectés et donc de permettre d'échanger des mails d'un réseau à l'autre.
5. Unix to Unix CoPy

L'âge d'or du Minitel

En France, le phénomène le plus important dans le domaine des Technologies de l'Information et de la Communication des années 80 est bien sûr le Minitel [6]. Alors qu'Internet est réservé aux universitaires, le Minitel vise le grand public et même s'il n'atteint que le grand public français, les chiffres parlent d'eux même :

- 1984
  - début de l'Internet moderne, le DNS vient d'arriver suite au trop grand nombre d'ordinateurs, il faut dire qu'on vient de franchir le cap des 1000 ordinateurs,
  - le Minitel a aussi passé ses tests avec succès et le déploiement se fait à grande vitesse : déjà 120 000 terminaux.
- 1993
  - sur Internet le Web est né, les premières offres d'abonnement au grand public ont vu le jour aux États-Unis, toutes les universités occidentales sont connectées, il y a plus d'un million de machines.
  - le Minitel est à son sommet, plus de 6 millions de terminaux, 9 d'après d'autres sources, un taux de pénétration très important car ces millions de terminaux ne sont que pour la France. En même temps le Minitel offre 23 000 services quand les serveurs web ne se comptent qu'en centaines sur Internet.

Au début des années 90 le Minitel est le plus grand réseau informatique mondial. Pourtant Internet l'a tué.

Comment expliquer que David ait tué Goliath ?

La principale raison semble être le retard technologique du Minitel. Les évolutions entre les terminaux des années 80 et ceux des années 90 n'ont pas suivi la progression de la micro-informatique. La simple comparaison entre une page Videotex et une page Web suffit à voir l'écart. Pire, le Minitel reposait sur des terminaux "bêtes" qui ne peuvaient pas offrir à leur utilisateur la souplesse et la puissance d'un micro-ordinateur. Envoyer un mail avec une photo du dernier né en pièce jointe n'était pas envisageable avec un Minitel.

D'autres raisons ont fait pencher la balance. Alors que le Minitel est perçu comme un produit commercial, Internet est perçu comme un mass média mis à la disposition de chacun [7]. Pour certains, l'attachement à Internet est semblable à celui que l'on peut porter à la presse ou à un droit fondamental.

Enfin Internet est ouvert ce qui permet de de déployer un site web ou construire une application sans avoir à payer des royalties et sans crainte de devoir arrêter tout développement pour des raisons juridico-commerciales. Ainsi chacun peut construire sur les technologies de l'Internet sans n'avoir rien à demander ni d'un point de vue légal, ni pour la mise en production. À l'inverse le Minitel s'appuie sur le réseau centralisé et fermé Transpac. Pour proposer un service dans le kiosque (l'équivalent d'un site web), il fallait passer par des procédures administratives et utiliser les serveurs de France Télécom.

6. cf l'article *Du Minitel à l'Internet* de Christophe Cariou et Morgane Gaulon-Brain, https://larevuedesmedias.ina.fr/du-minitel-linternet pour une histoire complète du Minitel
7. les blogs d'aujourd'hui en sont un exemple remarquable.

La chronologie

Date	Généralités	Chiffres	Hors Internet
1983	(1er janvier) Arpanet se convertit entièrement de NCP à TCP/IP en une nuit : début de ce que l'on appelle l'Internet. Arpanet se sépare en ARPANET et MILNET, le second étant le réseau des militaires des E.U..		
1984	Mise en service du DNS (Domain Name Service) : les noms sur Internet ne sont plus centralisés. Richard Stallman lance le projet GNU, source du logiciel libre politique.	Internet : 1000 Minitel : 120 000 	2 ans après le CD Audio inventé par Sony et Philips, voici le CD-ROM pour stocker les données.
1985		Minitel : 1 millions de	
1986	La National Science Foundation met en service NSFNET qui relie 5 centres de super-ordinateurs *via* une infrastructure à 56 kbps. NSFNET remplace l'ARPNET pour les universités et les agences gouvernementales.		
1987	Première TCP/IP Interoperability Conference. Elle deviendra INTEROP en 1988. Les premiers routeurs dédiés apparaissent (Cisco, Proteon, Wellfleet...).	Internet : 10 000 Minitel : 3 millions de	
1988	Le ver de l'Internet affecte 6000 machines sur les 60.000 du réseau. L'importance de la sécurité apparaît. IRC (Internet Relay Chat)		Première fibre optique posée entre l'Europe et l'Amérique du Nord. Elle permet 40 000 connexions téléphoniques simultanées.

Date	Généralités	Chiffres	Hors Internet
	Pays connectés à NSFNET : Canada, Danemark, Finlande, France, Islande, Norvège, Suède.	NSFNET 1,5 Mbps	
1989	Nouveaux connectés à NSFNET : Australie, Allemagne, Israël, Italie, Japon, Mexique, Hollande, Puerto Rico, Royaume Uni. Apparition des premiers opérateurs Internet commerciaux aux E.U.	Internet : 100 000	
1990	Tim Berners-Lee crée le Web au CERN (Centre Européen pour la Recherche Nucléaire) à Genève. Les derniers restes d'ARPANET sont arrêtés.		
1991		NSFNET 45 Mbps Minitel : 6 millions de	Linux, le système d'exploitation libre écrit par Linus Torvalds.
1992	Création de l'ISOC, l'association des internautes. Elle devient le cadre légal de l'IAB, l'IETF et l'IRTF.	Internet : 1 million d' Internet Society	
1993	création de Renater, réseau pour la recherche. Sortie du navigateur Mosaic : les graphismes apparaissent sur le Web. premiers fournisseurs commerciaux d'Internet. création de Usenet `fr.*`		

2.4 1994– L'ouverture au grand public

L'ouverture au grand public est retrospectivement la plus grande révolution de l'Internet. Elle a changé la nature physique de l'internet, les réseaux appartenant aux monde universitaire ayant laissé place aux réseaux commerciaux, elle a changé son fonctionnement avec la création d'organismes de gouvernance comme l'ICANN, elle a enfin changé la mentalité dominante en transformant cet outil universitaire en mass média accessible à tous avec toute les conséquences qu'on connait aujourd'hui. Seule la technologie de l'internet a échappé à cette révolution, son évolution actuelle suivant son chemin imperturbablement. On notera à ce propos que les applications les plus utilisées de nos jours, le courrier électronique et le Web, sont des inventions d'avant l'ouverture au grand public.

L'arrivée du grand public a commencé aux Etats-Unis. L'Europe a suivit, puis le reste du monde. Rapidement, les réseaux informatiques grand public existants, AOL, Compuserve, mais aussi le Minitel, se sont connectés à Internet. Puis des fournisseurs d'accès à Internet sont nés permettant à chacun d'accéder pleinement à Internet, par téléphone au début, donc facturé à la minute, puis par ADSL, le cable ou la fibre aujourd'hui, donc au forfait.

De leur coté, les institutions ont suivi le mouvement. Les ministères, les services liés à l'État [8], les mairies et toute l'administration se sont connectés pour y proposer leurs services. Les entreprises ont fait de même et la bourse, éblouie par ce marché à la croissance exponentielle, s'y est brûlé les ailes (crack de l'an 2000) pour y revenir avec un véritable succès. Aujourd'hui les entreprises les plus valoriséevalorisées sont liées à Internet.

Nos dirigeants, surpris par ce nouveau venu, ont naturellement cherché à prendre le contrôle de cet engin arrivé de nul part et bien loin de leur monde. Cela a commencé par l'établissement de lois pas toujours heureuses, voire inconstitutionnelles [9], puis par la mise en place d'organismes de surveillance, de suggestion et enfin par le noyautage d'instances fonctionnelles d'Internet. Mais si les États ont aujourd'hui un certain contrôle de l'internet, force est de constater que ce contrôle n'est que partiel, l'évolution des technologies et des comportements obligeant trop souvent nos députés à légiférer avec un train de retard.

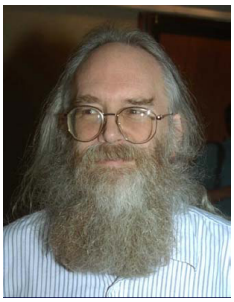
Au niveau mondial, les États-Unis contrôlent toujours le nœud central d'Internet à savoir l'attribution des noms de domaines et des adresses IP. Ce pouvoir, contestable puisqu'Internet est devenu un bien mondial, est d'autant plus contesté par les autres pays que les E.U. l'utilisent à des fins privées. Ainsi le gouvernement américain a fermé les domaines de l'Afghanistan et de l'Iraq, `.af` et `.iq`, durant les guerres qu'il a mené contre ces pays. Il a aussi pu retarder de plusieurs années l'ouverture de la terminaison de domaine `.xxx` pour les sites pornos alors que l'organisme en charge des noms de domaine, l'ICANN, avait décidé de son ouverture.

8. on se souviendra de la lutte pour obtenir que les textes de loi soient disponibles gratuitement sur Internet alors qu'une société les vendait sur le Minitel.

9. comme l'établissement d'un conseil administratif de validation des pages web proposé par Mr Fillon, ministre des Technologies de l'Information de l'époque.

La chronologie

Date	Généralités	Chiffres	Hors Internet
1994	premiers fournisseurs d'Internet par téléphone pour le grand public Amazon, la librairie en ligne Les développeurs de Mosaic lancent le navigateur Netscape Création du W3C pour gérer le Web. Yahoo ! indexe le web.		
1995	La NSF arrête le financement de NSFNET. La plus grande partie de l'infrastructure appartient désormais à des opérateurs commerciaux. Plus de 50% des réseaux sont extérieurs aux USA. Real Audio lance le flux sonore. Il est possible d'écouter la radio sur son ordinateur. Altavista est le premier moteur de recherche de la toile. Sun lance le langage Java pour exécuter des programmes, dits applettes, au sein du navigateur.	Ethernet 100 Mbps	Lancement de Windows 95 et du navigateur Internet Explorer.
1996	Création de l'Association des Utilisateurs d'Internet (AUI). D'autres associations suivront dont la branche française de l'ISOC.	Internet : 10 millions de 16 millions d'	Le support DVD arrive en remplacement des cassettes VHS.
1997	Première version du Wifi, 2 Mbps	36 millions d'	Les DVD gravables apparaissent au Japon. Il faudra attendre quelques années pour les voir en Europe.

Date	Généralités	Chiffres	Hors Internet
1998	 L'ICANN (Internet Corporation for Assigned Names and Numbers) est créée pour superviser la gestion des noms de domaine et des adresses IP. Elle cassera le monopole de la NSI pour permettre à d'autres registrars d'enregistrer les noms de domaine en `.com`, `.net` et `.org`. Arrivée de Google qui prend rapidement la première place des moteurs de recherche devant Altavista, Lycos ou Yahoo.	70 millions d'   Jon Postel 1943-1998 Google	
1999	Arrivée de l'ADSL.  Napster permet le partage et donc la copie de la musique. L'accès à la musique ne sera plus comme avant.	150 millions d'  Ethernet 1 Gbps Internet2 2,5 Gbps Wifi v2 10 Mbps	 Apple sort Mac OS X (dix), un système d'exploitation UNIX.
2000	Première élection mondiale par Internet pour choisir 5 des 19 administrateurs de l'ICANN. L'ICANN crée 7 nouvelles terminaisons d'adresse (Top Level Domain) à savoir `.aero`, `.biz`, `.coop`, `.info`, `.museum`, `.name`, `.pro`	10 millions noms de domaine 100 millions d'  250 millions d' 	Le bug de l'an 2000 passe comme une lettre à la poste, ouf! La bourse ne croit plus en la nouvelle économie, le crack est violent, à la mesure de l'envolée des années 90.
2001	Les *majors* obtiennent l'arrêt de Napster. Wikipedia, l'encyclopédie en ligne qui va balayer les encyclopédies papier.	450 millions d'  . 	Lancement de la 3G

Date	Généralités	Chiffres	Hors Internet
2002	Après la chute de Napster, de nombreux réseaux de P2P naissent.	550 millions d' 	
2003	Les réseaux de contacts professionnels ou d'amis, Plaxo, Orkut, LinkedIn, prennent leur essor. Verisign renvoie les erreurs web en `.com` et `.net` vers son site SiteFinder et perturbe ainsi le DNS. L'ICANN ordonne à Verisign d'arrêter son *service*. 1er volet du Sommet Mondial sur la Société de l'Information (SMSI), sommet au niveau des chefs d'états organisé par l'UIT (Genève).	600 millions d'  Internet2 10 Gbps Wifi 3 50 Mbps sommet mondial sur la société de l'information Genève 2003 - Tunis 2005	
2004	Google entre en bourse. Succès digne des années fastes. Création du réseau social Facebook Naissance des Anonymous	250 M d'  720 M d'  facebook	 World of Warcraft (WoW) conquière le massivement multi-joueur
2005	Second volet du SMSI avec le problème du partage du contrôle d'Internet (Tunis). YouTube, site d'hébergement de vidéos. Il sera racheté l'année suivante par Google.	830 M d'  5 M d' 	 Android est créé
2006	1er Forum sur la Gouvernance de l'Internet (Athènes). nouveaux TLD : `.cat`, `.eu`, `.asia`, `.travel`, `.jobs` Twitter crée le tweet, message d'une ligne (140 caractères). Amazon Web Services Le nuage prend son envol.	1 milliard d'  10 M d'  Ethernet 10 Gbps  amazon web services	

Date	Généralités	Chiffres	Hors Internet
2007	Le nom de domaine `porn.com` est vendu pour 9,5 M$ Netflix passe au *streaming*	50 M d'	Ordiphone : - iPhone d'Apple - GPhone de Google
2008	IPv6 activé sur des serveurs racines du DNS	500 M d' 100 M d'	
2009	Stuxnet est le premier virus attribué à un État afin de détruire les infrastructures d'un autre. Création du bitcoin Oracle achète Sun	4G : 80 Mbps / Wifi 4 600 Mbps 1 G de vidéos vues par jour 250 M d'	La 4G utilise l'IP
2010	Wikileaks commence la publication des dépêches diplomatiques US Instagram, un réseau social plus imagé, pour ordiphones surtout	2 G[10] d' 500 M d'	iPad d'Apple 
2011	Microsoft achète Skype Snapchat, le réseau social aux données éphémères	Ethernet 100 Gbps	Printemps arabe attribution des licences 4G pour 3,5 G€
2012	Minitel ferme le 30 juin La vidéo "Gangnam Style" atteint 1 milliard de vues	0 1 G d' 500 M d'[11]	création de Free Mobile, 2 fois moins cher que la concurrence
2013	Edward Snowden révèle l'espionnage total de la NSA (PRISM, Muscular...)		
2014	Facebook achète WhatsApp pour 19 G$	1 G d' Wifi 5 7 Gbps	Android Wear
2015	TikTok le réseau social made in China Lancement de l'Ethereum, une crypto-monnaie et un système de contrats → DeFi[12]	3 G	EDF déploie Linky, le smart-grid avance

10. giga c.a.d. milliard
11. comprend probablement les faux comptes
12. La finance décentralisée fonctionne sans intermédiaires financiers, banques, courtiers ou bourses.

Date	Généralités	Chiffres	Hors Internet
2016	L'ordiphone plus utilisé que l'ordinateur pour se connecter à Internet		L'IA AlphaGo bat au go Lee Sedol (18 titres internationaux) permet de fausser les élections aux É.U. (Cambridge Analytica, publicités russes)
2017	Le poids de la pub sur Internet dépasse celui sur la TV Les É.U. abadnonnent la neutralité du net	2 G d'	AlphaZero apprend à jouer aux go et échecs seulement avec les règles et bat tous les autres programmes.
2018		4 G d' 100 M d'	
2019	Le nom de domaine `voice.com` est vendu pour 30 M$	5G : 2 Gbps /	Les ÉU mènent le boycott de la 5G chinoise
2020		Wifi 6 9,6 Gbps	Covid : confinements généralisés (3 mois) → télétravail attribution des licences 5G pour 2,8 G€
2021	L'entreprise devient Meta	1 G d'	
2022	Elon Musk achète Twitter pour 45 G$ Ethereum passe à la preuve par enjeu (moins énergivore) ChatGPT, une IA en ligne qui dialogue au niveau humain	5 G d'	
2023	Meta ouvre son IA Llama Twitter devient	100 M d'	
2024	Claude 3.5 d'Anthropic concurrence ChatGPT 4o	3 G d'	

2.5 Histoire du oueb

Voici un résumé rapide de l'histoire (essentiellement technique) du web en une figure et des marqueurs qui notent les étapes.

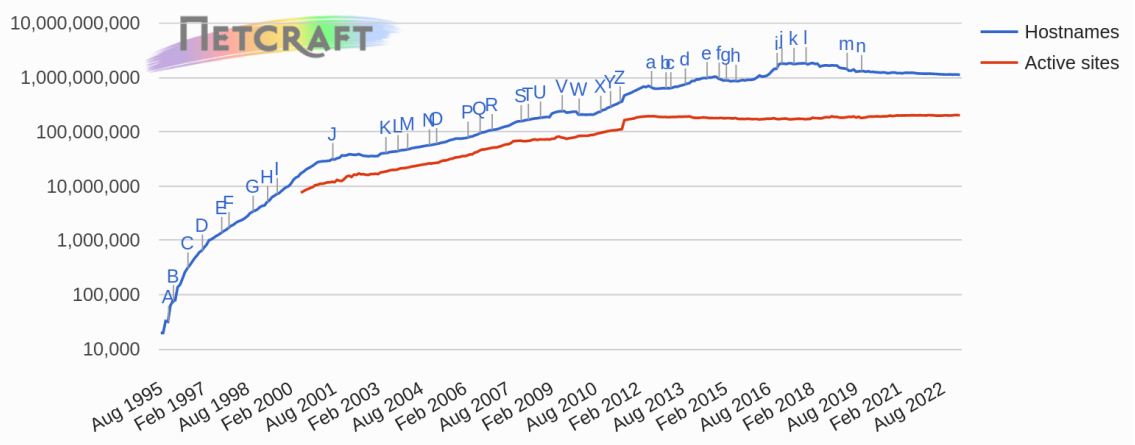


FIGURE 2.3 – Nombre de sites web (échelle logarithmique)

A	IE supporte les cookies	S	HTML 5
B	Netscape annonce Javascript	T	Google Cloud
B	Sun lance Java	U	Google Chrome
C	Répartiteur de charge de Cisco	V	Cloudfare
D	Flash	V	Bing
D	HTML 3.2	W	npm (paquets Javascipt)
E	Google.com	X	Angular JS
F	HTML 4.0	Y	IANA n'a plus d'adresse IPv4
G	Akamai	Z	Google+
G	ICANN	a	Hotmail devient Outlook
G	Serveurs dédiés de Rackspace	b	Yahoo : 3 giga de comptes piratés
H	Flux RSS	c	*Certificate Transparency*
H	Fin du monopole pour l'enregistrement des noms de domaine	d	ICANN délègue son 1er gTLD
I	Red Hat entre en bourse	e	Kubernetes
I	Débuts de Blogger	f	Let's Encrypt
J	VMWare (virtualisation)	g	HTTP/2
K	Wordpress	h	Javascript ES6
L	Xen 1.0	i	HTML 5.1
M	Facebook	j	Plus de 10 M de certificats SSL
N	Mozilla Firefox 1.0	k	Facebook : 2 G utilisateurs par mois
O	Ajax	l	HTML 5.2
P	Twitter	m	Fin de Google+
Q	Amazon EC2 (cloud)	n	100 M de sites web sécurisés (https)
R	iPhone		

source : Netcraft, 2023

2.6 Internet aujourd'hui

2.6.1 Les internautes

Avertissement *Il est difficile de savoir combien de personnes sont connectées à Internet. Les instituts de sondage n'ont pas obligatoirement tous la même définition de l'internaute*[13] *et même si tel est le cas, ils n'ont pas tous les mêmes outils de mesure. Ainsi le rapport 2003 de l'UIT souligne l'exemple de l'Espagne où, suivant les sondages, plus de 50% ou moins de 20% de la population était connectée à Internet. Plus généralement, ce rapport indique qu'en Europe, les instituts de sondage nationaux ont en moyenne des chiffres inférieurs de 30% à ceux des instituts de sondage privés. Les chiffres doivent donc être pris pour ce qu'ils sont, à savoir un résultat de sondage, et non une vérité absolue. Cet avertissement fait, on peut généralement comparer les chiffres entre eux lorsqu'ils proviennent de la même source.*

Internet est utilisé par plus de 5 milliards d'humaine pour une population de 8 milliards (en 2023). La répartition du 20e siècle où les pays développés étaient largement sur-représentés, tend à s'homogénéiser, l'Asie et l'Afrique accélèrent leur progression quand l'Amérique du Nord et l'Océanie stagnent.

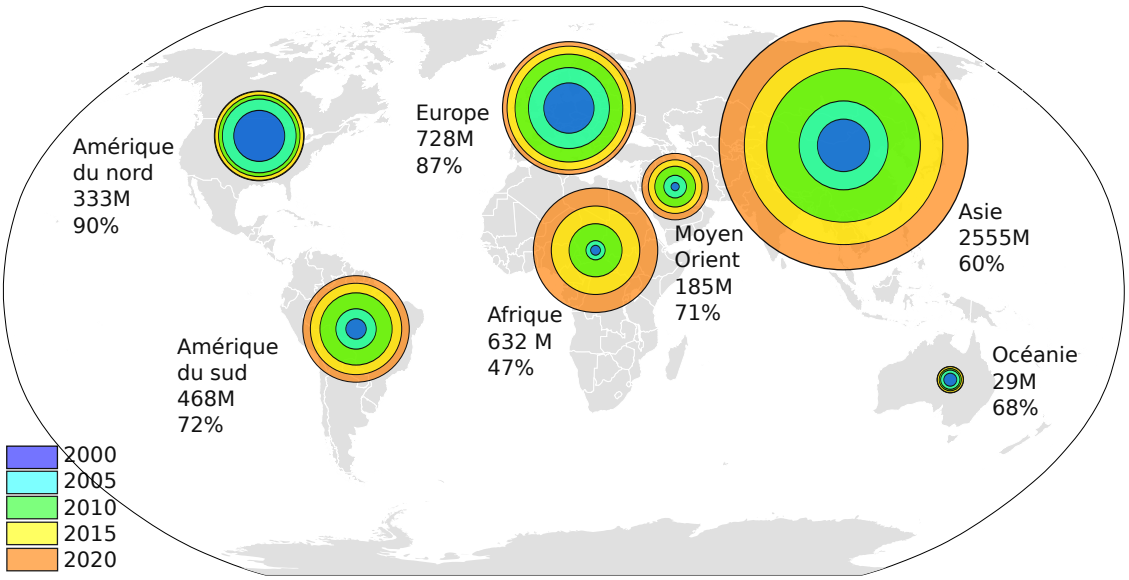


FIGURE 2.4 – Nombre d'internautes par continent en millions et en pourcentage

Ce sont les surfaces qui représentent le nombre d'internaute, donc un écartement constant entre les anneaux indique une progression quadratique.

source : Internet World Stats, 2005,2020

13. pour le NUA, www.nua.com, est *internaute* toute personne s'étant connectée durant les 3 derniers mois. Lorsque cette information n'est pas disponible, on estime le nombre d'internautes à 3 fois le nombre de personnes ayant un compte Internet.

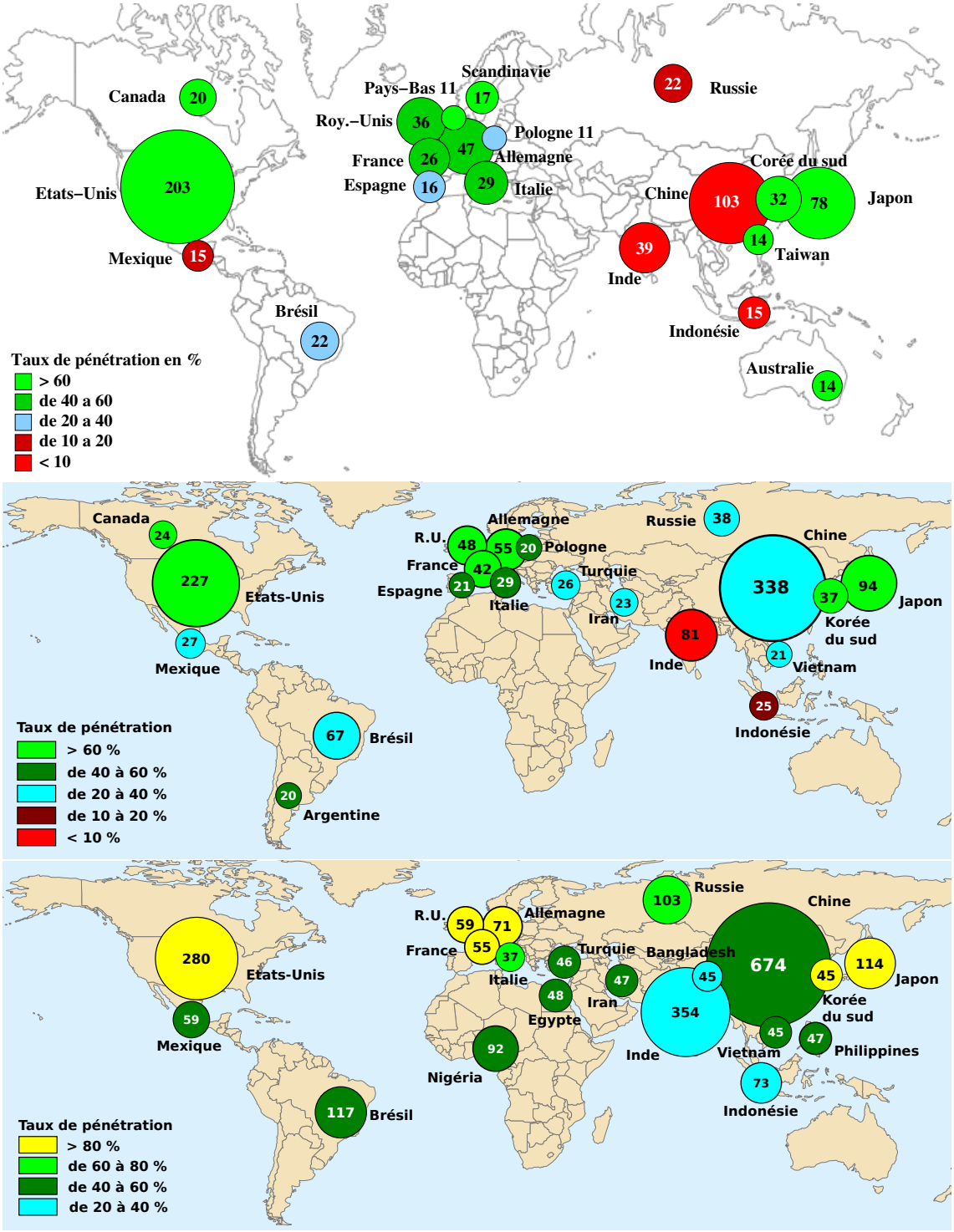


FIGURE 2.5 – Top 20 des pays ayant le plus d'internautes en 2005, 2009 et 2015 (en millions)

En 2020 le top20 correspond aux 20 pays les plus peuplés moins le Pakistan, l'Éthiopie et le Congo.

source : Internet World Stats

Un regard plus précis sur les taux de pénétration et leur évolution, cf figure 2.5, permet d'imaginer l'avenir. Ainsi la Chine, premier pays en nombre d'internautes a encore 25 % de sa population non connectée. L'Inde et l'Indonésie, géants démographiques, sont largement sous-représentés. À l'inverse, la Scandinavie où plus de 95% des habitants sont connectés à Internet, les États-Unis, le Japon, l'Australie n'ont plus beaucoup de progrès possible concernant le nombre d'internautes mais progressent rapidement sur d'autres aspects tout aussi importants comme la vitesse des connexions, le sans fils et les usages. Il est donc illusoire d'imaginer que les inégalités disparaissent.

L'évolution du nombre d'internautes en pourcentage de la population sur les 20 dernières années, figure 2.6, fait bien apparaître ces différences entre pays et l'histoire de chacun. On y voit que si les États-Unis ont bien commencé avant tout le monde, et tire logiquement l'avantage du premier arrivé, les suèdois les ont doublés en 1997. On voit aussi l'éveil de la Chine mais celui de l'Inde tarde. Notons aussi que les pourcentages doivent être rapportés au poids démographique des pays pour avoir une idée de la puissance de ces pays sur Internet. La Norvège ne peut pas espérer avoir la même influence sur Internet que les États-Unis ou la Chine, par contre elle peut tirer un avantage économique et culturel du fait que toute sa population est connectée.

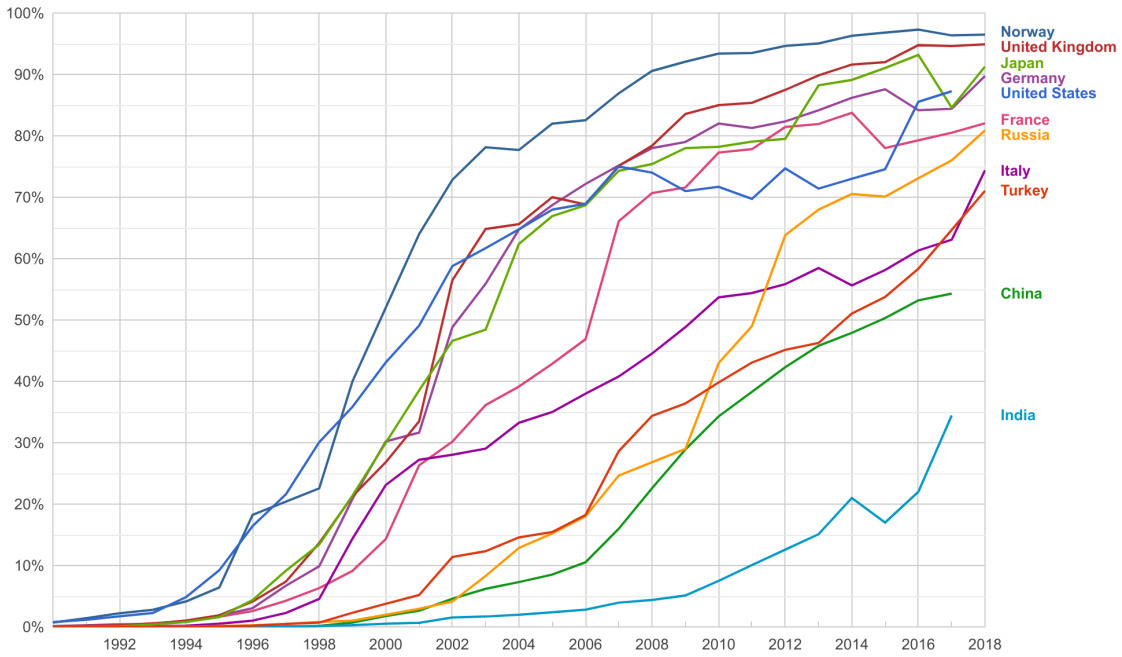


FIGURE 2.6 – Évolution du pourcentage d'Internautes dans différents pays
source : Google Data à partir de données de la Banque Mondiale (avr. 2020)

2.6.2 L'infrastructure

L'infrastructure d'Internet était plus facile à mesurer du temps où chaque ordinateurs avait son adresse IP. Avec la translation d'adresse [14], définie en 1992 et déployée les années suivantes, la

14. Le *Network Translation Address*, NAT, permet de cacher tout un réseau d'ordinateurs derrière une adresse IP qui fait le relais entre le monde extérieur et le réseau interne.

tache s'est compliquée. Puis l'Internet des objets est arrivé qui représente aujourd'hui la plus grande masse d'appareils connectés, appareils encore plus difficiles à compter.

Internet représentait fin 2015 :

— plus d'un millard d'ordinateurs connectées,
— 900 millions de sites web (dont seulement 170 millions de réellement actifs),
— 50 000 réseaux autonomes (Autonomous System ou AS).

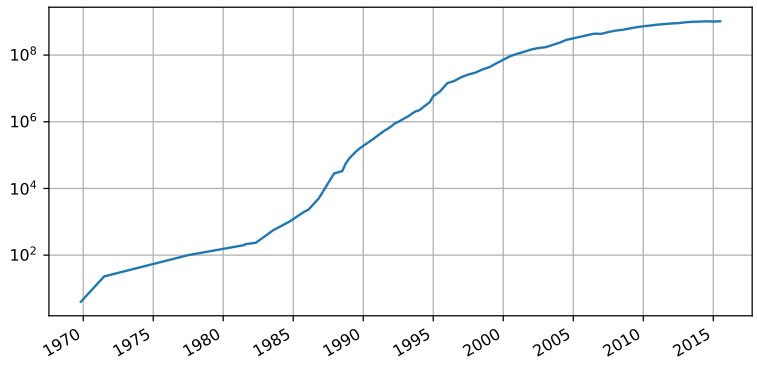


FIGURE 2.7 – Nombre de machines connectées à Internet
source : Internet Systems Consortium, 2015

Depuis, le nombre d'ordinateurs connectés ainsi que le nombre de site web sont stables. Les AS ont par contre plus que doublés.

À coté des ordinateurs de nouveaux appareils sont connectés à Internet. Le plus visible est l'ordiphone qui est passé devant les ordinateurs pour consommer de la bande passante sur Internet. En nombre d'appareils connectés, les ordiphones sont 6 fois plus nombreux que les ordinateurs en 2019.

Mais ce qui a totalement explosé, ce sont les objets connectés, qu'ils soient à domicile (domotique, capteur, majordome...) ou dans les entreprises.

Tout ces chiffres étaient inimaginable lorsque qu'Internet a été créé et pourtant ça marche. Ces appareils communiquent entre eux sans problème et de nouvelles applications voient le jour régulièrement. Ainsi l'arrivée de la vidéo (YouTube, la télévision, la vidéo-conférence) a augmenté de façon significative l'occupation de la bande passante et donc oblige à réadapter l'infrastructure, à poser de nouveaux câbles, mais rien qui n'affaiblisse Internet, au contraire.

Internet a prouvé que son schéma de fonctionnement décentralisé est solide et tient le passage à l'échelle [15].

Le seul problème d'Internet est lié à la seule partie centralisée à savoir la répartition des noms

15. c.a.d. peut voir le nombre d'utilisateurs multiplié plusieurs fois sans que cela n'ait d'influence sur le bon fonctionnement du réseau.

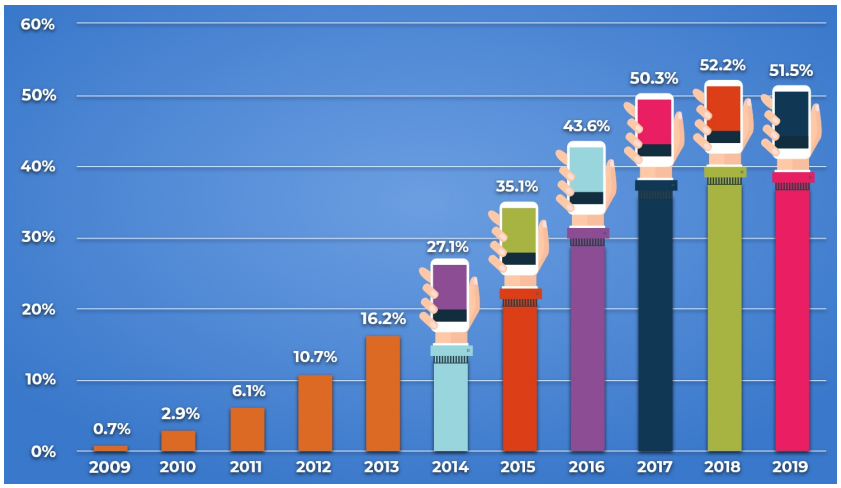


FIGURE 2.8 – Part des ordiphones dans le trafic sur Internet
source : Broadband Search, 2020

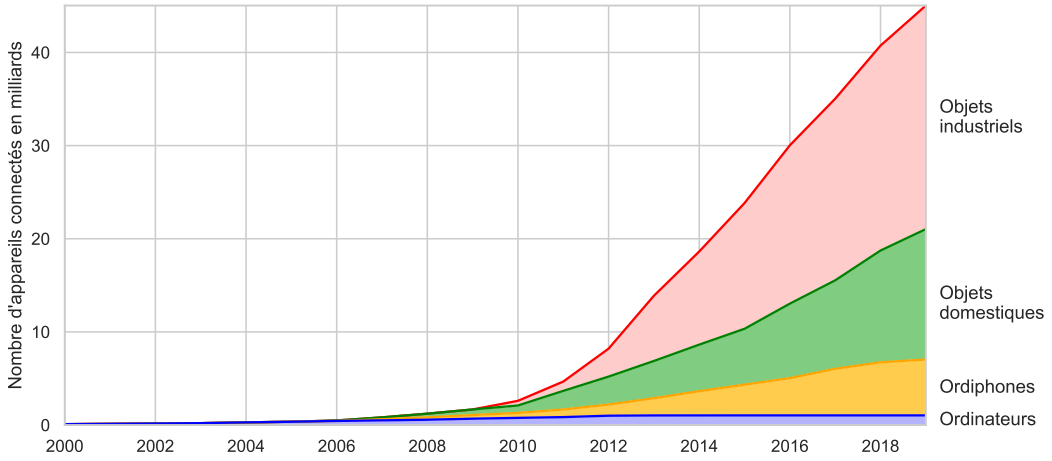


FIGURE 2.9 – Appareils connectés à Internet

de domaines et des adresses IP. Pour les noms de domaines le problème est politique [16] car il existe des solutions techniques pour créer autant de domaines qu'on le souhaite. Pour ce qui est de la répartition des adresses IP, la version 4 qui date des années 70, arrive à sa fin. Elle a été source d'une injustice évidente, les premiers arrivés ayant récupérer la part du lion. Heureusement la version 6 d'IP offre assez d'adresses pour tout le monde.

La pénurie d'adresses IP

La pénurie d'adresses IP concerne bien sûr les adresses IP du protocole IP version 4, IPv4, mis en place en 1983 et encore le plus utilisé par le grand public.

16. on abordera ce point dans le chapitre lié à la gouvernance d'Internet, en particulier page ...

Historiquement, les adresses IP ont été distribuées par paquets de 256 adresses, ce qu'on appellait une classe C, par paquets de 256×256, pour une classe B ou par paquets de 256×256×256 = 16 millions pour une classe A [17]. Bien sûr ce système tend à générer du gaspillage, le MIT ne va pas utiliser les 16 millions d'adresses qui lui sont attribuées.

Au début des années 90 les architectes de l'Internet ont compris qu'ils allaient droit dans le mur s'ils continuaient ce mode de distribution. La fin était prévue pour 1995. Aussi a-t-on arrêté de distribuer des classes entières pour ne plus distribuer que le strict nombre d'adresses nécessaires.

En même temps une astuce informatique, le NAT, a permis de cacher des parcs entiers de machines derrière une seule adresse IP, adresse donnée à la passerelle de cet ensemble de machines. Cela a permis de réduire très largement le besoin en adresse IP.

Grace à ces mesures, la date fatidique a été repoussée, mais pas si loin. En 2005, Geoff Huston de APNIC a estimé [18] qu'en 2012 l'organisme central en charge de la distribution des adresses, l'IANA, n'aura plus de blocs d'adresses à distribuer aux organismes régionaux, les RIR (c'est finalement arrivé en 2011). Pour les RIR cela varie, cf figure **??**, et la même personne estime la dernière adresse IPv4 libre sera utilisée en 2023.

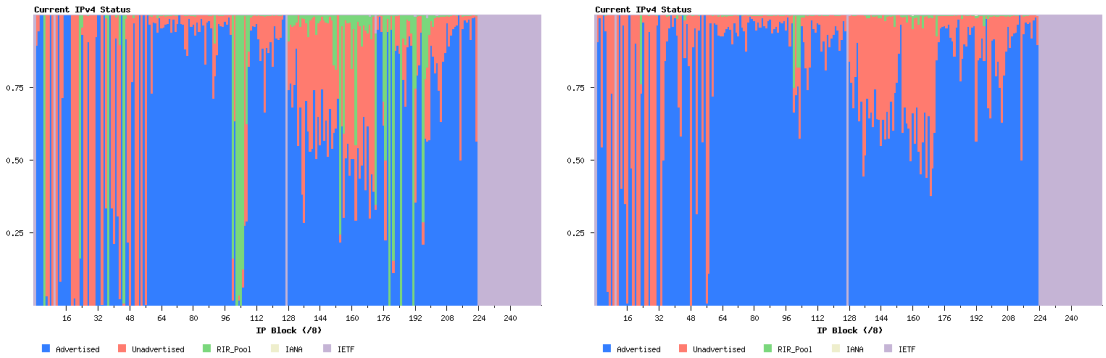


FIGURE 2.10 – Allocation des adresses IPv4 en 2011 et 2020
Chaque colonne est une classe A soit 16 millions d'adresses (2^{24})
Bleu est utilisé, rouge pris mais pas utilisé, vert libre, mauve réservé.
source : Geoff Huston – APNIC

Aujourd'hui il ne faut plus compter sur IPv4. Durant les dernières années les pays émergeants comme l'Inde et la Chine ont été les principaux bénéficiaires de l'attribution de nouvelles adresses IPv4, mais c'est fini et cela n'a pas suffit pour répondre à la demande.

La solution : IP version 6

La version 6 de IP a été créée en 1994 pour remédier à la pénurie d'adresses IPv4. Pour cela la nouvelle version a un système d'adressage qui permet de disposer de $2^{128} = 3,4\ 10^{38}$ adresses

17. en regardant dans le sens des adresses, une classe A ne fixe que le premier nombre, une classe B les 2 premiers et une classe C les 3 premiers. Ainsi le MIT possède la classe A 18.xxx.xxx.xxx et Jussieu la classe B 134.157.xxx.xxx.
18. cf http://www.apnic.net/community/presentations/docs/ipv6/20051031-v4-projections.pdf

ce qui fait 670 péta adresses par millimètre carré ou $10^{24}/m^2$ sur Terre. À première vue cela semble large, mais comme pour IPv4, chaque adresse ne sera pas attribuée puisqu'on attribue des paquets d'adresses par réseau et que rien ne dit que le réseau les utilisera toutes. Cela étant, si problème il y aura, on devrait avoir le temps de le voir venir.

En pratique, le déploiement d'IPv6 [19] a pris plus de temps que prévu initialement, essentiellement car IPv4 a résisté mais aussi pour des raisons économiques (pourquoi payer le passage en IPv6 tant qu'IPv4 fonctionne ?).

En 2023, les États-Unis, l'Europe et la Chine représentent environ 20 % chacun des adresses IPv6 déjà distribuées. Le progression d'IPv6 est constante et forte. L'administration américaine a basculé ses infrastructure sous IPv6 dès 2008, Vista, le système d'exploitation de Microsoft, utilise par défaut IPv6, Free propose à ses clients l'IPv6 depuis 2008 et en 2023 90 % des fournisseurs d'accès à Internet en France proposent IPv6 à leurs clients.

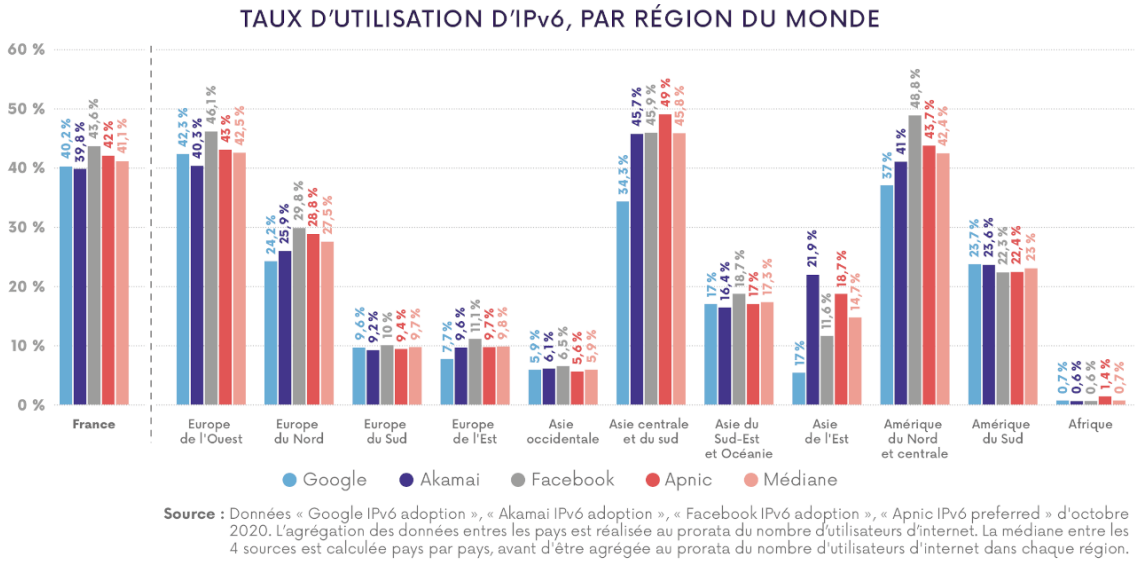


FIGURE 2.11 – Pourcentage de connexion en IPv6 vu par différents réseaux importants
source : Arcep, oct. 2020

2.6.3 Internet en France

La France n'a pas choisi une politique agressive de connexion à Internet. Contrairement à des pays comme la Suède ou le Canada qui considèrent l'accès à Internet quasiment comme une mission de service public, la France s'en remet entièrement au secteur privé pour le déploiement d'Internet auprès des particuliers. Cela s'est traduit par un blocage de la part de France Telecom (Orange) qui a tout fait pour que l'ADSL ne se développe pas, les connexions en RTC (modem payé à la minute) étant bien plus rentable, voir l'encart page **??**. Une fois que le verrou FT a sauté, l'ADSL s'est largement développé. Free au aussi bien aidé à ce déploiement avec sont offre [20] sur laquelle la concurrence a été obligée de s'aligner.

19. une fois fait, vous pouvez le tester sur http://ipv6.he.net/certification/
20. Combo Internet-Téléphone-Télévision pour 30 € par mois.

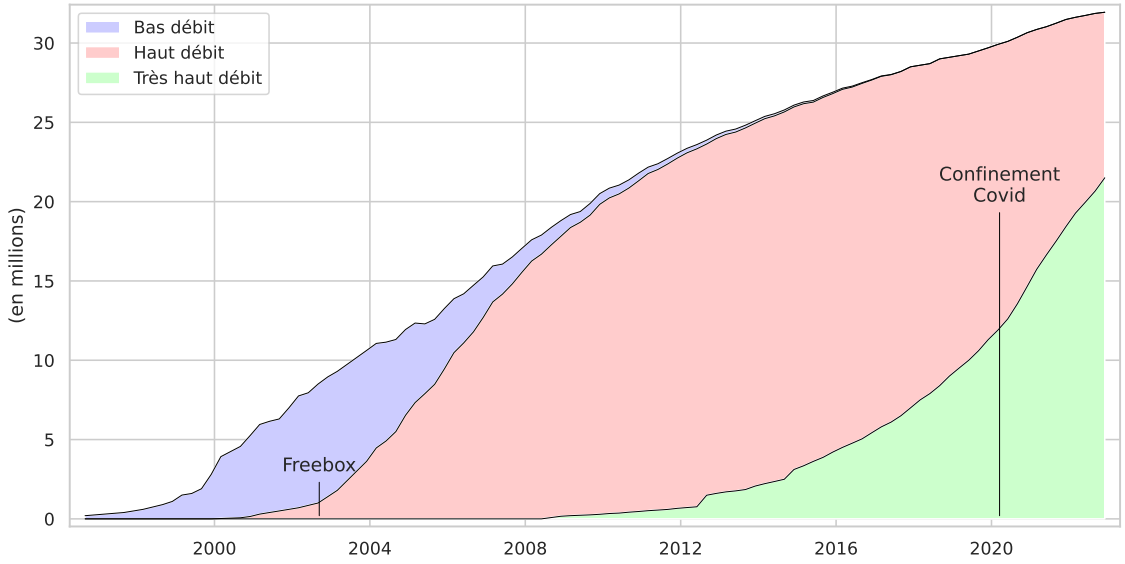


FIGURE 2.12 – Nombre d'abonements filaires à Internet en France
Le haut débit est l'ADSL à 95%. Le très haut débit est la fibre à 92 %.
Fin 2012, le très haut débit devient > 30 Mbps (contre > 50 Mbps avant).
source : AFA jusqu'en 2003 et ARCEP ensuite

La 3e vague concerne le très haut débit, plus de 30 Mbits, en particulier la fibre optique. Afin d'éviter une concurrence inutile, l'ARCEP, l'organisme de régulation, a décidé que les derniers mètres resteront accessibles à tous les fournisseurs d'accès internet, ce qui veut dire que l'opérateur ayant posé la fibre dans une zone n'en a pas l'accès exclusif. Si Bouygues pose toute la fibre dans un immeuble, Free peut quand même y avoir des clients, dans ce cas Free paie une redevance à Bouygues. Il s'agit du même mécanisme que pour l'ADSL dont l'infrastructure appartient à Orange mais qui peut être utilisée par tous les FAI.

Le résultat n'a pas été à la hauteur des espérances dans le domaine du très haut débit (cf figure 2.13). Cela peut être dû à une mauvaise offre ou au fait que la France étant très bien équipée en ADSL, les utilisateurs n'ont pas jugés bon de passer à la fibre. Cela étant les choses évoluent et début 2023, le nombre d'abonnés à la fibre était le double de ceux à l'ADSL. Notons que les vieux câbles en cuivre de la téléphonie vont disparaître en 2030 et donc l'ADSL avec eux.

Concernant l'équipement de foyers, là encore les choses n'ont plus rien à voir avec l'an 2000. Accéder à Internet quotidiennement est devenu la norme. La figure 2.14, montre cette évolution. Notons que les valeurs bizarre pour les ordinateurs en 2021 puis en 2002 sont dues aux questions posées. En 2021, pendant la période du confinement, à la question "Avez vous accès à un ordinateur à la maison ?", les enquêteurs soupçonnent que de nombreuses personnes ayant un ordinateur à la maison mais occupé par une autre personnes ont répondu non. En 2022, les enquêteurs ont changé la question pour spécifier "Avez vous accès à un ordinateur personnel ou professionnel" d'où les chiffres qui augmentent significativement.

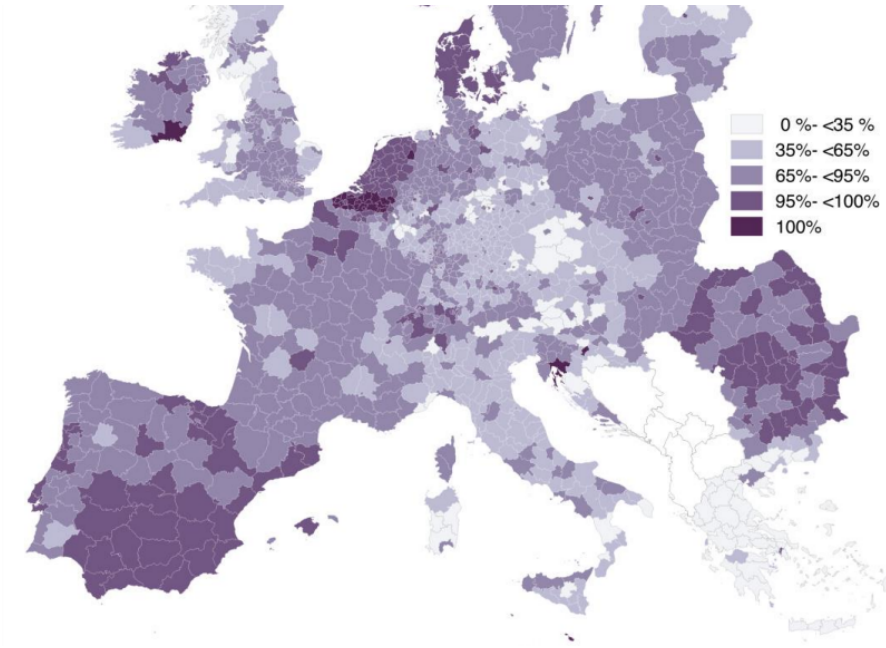


FIGURE 2.13 – Couverture de l'accès au très haut débit en 2023 (fibre + cable 1Gb)
source : Broadland Coverage in Europe 2024

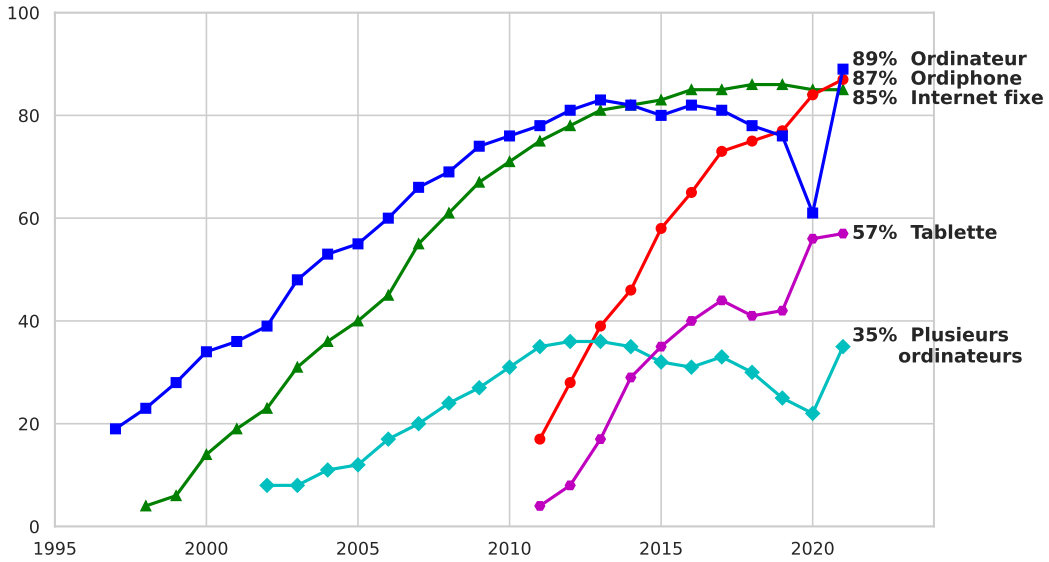


FIGURE 2.14 – Taux d'équipement à domicile (en %)
Proportion d'individus âgés de 12 ans et plus (18 ans et + avant 2003)
source : CREDOC & ARCEP

m.à.j. sur http://www.ricou.eu.org/e-politique.html

L'infrastructure en France

L'accès à Internet repose donc sur les fournisseurs d'accès privés. Avec l'offre dite *triple-play* à un tarif en rupture avec ceux de la concurrence, Free a probablement fait plus pour apporter Internet dans les foyer que n'importe quel autre entreprise ou administration [21]

Les principaux fournisseurs d'accès français, FAI, sont par ordre d'abonnés avec en sous-item les concurrents rachetés avec la date de l'achat ou de la fusion entre parenthèses :

- Orange, ex Wanadoo, créé en 1996 par France Télécom à partir du rachat de petits FAI
- SFR Fibre (anciennement Numéricable-SFR)
  - (2014) Numéricable (groupe Altice) acquière SFR pour 13 G€
    - (2007) Numéricable, résultat de la fusion entre NC Numéricable et Noos
      - (2006) NC Numéricable
        - (2005) France Télécom Câble
  - (2014) SFR
    - (2008) Neuf Cegetel, absorbé par SFR qui achète les parts qui lui manquait
      - (2007) Tele2 France, filiale de l'opérateur privé suédois,
      - (2007) Club Internet, créé en 1995 par le groupe Lagardère, acheté en 2000 par T-Online, la filiale Internet de Deutsche Telekom,
      - (2005) Cegetel, créée par Vivendi (propriétaire de SFR) à partir d'AOL-France rachetée en 1998
      - (2005) 9 Telecom, crée en 1997
- Free, le trouble fête crée en 1999
  - (2008) Alice la filiale de l'opérateur historique Italien
    - (2005) Tiscali (section Internet),
      - (2001) Liberty Surf, avec un business plan basé sur le gratuit,
      - (2001) Infonie, créée en 1995 et passé par Belgacom,
- Bouygues Telecom le dernier arrivé en 2008
- des tout petits : OVH, Nerim, FDN

L'époque des rachats semble finie avec aujourd'hui quatre FAI qui contrôlent le marché. De tous les FAI indépendants créés durant les années 90 seul Free a survécu pour devenir un grand. Les monstres des télécoms que sont Orange, Bouygues et SFR ont, tôt ou tard, su attraper le train de l'Internet. Enfin, le monde de la télévision par câble a fusionné et fusionné pour arriver aujourd'hui à un seul représentant assez important pour survivre dans un monde où l'acces à la télévision est devenu le même que celui à Internet et au téléphone. Le rachat en 2014 de SFR par Numéricable porte surtout sur l'aspect téléphone portable mais aura aussi un impact sur la partie Internet.

Si ces grands FAI couvrent l'immense majorité des connexions des particuliers à l'Internet, il existe d'autres réseaux, résultats d'initiatives locales ou dédiés à des niches. On les trouve

21. Free serait le champion parfait s'il n'avait la volonté de casser la neutralité du réseau, cf le chapitre sur la gouvernance d'Internet.

dans un grand nombre de villes, de départements ou de régions le plus souvent dans le but d'offrir localement un accès à Internet aux entreprises et aux particuliers, lorsque les opérateurs classiques font défaut.

Enfin pour rendre justice à l'État, soulignons la mission assigné en 2001 à Arteria, filiale du Réseau de Transport de l'Electricité, RTE, elle même filiale d'EDF.

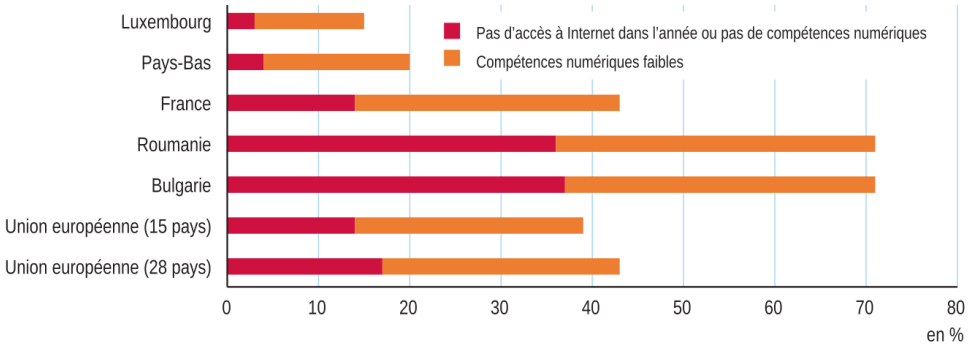
L'idée est simple mais a failli être comprise trop tard. Si l'État met en place un squelette de réseau au niveau national, on parle de dorsales, alors il ne restera plus qu'aux régions puis aux villes a s'y raccorder pour avoir un réseau informatique national. Pour les dorsales il y avait bien le réseau de France Télécom mais cette derniére devenant privée, cela n'était pas possible. Cégétel ayant récupéré le réseau de la SNCF car en effet il y a des fibres optiques qui courent le long des voies ferrées, ce réseau n'était plus disponible non plus. Aussi l'État à demandé au dernier réseau restant, celui d'EDF. de remplir ce rôle de squelette au niveau national pour permettent aux collectivités locales de se raccorder à un réseau très haut débit.

Aujourd'hui Arteria développe son réseau, le long du réseau électrique, et le propose aux collectivités locales, aux opérateurs téléphoniques et aux entreprises.

2.6.4 La fracture numérique

Avant la fracture numérique soulignait la séparation entre ceux qui avaient accès à un Internet et les autres. Cette fracture existe encore, en particulier dans certains pays mais on peut dire qu'elle est résorbée en occident. La raison pour laquelle certains n'ont pas Internet n'est plus le manque d'offre.

Aujourd'hui la fracture numérique concerne la capacité à utiliser Internet et, plus largement, le numérique.



Lecture : en 2017, au Luxembourg, 3 % de la population n'a pas accédé à Internet pendant l'année ou n'a pas de compétences numériques, et 12 % a des compétences numériques faibles.

FIGURE 2.15 – Illectronisme : Incapacité à utiliser Internet et le numérique
source : sondage ICT Survey auprès des 16 à 74 ans – 2017

On sent bien qu'il ne suffit pas d'avoir accès à Internet pour en tirer parti pleinement. Pour beaucoup une formation à l'outil Internet serait nécessaire pour savoir trouver l'information,

accéder aux services publics, remplir des formulaires administratifs en ligne, envoyer un courriel, payer ses factures, gérer les problèmes, faire ses devoirs scolaires, ne pas se faire avoir... D'après un sondage de l'INSEE de 2019 [22] un français sur quatre ne sait pas s'informer, un sur cinq est incapable de communiquer via Internet.

La crainte de la technologie associé à l'effort à faire pour acquérir les bases, freinent certaines personnes, en particulier les personnes âgés (53 % des plus de 75 ans n'ont pas accès à Internet d'après le même sondage). Dans un monde qui change, où l'administration se dématérialise et les administrations physiques ferment, ce rejet d'Internet a un coût de plus en plus élevé.

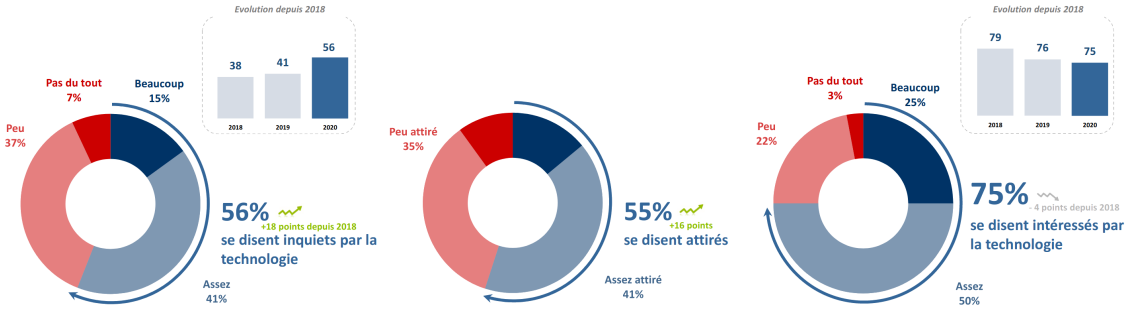


FIGURE 2.16 – Quel est votre rapport aux technologies ?
source : sondage IFOP 2020

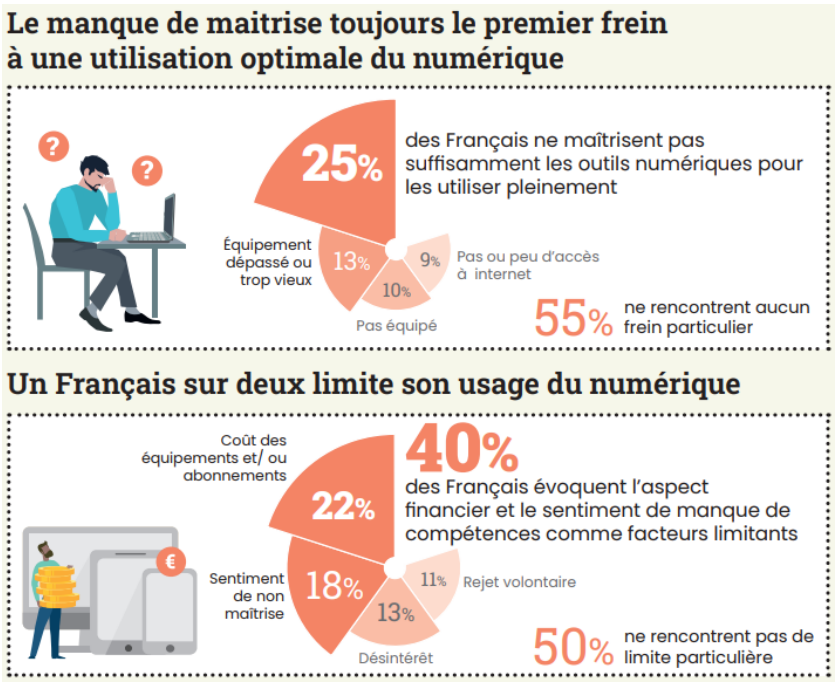


FIGURE 2.17 – Fracture numérique en France
source : ARCEP - Baromètre du numérique 2024

22. Insee Première n°1780 d'octobre 2019

Déjà en 2002, le Conseil Général de Technologies de l'Information indiquait dans son rapport « Rôle et responsabilité des pouvoirs publics dans la lutte contre la fracture numérique » :

> *S'il est essentiel que chaque citoyen ait accès aux technologies de l'information, c'est, d'une part, parce qu'elles agissent sur la qualité et la productivité du travail et le volume d'emplois et, d'autre part, parce que, utilisées de façon adéquate, elles sont un facteur de cohésion sociale et d'amélioration des conditions de vie déterminant. S'il est donc un domaine où la préoccupation sociale et l'intérêt économique convergent sans ambiguïté, c'est bien celui de la lutte contre la fracture numérique.*

Chapitre 3

La gouvernance de l'Internet

Qui dirige Internet ?

La réponse à cette question se trouve dans la structure technique d'Internet et dans l'usage qu'on en fait.

En tant qu'union de réseaux, chaque réseau est libre de s'y connecter à condition d'utiliser TCP/IP et d'obtenir des adresses IP pour ses machines. Il est probable qu'il lui faille aussi payer la connexion auprès d'un fournisseur d'accès à Internet. Les utilisateurs de ce réseau sont libres d'y faire ce qu'ils veulent tant qu'ils respectent les lois de leur pays voire les lois d'autres pays si leur activité sur Internet déborde de leur pays. Enfin, il leur est vivement recommandé de respecter les us et coutumes de l'Internet.

On voit donc apparaître différentes contraintes. L'aspect technique impose l'utilisation de TCP/IP ainsi que celle des protocoles applicatifs comme celui du courrier électronique, du web, des forums de discussion, etc. La mise en place de ces normes est la manifestation la plus ancienne d'un pouvoir sur Internet. En fait, il s'agit d'un pouvoir consensuel, ces normes étant définies en bonne intelligence par l'ensemble des personnes concernées par ces aspects techniques. Aujourd'hui des organismes, ouverts à tous pour la majorité d'entre eux, continuent ce travail de définition et de normalisation des protocoles. Ils forment ce qu'on appellera le pouvoir technique.

L'utilisation du protocole TCP/IP impose d'avoir une adresse IP pour être joignable. Bien sûr deux machines connectées à Internet ne doivent pas avoir la même adresse sous peine de ne pouvoir les différencier. Aussi un organisme a été créé pour distribuer ces adresses et tenir à jour une base de donnée qui indique qui possède quelles adresses. Cette base est unique et forme le nœud central du fonctionnement d'Internet avec celle des noms de domaines qui sont l'équivalent des adresses IP en langage humain. Les adresses IP et les noms de domaine étant gérés par un même organisme, qui dispose ainsi du pouvoir d'arrêter Internet ou des parties d'Internet en les rendant injoignables, certains considèrent que cet organisme dirige Internet. On parlera ici plutôt du pouvoir d'adressage.

S'il faut payer pour se connecter, la notion de pouvoir économique entre en jeu avec en particulier les aspects de concurrence. Et puisque Internet est devenu aussi un vecteur commercial,

là encore le pouvoir économique entre en jeu. La jeunesse de ce pouvoir sur Internet fait qu'il y est encore moins puissant qu'il ne l'est dans nos sociétés occidentales, mais cette différence s'atténue. L'attaque de la société VeriSign contre le pouvoir technique et d'adressage en est une illustration (voir encart page 119). Aujourd'hui les sociétés comme Google ou Free en France, phares de l'Internet à travers leurs innovations et le large public qu'elles touchent, témoignent de l'importance de l'économie comme moteur du développement de l'Internet.

Enfin, puisque tout utilisateur majeur est responsable de ses actes sur Internet comme ailleurs, le pouvoir législatif de chaque pays impacte localement sur le fonctionnement de l'Internet. Internet n'est pas une zone de non droit où un internaute français pourrait exprimer des propos hors la loi, comme des propos racistes. Sa nature internationale et le fait que de tels propos sont autorisés dans d'autres pays ne change rien à la porté de la loi française. Mais dans d'autre cas Internet rend les lois françaises difficiles à appliquer. Ainsi la loi imposait à toute publication d'avoir un directeur de la publication déclaré auprès du procureur de la République, donc à chaque internaute possédant une page Web de se déclarer auprès du procureur de la République. Cette loi prévue pour les médias classiques n'était plus applicable dans le cas d'Internet et a dû être révisée. Enfin des lois nationales peuvent influencer globalement le fonctionnement d'Internet. La brevetabilité des logiciels en est l'illustration la plus flagrante. Il est actuellement interdit de breveter un logiciel [1] et plus globalement une idée abstraite comme un théorème de mathématique en Europe. Aux Etats-Unis et au Japon les brevets logiciels sont autorisés mais tout laisse à penser qu'ils ne sont pas utilisés pleinement dans la crainte de faire fuir les nouvelles entreprises innovantes en Europe. Cette interdiction européenne est aussi la plus forte protection du monde des logiciels libres qui n'entrent pas dans la logique commerciale et donc des brevets. Que l'Europe change d'avis et les logiciels libres risquent de disparaitre et, avec eux, des pans entiers de l'Internet actuel. On voit donc que le pouvoir politique, à travers ses lois nationales, pèse aussi sur le fonctionnement d'Internet [2].

Reste l'autre pouvoir politique, celui qui intervient directement auprès des autres pouvoirs cités. Celui là appartient principalement aux Etats-Unis.

Quatre pouvoirs pour un hyper-espace

On a donc non pas un gouvernement de l'Internet mais quatre pouvoirs qui contribuent au bon fonctionnement de l'Internet :

- Le pouvoir technique gère la stabilité et le développement technique d'Internet,
- le pouvoir d'adressage distribue les adresses IP et les noms de domaine,
- le pouvoir économique impulse les usages et pousse les autres à s'adapter,
- le pouvoir politique travaille à maîtriser le plus possible ce média mis à la disposition des citoyens.

Bien sûr ces pouvoirs ne représentent qu'une vision grossière. Chaque pouvoir est composé de différents organismes qui parfois influencent aussi d'autres pouvoirs. Une représentation de la gouvernance de l'Internet ne peut qu'être simplifiée et tronquée. La simplification usuelle

1. Un logiciel est protégé par le droit d'auteur comme l'est une œuvre littéraire.
2. Dans d'autres pays, comme la Chine, le poids du politique sur Internet est nettement plus visible en particulier à cause de la censure.

consiste à se restreindre à l'interaction entre les organismes en charge des aspects techniques en y ajoutant, quand c'est possible, ceux qui contrôlent ou influencent ces organismes. Cela revient à limiter l'Internet à un outil en oubliant son aspect monde virtuel lequel est d'avantage contrôlé par les usages et les lois.

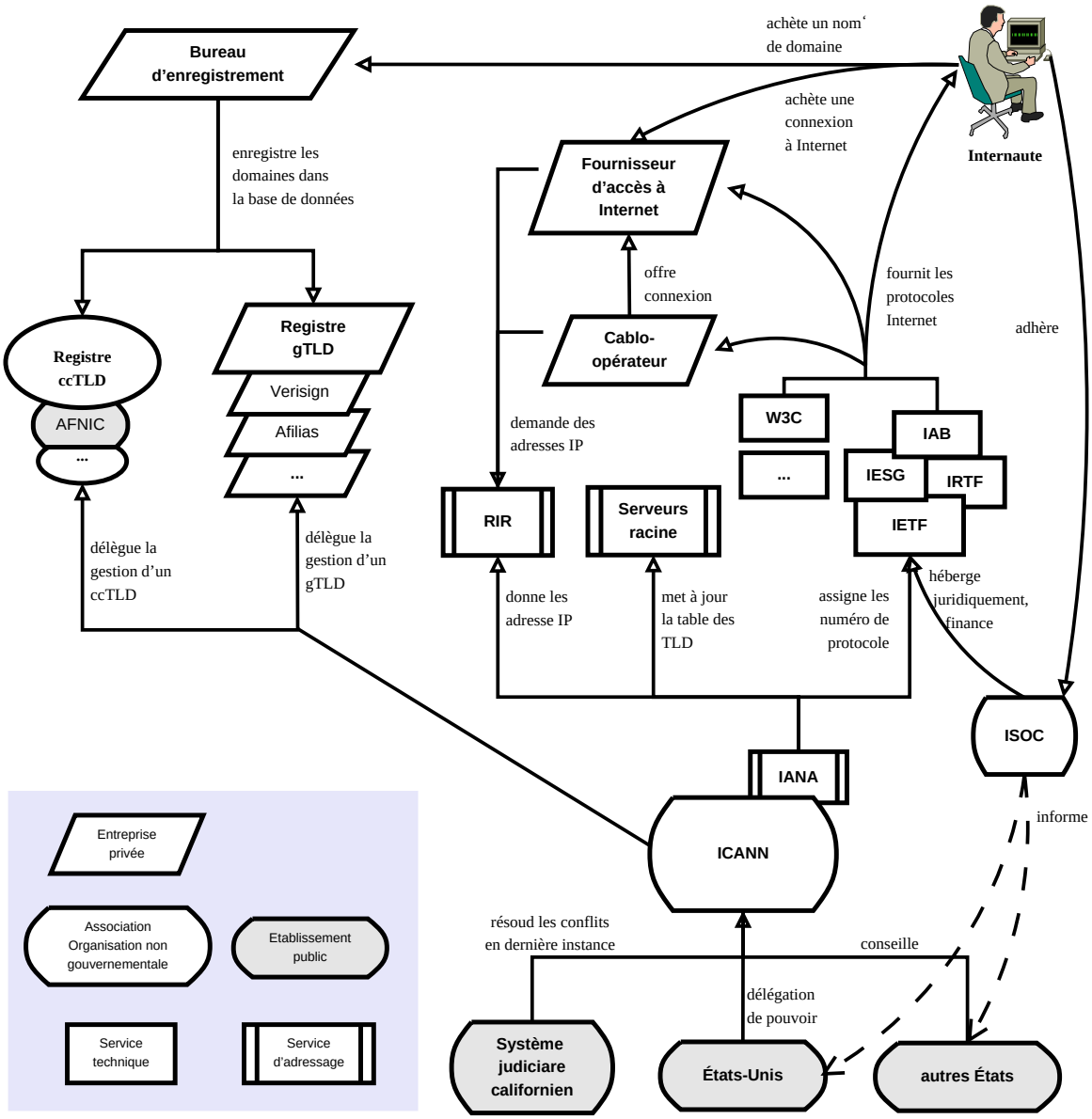


FIGURE 3.1 – Gouvernance de l'Internet : intervenants et relations

L'ensemble de ces organismes et leurs relations sont étudiés dans les chapitres qui suivent.

3.1 Le pouvoir technique

À partir du moment où le réseau a offert des possibilités d'applications et d'interconnexion, il a été nécessaire de se mettre d'accord sur des protocoles permettant l'interopérabilité. Aussi des groupes de travail, Working Group – WG, ont été créés en même temps que l'ancêtre d'Internet, ARPANET. Ces groupes de travail sont devenus des groupes de travail sur Internet puis des organismes plus ciblés ont été créés. Ainsi l' Internet Configuration Control Board (ICCB), mis en place en 1979, a eu pour mission de conseiller le responsable du DARPA, fondateur et principal responsable à l'époque du réseau, sur les aspects techniques. Ce comité, devenu aujourd'hui l'Internet Architecture Board, est toujours la référence technique de nos jours même si la DARPA ne gère plus Internet.

De leur coté les groupes de travail se sont scindés en deux parties avec d'un coté les groupes de travail en rapport avec la recherche, rassemblés aujourd'hui au sein de l'IRTF, et ceux en rapport avec l'écriture des protocoles, les RFC [3], rassemblés au sein de l'IETF.

Enfin, devant l'importance du Web, le World Wide Web Consortium a été créé en 1994 pour gérer l'évolution des protocoles du Web.

Depuis, aucun nouvel organisme technique n'a été créé (l'ICANN crée en 1998 entre dans la catégorie organisme d'adressage qu'on a séparé en introduction).

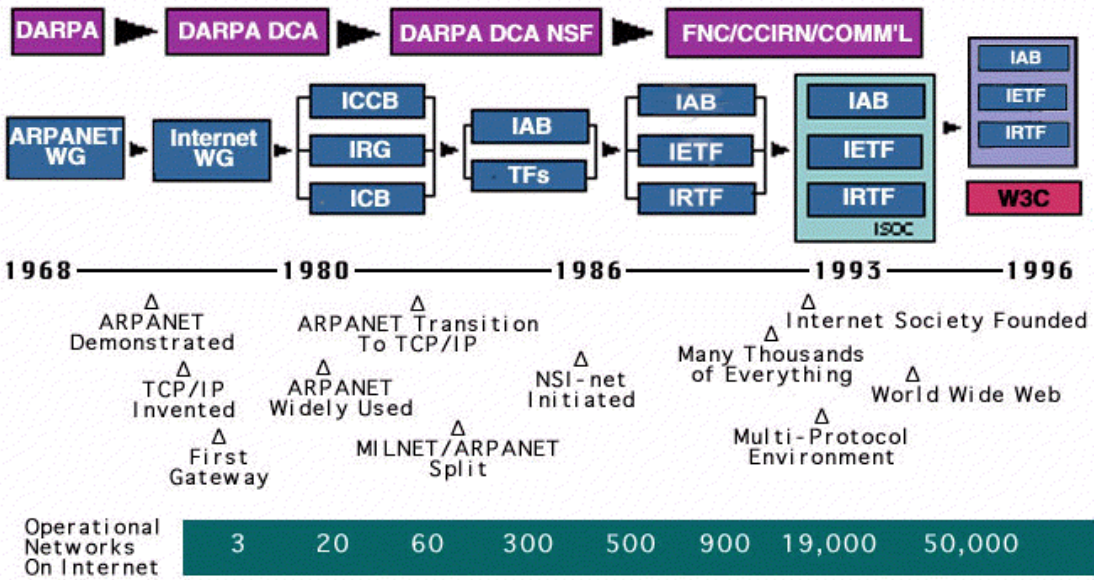


FIGURE 3.2 – Histoire des organismes techniques de l'Internet de la création à 1996
source : ISOC

3. Les RFC sont de facto les lois techniques de l'Internet.

3.1.1 L'IETF et l'IESG, les protocoles et l'évolution technique

> *The Internet Engineering Task Force is a loosely self-organized group of people who contribute to the engineering and evolution of Internet technologies. It is the principal body engaged in the development of new Internet standard specifications. The IETF is unusual in that it exists as a collection of happenings, but is not a corporation and has no board of directors, no members, and no dues.*
> *Extrait du Tao, http://edu.ietf.org/tao*

L'Internet Engineering Task Force est le témoignage du fonctionnement de l'Internet des débuts. Initialement sans statut [4], l'IETF est un ensemble cohérent de groupes de travail [5] qui travaillent à la création des protocoles et règles de l'Internet (les RFC, Request for comments). Ces groupes sont ouverts à tout le monde et fonctionnent principalement via des listes de diffusion où les points sont débattus jusqu'à obtention d'un consensus.

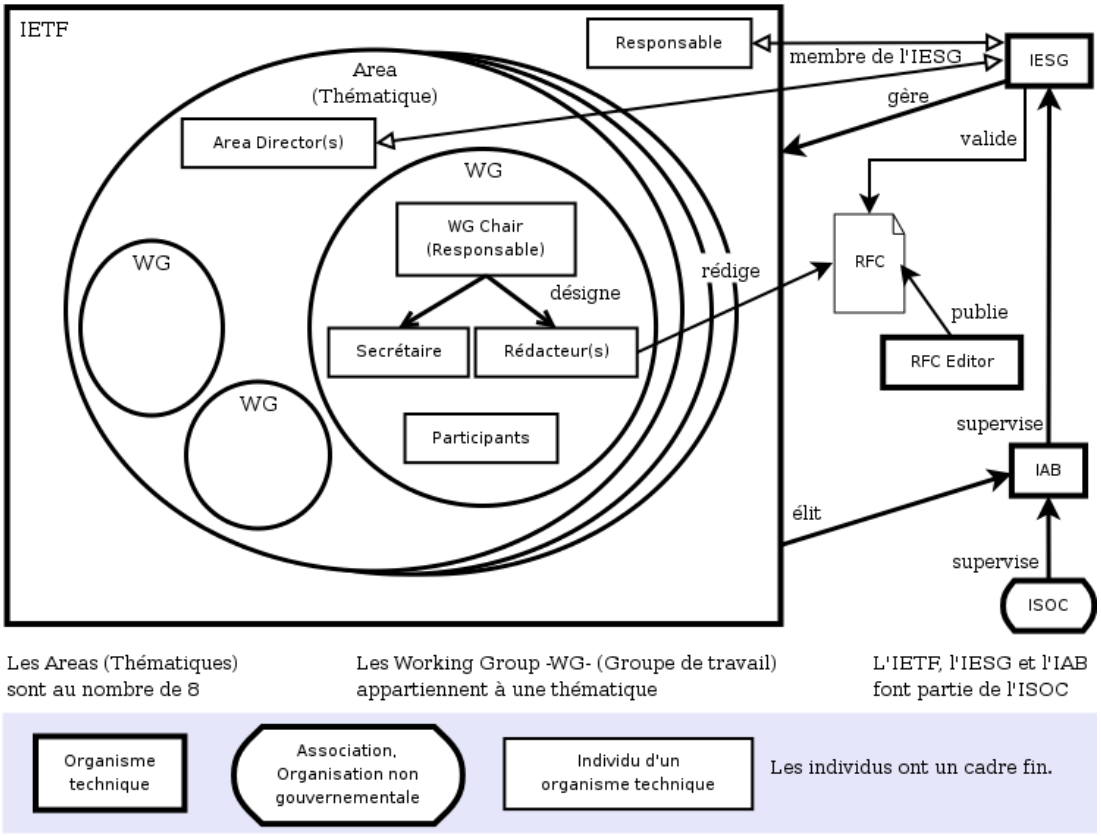


FIGURE 3.3 – Fonctionnement du pouvoir technique de l'Internet lié aux RFC

On notera figure 3.3, l'existence de rédacteurs au sein des groupes de travail. Ils sont en charge de l'écriture du RFC et d'incorporer les résultats des discussions. Leur travail, le RFC, sera ensuite publié par l'éditeur des RFC, lequel est aujourd'hui une équipe liée à l'IETF.

4. aujourd'hui l'IETF fait partie de l'association des utilisateurs d'Internet, l'ISOC
5. La liste des groupes de travail est disponible sur http://www.ietf.org/html.charters/wg-dir.html.

La création d'un groupe de travail et son interaction avec les autres et plus globalement avec l'IETF est définie dans la RFC 2418, "IETF Working Group, Guidelines and Procedures". Chaque groupe de travail doit être lié à l'une des thématiques existantes au sein de l'IETF. Il doit avoir un objet précis qui n'entre pas en conflit avec les groupes existants. Un groupe peut disparaitre lorsqu'il a accompli sa mission ou s'il n'a plus de raison d'être.

Les thématiques sont :

— Internet (IPv6, DNS...)
— Opérations et gestion du réseau (Surveillance du réseau, configuration...)
— Applications en temps réel et Infrastructure (Téléphonie sur IP, transport de la vidéo...)
— Routage (OSPF, Routage sur réseaux mobiles...)
— Sécurité (PKI, Open PGP, Kerberos...)
— Transport (NFS, Mesure de la performance des paquets IP,...)

Si le fonctionnement de l'IETF est essentiellement basé sur le consensus, il existe quand même une structure gouvernante chargée de trancher en cas de conflit et plus généralement de prendre in fine les décisions ou plus généralement de valider les décisions prises par les groupes de travail. Cette structure gouvernante de l'IETF est l'Internet Engineering Steering Group (IESG). Elle est composée des responsables des thématiques, du responsable de l'IETF et d'agents de liaison avec les autres organismes techniques de l'Internet.

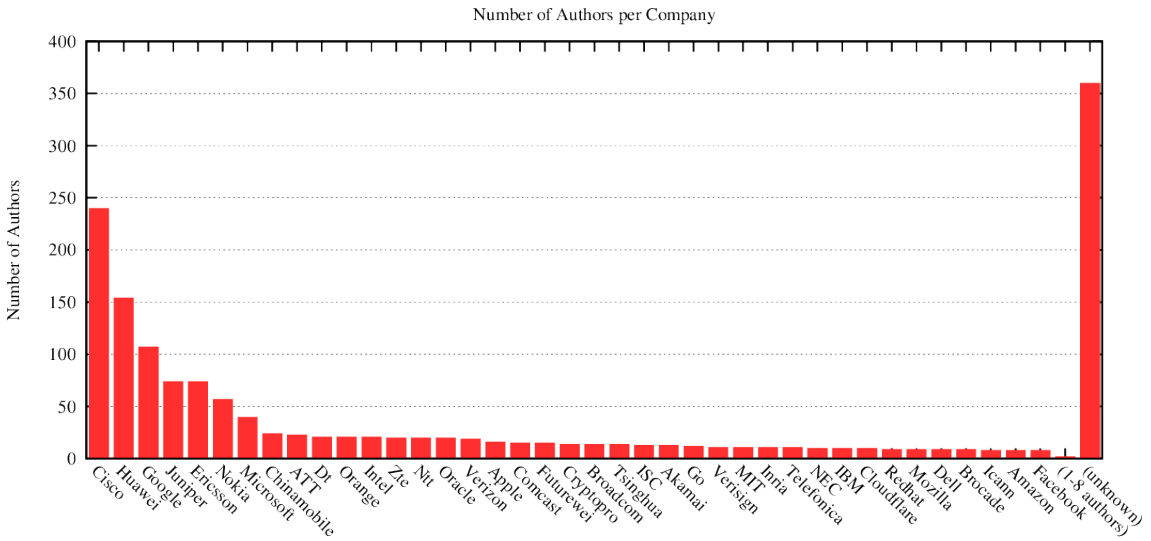


FIGURE 3.4 – Nombre de rédacteurs de RFC récents par entreprise
source : http://www.arkko.com/tools/stats/rerfc_companydistr.html – 2024

Officiellement les participants ne représentent qu'eux-même, leur affiliation n'étant donnée qu'à titre d'information. Seules l'expertise et la qualité des interventions interviennent dans la construction d'une RFC. Mais l'impact des RFC sur certaines entreprise est tel, qu'il n'est pas surprenant qu'elles déléguent du personnel pour y participer pleinement et pousser les RFC dans leur sens (ou au moins se tenir informé). On note figure 3.4 que les les grands constructeurs de matériel lié à l'Internet sont bien représentés.

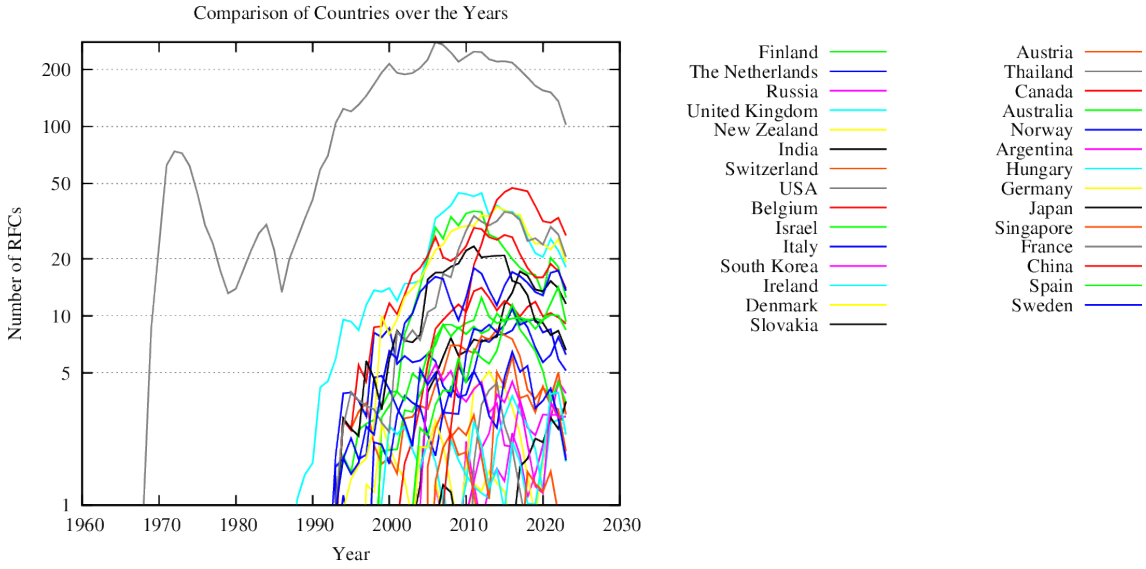


FIGURE 3.5 – Nombre de rédacteurs des RFC par pays
source : https://www.arkko.com/tools/recrfcstats/companydistr.html – 2024

Proposition indépendante de RFC

Il existe une seconde voie pour publier une RFC qui est la soumission indépendante. En premier la soumission doit commencer par la publication d'un document appelé "Internet Draft" (brouillon) afin de pouvoir être étudié par l'IETF. Ensuite, la RFC doit être soumise au RFC Editor. Si le document respecte les règles éditoriales, il sera soumis à l'IESG pour vérifier qu'il n'interfère pas avec des travaux en cours de l'IETF, et alors seulement il pourra être publié.

3.1.2 L'IAB, les grands architectes de l'Internet

Au-dessus de l'IESG, se trouve l'Internet Architecture Board. Ce comité composé de 13 membres élus par l'IETF et du responsable de l'IETF, est l'autorité supérieure pour tous les aspects techniques de l'Internet. L'IAB

- supervise le travail des IETF et IRTF
- nomme les membres de l'IESG sur proposition des groupes de travail
- règle les litiges au sein de l'IETF et de l'IRTF
- publie les RFC soumis par les groupes de travail (cet aspect est délégué au RFC Editor qui a longtemps été Jon Postel)
- résout les problèmes en dehors des compétences de l'IETF et de l'IRTF
- sert d'intermédiaire entre les internautes représentés par l'ISOC et l'IETF

Ainsi l'écriture des RFC fait intervenir 3 organismes qui se contrôlent les uns les autres (cf figure 3.3). Un 4^{e} organisme intervient dans ce fonctionnement en tant qu'entité morale et structure administrative hébergeant ces 3 organismes : il s'agit de l'association des internautes, l'ISOC. Cette dernière, qui chapeaute l'IAB, ne peut intervenir que sur des aspects administratifs.

3.1.3 L'IRTF, la recherche

L'Internet Research Task Force est le pendant de l'IETF pour le long terme. Elle se consacre à la recherche dans les domaines des protocoles, des applications, de l'architecture et des technologies.

Le fonctionnement de l'IRTF est semblable à celui de l'IETF avec l'IRSG qui gouverne sous la supervision de l'IAB.

3.1.4 Le W3C, tout pour le Web

Avec le succès du Web, HTML est devenu le premier langage dont la puissance économique aurait pu mettre à mal Internet. Lorsque l'équipe de Mosaic, le navigateur qui a rendu convivial le Web, est partie créer Netscape, elle a rapidement voulu «embellir» le langage HTML et a profité de sa situation dominante pour ajouter des mots clés sans prendre l'avis des comités en charge de ce langage. D'autres navigateurs allaient dans d'autres directions et avec l'arrivée du navigateur Internet Explorer de Microsoft en 1995, on pouvait craindre d'avoir rapidement des langages HTML différents voire incompatibles. On risquait d'avoir le Web Netscape, le Web Microsoft et le Web HTML pur, chacun avec ses navigateurs incapables de comprendre les sites des autres.

Aussi le World Wide Web Consortium a été créé en 1994 par Tim Berners-Lee au sein du MIT, avec l'INRIA et l'université de Keio, pour éviter cette débâcle en poussant les acteurs du Web à travailler en bonne intelligence. Il a permis, avec le concours de l'IETF, de faire évoluer HTML rapidement afin de satisfaire les besoins de chacun. En ce sens

le W3C se rapproche de l'IETF, mais contrairement à l'IETF, le W3C est un club fermé dont le prix du ticket d'entrée est très élevé, entre 7 800 et 68 000 euros [6] par an suivant le type d'organisme [7].

Aujourd'hui le W3C travaille sur les nouveaux protocoles et techniques du Web et de ce qui s'y attache :

6. en 2013
7. une adhésion individuelle est à 6 500 euros, cependant il est possible de participer aux travaux du W3C en étant invité ou d'y participer partiellement sans adhérer.

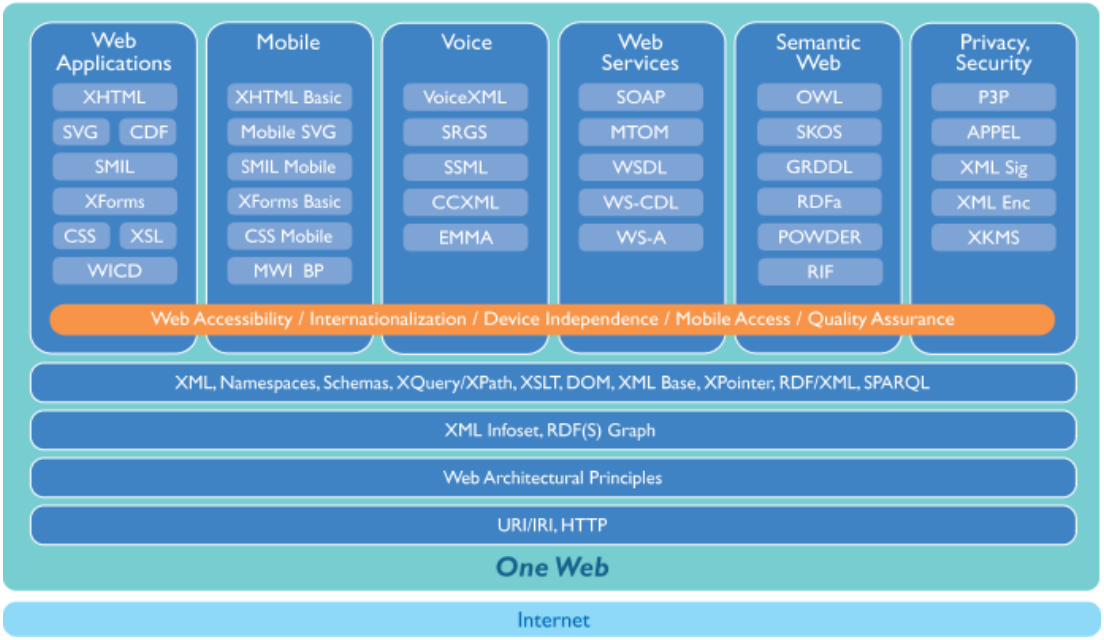


FIGURE 3.6 – Les technologies gérées par le W3C
source : W3C, 2010

3.1.5 Les autres, IEEE, UIT...

Plusieurs organisations nationales, professionnelles ou internationales de normalisation contribuent [aussi] au processus de standardisation d'éléments de l'infrastructure Internet. Ainsi l'IEEE (Institute of Electrical and Electronics Engineers) est le lieu privilégié de la normalisation des réseaux locaux (Ethernet à 10, 100 et 1000 Mbit/s, Wifi, Bluetooth, Firewire ...).

L'ETSI (European Telecommunications Standards Institute) mène une activité de standardisation dans des domaines avancés des télécommunications (téléphonie mobile de 3^{e} génération, terminaux, voix sur IP, sécurité, réseaux intelligents, ...). Les technologies traditionnelles des télécommunications, dont les technologies optiques et SDH, sont normalisées à l'UIT (Union Internationale des Télécommunications) qui reprend également dans sa nomenclature des normalisations issues, entre autres, de l'IEEE (réseaux locaux) et des Bell Labs (SONET). Forums et consortiums s'attachent à définir avec célérité des fonctionnalités spécifiques (ADSL Forum, ATM Forum, QoS Forum, par exemple). [8]

3.2 Le pouvoir d'adressage

Le pouvoir d'adressage découle directement du pouvoir technique. Ce pouvoir est lié à l'unicité des identifiants nécessaires au bon fonctionnement de TCP/IP, du DNS mais aussi de

8. paragraphe extrait du rapport «Développement technique de l'Internet» de Jean-François Ambramatic, 1999, disponible sur le site de l'INRIA à http://mission-dti.inria.fr/Rapport/

nombreux autres protocoles.

À la création d'Arpanet, la gestion de ces identifiants a été attribuée à Jon Postel [9], responsabilité qu'il a gardée jusqu'à sa mort en 1998. En concentrant la distribution de tous ces identifiants entre ses seules mains, Jon était de fait, le point central du fonctionnement de l'Internet. Pour certain il en était le Dieu.

À sa mort, l'Internet Assigned Number Authorithy, IANA, qui lui servait de cadre pour l'exercice de cette mission, a été intégrée dans la naissante ICANN, organisme voulu par le gouvernement américain pour gérer les identifiants numériques uniques et les noms de domaines.

Jon Postel, 1943–1998

«*Soyez conservateur avec ce que vous envoyez, soyez libéral avec ce que vous recevez.*»

En 1969, l'Institut de Recherche de l'université de Stanford (SRI), était le second nœud connecté à l'Arpanet. Il avait été choisi pour être le Centre d'Information du Réseau et Jon Postel, qui y travaillait, fut choisi pour gérer les RFC ainsi que l'attribution des identifiants uniques. Il gardera ce rôle toute sa vie. Mais Jon a été bien plus que cela. Sa participation à travers la rédaction de très nombreuses RFC, au développement du Réseau et des applications qui s'y développaient a marqué l'Internet. On retiendra sa participation au développement des protocoles IP, TCP, UDP, Telnet, SMTP, FTP et du DNS.

Son travail d'éditeur des RFC, mais aussi de conseiller auprès des rédacteurs des RFC, ainsi que son travail de gestion des identifiants uniques durant ces 30 années ont fortement participé à la stabilité technique de l'Internet. Il était un des sages de l'Internet.

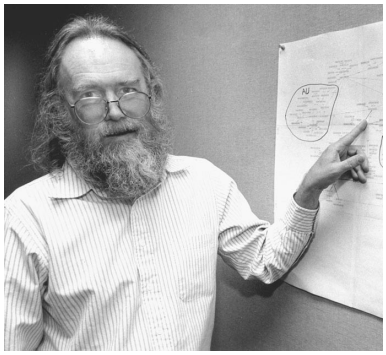


FIGURE 3.7 – Jon Postel
source : photo d'Irène Fertik
©1994 USC News Service

> *Someone had to keep track of all the protocols, the identifiers, networks and addresses and ultimately the names of all the things in the networked universe. And someone had to keep track of all the information that erupted with volcanic force from the intensity of the debates and discussions and endless invention that has continued unabated for 30 years. That someone was Jonathan B. Postel, our Internet Assigned Numbers Authority, friend, engineer, confidant, leader, icon, and now, first of the giants to depart from our midst.*

source : Extrait de la RFC 2468, l'hommage de Vinton Cerf à Jon Postel.

3.2.1 L'ICANN, l'Internet Corporation for Assigned Names and Numbers

La création de l'ICANN a été longue et difficile. Alors qu'Internet subissait un changement structurel profond suite à son ouverture au grand public, nombreux étaient ceux qui remettaient en cause son fonctionnement. Les deux points de conflit étaient le monopole de la Net-

9. voir encart

work Solution Inc., NSI, sur la distribution des noms de domaine génériques (`.org`, `.com` et `.net`) et la mainmise du gouvernement des Etats-Unis sur le fonctionnement de l'Internet.

Les informaticiens pères de l'Internet, dont Jon Postel en tant que IANA, désiraient conserver l'esprit initial du réseau tout en l'ouvrant au monde. Ils ont, dans ce but, proposé la création d'un organisme, le Council of registres [10], CORE [11], basé en Suisse et offrant une place à l'ONU via l'Union Internationale des Télécommunications, ITU. Cet organisme n'avait clairement pas la faveur du gouvernement des Etats-Unis qui imposa à la place une association de droit Californien, l'ICANN [12].

La création de l'ICANN n'a donc pas réglé le problème de la mainmise des Etats-Unis sur l'Internet. Elle a par contre permis de casser le monopole de la NSI en offrant à d'autres entreprises, les registres, la possibilité d'enregistrer des noms de domaine dans les 3 Top Level Domains, TLD, génériques d'alors.

Missions et actions de l'ICANN

En tant que successeur de l'IANA et de NSI, l'ICANN a pour mission la gestion des noms de domaines terminaux, TLD, des adresses IP et des serveurs de noms racines, les *DNS root servers*.

Sa première action a été de casser le monopole de la NSI en créant les registres, les sociétés habilitées à enregistrer des noms de domaine dans les TLD non nationaux.

Elle a ensuite mis au point avec l'OMPI une charte de résolution des disputes liées aux noms de domaine, l'UDPR.

En 2000, l'ICANN a lancé un appel pour la création de nouvelles terminaisons de domaine générique, TLD. Seuls 7 nouveaux gTLD on été retenus : `.aero`, `.biz`, `.coop`, `.info`, `.museum`, `.name` et `.pro`.

En 2003, 7 autres gTLD ont été créés, certains réservés, d'autres ouverts à tous (`.asia` `.cat` `.jobs` `.mobi` `.tel` `.travel` `.post`).

Depuis d'autres ont été ajoutés, dont `.xxx`. En 2012 l'ICANN a décidé d'ouvrir plus largement la possibilité de créer des nouveaux gTLD avec la possibilité d'utiliser des caractères non latins (IDN pour Internationalized Domain Names). Début 2013, avant que l'impact de cette décision soit effectif, la liste des TLD génériques était :

`.aero`	le domaine réservé de l'aéronautique,
`.arpa`	réservé à l'IAB pour l'administration du réseau,
`.asia`	réservé à l'Asie,

10. Les registres sont les entreprises qui vendent les noms de domaine et donc enregistre qui est propriétaire de quel domaine.
11. concernant ce point, on se référencera aux travaux de l'Internet International Ad Hoc Committee et du document proposé, le TLD Memorandum of Understanding, TLD-MoU.
12. voir le Green-Paper et sa révision, le White-Paper, documents proposés par les Etats-Unis et ayant servi de base à la constitution de l'ICANN.

`.biz`	pour ce qui concerne le businesses, ouvert à tous
`.cat`	les domaines en catalan,
`.com`	le domaine historique pour tout ce qui est commercial,
`.coop`	pour les associations et ceux qui se veulent coopératifs, ouvert à tous,
`.edu`	réservé aux établissement supérieurs reconnus par les États-Unis,
`.gov`	réservé au gouvernement des États-Unis,
`.info`	a priori pour l'information mais ouvert à tous,
`.int`	réservé aux agences internationnales,
`.jobs`	réservé aux entreprises pour leurs ressources humaines,
`.mil`	réservé à l'armée des Etats-Unis,
`.mobi`	le domaine des téléphones, assistant personnel..., ouvert à tous,
`.museum`	réservé aux musées,
`.name`	pour votre nom, ouvert à tous,
`.net`	pour tout ce qui touche au réseau, l'un des 3 premiers gTLD, ouvert à tous,
`.org`	pour les organisations, associations...mais en pratique, très utilisé pour les projets informatiques, ouvert à tous,
`.post`	réservé aux postes, probablement pour envoyer un courrier papier par mail...
`.pro`	le domaine réservé aux professionnels. Actuellement limité à certaines professions de certains pays,
`.tel`	pour faire un super annuaire, le système usuel du DNS étant détourné,
`.travel`	pour les professionnels du voyage,
`.xxx`	pour les sites pornographiques.

Depuis de nombreux nouveaux gTLD ont été créés. La liste est maintenue à jour par l'IANA sur http://www.iana.org/gtld/gtld.htm.

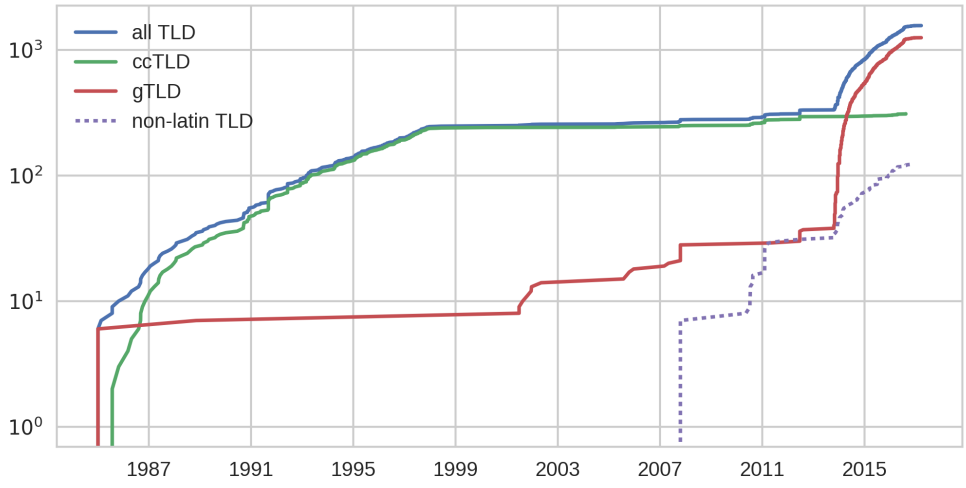


FIGURE 3.8 – Évolution du nombre de TLD (échelle logarithmique)
source : données IANA

m.à.j. sur http://www.ricou.eu.org/e-politique.html

L'organisation de l'ICANN

L'ICANN est une association de droit californien lié par un accord renouvelé annuellement avec le département du commerce des États-Unis. Ces statuts, issus de la réforme de 2002, sont disponibles sur son site, cf http://www.icann.org/general/bylaws.htm.

Le conseil d'administration Le CA est composé de 15 membres ayant un droit de vote et de 6 membres n'ayant pas de droit de vote, les 6 à droite sur la figure 3.9. Ces membres représentent les différents entités impliquées dans l'adressage ainsi que 8 membres élus par le Nominating Committee.

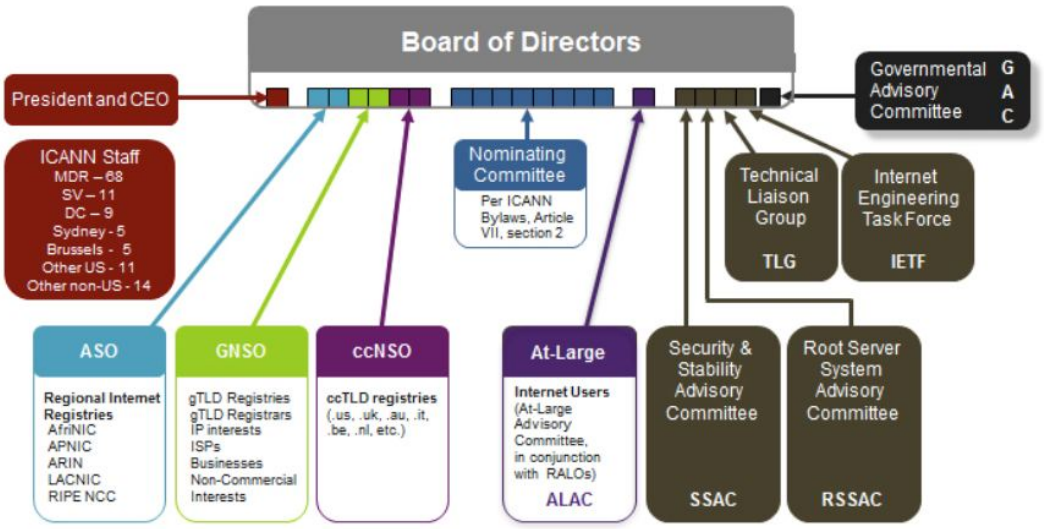
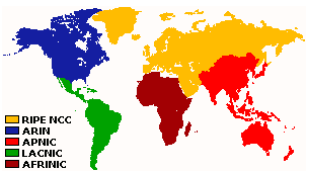


FIGURE 3.9 – Structure du Conseil d'Administration de l'ICANN

Les composantes de l'ICANN

L'ICANN est composé de différents comité chargé de donner des avis sur différentes thématiques. Ces comités sont représentés au Conseil d'Administration.

ASO (2 sièges) L'Address Supporting Organization est composée des différents organismes qui distribuent les adresses IP, les bureaux d'enregistrement "Internet Régional", RIR, à savoir l'ARIN pour l'Amérique du nord, la LACNIC pour l'Amérique Latine et les Caraïbes, le RIPE-NCC pour l'Europe et le Moyen-Orient, l'AfriNIC pour l'Afrique et l'APNIC pour l'Asie et le Pacifique.



Initialement Jon Postel était en charge de la distribution des adresses IP mais rapidement un système de délégation par continent a été mis en place, Jon Postel délivrant des paquets

d'adresses aux organismes en charge des régions continentales. Ce principe continue aujourd'hui avec l'IANA qui distribue les blocs adresses IPv4 et IPv6 aux RIR.

De l'autre coté les RIR distribuent les adresses officiellement à toute personne de leur région en faisant la demande, mais en pratique ils servent les fournisseurs d'accès à Internet et les opérateurs.

GNSO (2 sièges) La Generic Names Supporting Organization comprend toutes les personnes concernées par les gTLD :

— les bureaux d'enregistrement des gTLD,
— les registres,
— les fournisseurs d'accès,
— les utilisateurs commerciaux,
— les utilisateurs non-commerciaux,
— les représentants de la propriété intellectuelle,
— des membres du Nominating Committee.

CCNSO (2 sièges) La Country Code Name Supporting Organization représente les bureaux d'enregistrement nationaux des ccTLD sauf que les gestionnaires des domaines nationaux ne sont pas obligatoirement partant pour participer à ce qui peut être vu comme une ingérence étrangère dans leurs affaires. Le résultat est que la CCNSO n'a pas pu exister officiellement avant 2004 par manque d'adhérents, son règlement stipulant qu'il lui faut 4 représentants par continent [13].

Les pays rebelles, essentiellement les européens, ont de leur coté créé le Council of European National Top level domain Registrie, CENTR. En 2006, ce conseil européen des registres avec ses 50 membres débordait largement de l'Europe avec des pays comme le Canada ou le Japon.

Aujourd'hui le CENTR discute avec l'ICANN pour revoir les statuts de la CCNSO en particulier sur les aspects d'ingérence de l'ICANN dans la gestion des ccTLD. En mai 2006, l'ICANN a accepté de revoir partiellement les statuts de la CCNSO ce qui a été suivi de l'adhésion du Royaume Uni, mais le plus gros ccTLD, l'Allemagne, ainsi que la majorité des pays européens restent toujours en dehors du CCNSO.

RSSAC (1 siège sans droit de vote) Le Root-Server System Advisory Committee est l'organisme responsable du noeud central du DNS puisqu'il regroupe les gestionnaires des 13 serveurs racines.

Parmi ces 13 serveurs racines, 10 sont aux Etats-Unis, 2 en Europe et 1 au Japon. Avant 2002, un serveur racine était une seule machine ce qui posait un problème d'indépendance crucial pour les pays autres que les Etats-Unis. Que les États-Unis bloquent leurs 10 serveurs et le

13. pour avoir ces 4 représentants, l'ICANN a déplacé les îles Caïmans des Caraïbes en Europe et a convaincu Gilbraltar de participer, ce qui a donné comme adhérents européens : les Pays Bas, la Tchéquie, les Îles Caïmans et Gilbraltar.

reste du monde risquait un engorgement fatidique. Heureusement la technique de l'anycast qui permet d'avoir plusieurs machines derrière une même adresse IP, avec la machine la plus proche qui seule répond, a permis de remédier à ce problème. Aujourd'hui sur les 13 serveurs racines, 6 sont en mode anycast ce qui fait qu'il y a en fait plus de 100 machines qui répondent à une requête à la racine du DNS, la majorité étant en dehors de Etats-Unis [14].

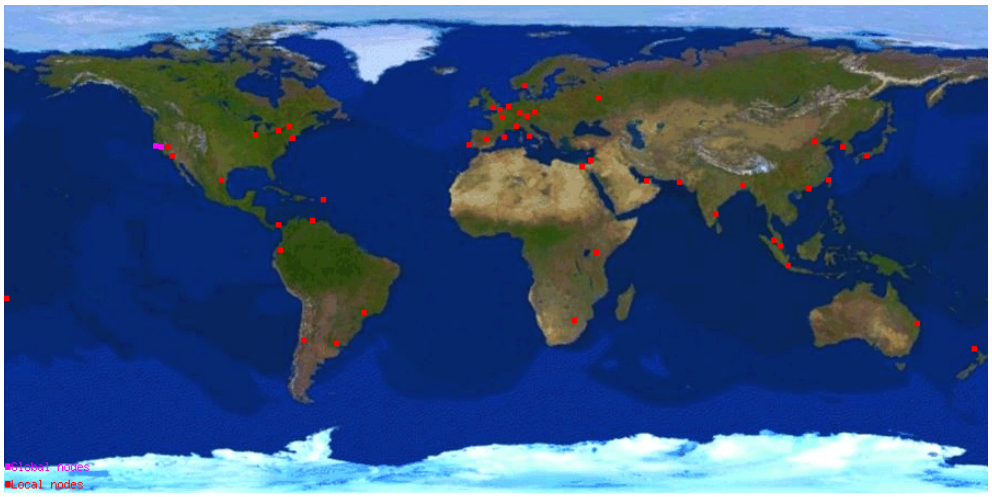


FIGURE 3.10 – Localisation des machines du serveur racine F
source : Internet System Consortium, 2009

SSAC (1 siège sans droit de vote) Le Security and Stability Advisory Committee, comme son nom l'indique, veille à la stabilité et à la sécurité d'Internet pour ce qui concerne l'ICANN. Cela va des mesures suggérées pour éviter le cyber-squatting, en particulier lorsqu'une personne oublie de renouveler un nom de domaine, en passant par les mesures de protection des données privées enregistrées lorsqu'on acquiert un nom de domaine, base `whois`, jusqu'à des aspects plus techniques comme l'allocation des adresses IP version 6.

Le travail de ce comité fait parfois double emploi avec celui de l'IAB ou de l'IETF. Le SSAC n'a pas vraiment plus de poids que ces derniers, même au sein de l'ICANN puisqu'il n'émet que des avis.

GAC (1 siège sans droit de vote) Le Governmental Advisory Committee pourrait être le nouveau siège de la légitimité de l'ICANN qui a rejeté les représentants des internautes en 2002, cf *L'expérience At Large* ci-dessous. Mais les relations entre la direction de l'ICANN et le GAC sont confuses. Il semble que l'ICANN cherche cette légitimité, les relations CA-GAC sont constantes en particulier à travers un groupe de travail, mais en même temps le GAC n'a pas de droit de vote

En pratique le CAG donne son avis sur les mêmes questions que le SSAC, mais d'un point de vue politique. A cela on peut ajouter la gestion des noms de domaine nationaux, les ccTLD, gestion qui est aussi du domaine du CCNSO, d'où un groupe de travail GAC-CCNSO.

14. cf http://root-servers.org/

ALAC (1 siège sans droit de vote) Le At-Large Advisory Committee représente les internautes. Son histoire est houleuse, cf ci-dessous, et sa relégation par le CA à un rôle purement consultatif a fortement contribué au manque d'intérêt que lui portent les internautes.

TLG (2 sièges sans droit de vote) Le Technical Liaison Group comprend les représentants des organismes techniques d'Internet et du monde des télécommunications que sont

— l'Institut européen des normes de télécommunication, ETSI,
— le département des normes de l'Union internationale des télécommunications, ITU-T,
— Le World Wide Web Consortium, W3C,
— l'Internet Architecture Board, IAB.

Le TLG a pour mission de répondre aux questions de l'ICANN et de l'avertir de nouveautés qui pourraient avoir un impact sur sa mission.

L'expérience "At Large"

En 2000, l'ICANN s'est ouverte au grand public en lui permettant de participer directement à l'élection de 5 membres du comité d'administration via l'élection At Large. Ce fut la première élection mondiale au suffrage direct. Elle a rassemblé 76 000 internautes qui ont pris la peine de s'inscrire auprès de l'ICANN pour être électeur «At Large».

Les 5 représentants représentaient les 5 «régions» du monde vu par l'ICANN. Ainsi les premiers élus ont été :

Personne élue	Région	nb voix	nb votants
Nii Quaynor	Afrique	67	130
Masanobu Katoh	Asie / Australie / Pacifique	13913	17745
Andy Mueller-Maguhn	Europe	5948	11309
Ivan Moura Campos	Amérique Latine / Caraïbes	946	1402
Karl Auerbach[a)]	Amérique du nord	1738	3449

TABLE 3.2 – Résultat de l'élection At Large de l'ICANN (automne 2000)
a) élu au sixième tour

Les chiffres de cette élection soulignent la disparité des régions et les différences d'implication des internautes. La seule élection difficile a été celle de l'Amérique du nord puisque Karl Auerbach n'a été élu qu'au sixième tour. Avec Andy Mueller-Maguhn, ces deux élus des régions les mieux connectées étaient les plus en opposition avec l'*establishment* de l'ICANN.

Andy était un jeune hacker libertaire, porte-parole du Chaos Computer Club connu pour son combat pour la transparence, la liberté d'information et pour ses intrusions dans des systèmes informatiques comme celui de la Nasa ou du gouvernement allemand. Il a critiqué le mode de fonctionnement de l'ICANN, sa dépendance vis à vis des Etats-Unis ainsi que sa vision

occidentale. Il désirait une plus grande place pour l'intérêt public sur Internet, menacé d'après lui par la prédominance des entreprises et du droit des marques.

Karl Auerbach était plus âgé. Chercheur chez Cisco, ancien responsable de projets à l'IETF, il était tout aussi critique sur la création et le fonctionnement opaque de l'ICANN. Lui aussi a demandé une plus grande transparence et une ouverture des TLD qu'il désirait créer par millions pour casser la pénurie artificielle des noms de domaine.

Si Andy Mueller-Maguhn semble avoir été muselé, Karl Auerbach a lutté en particulier pour essayer d'obtenir de l'ICANN une plus grande transparence. Cette lutte a culminé durant l'été 2002 avec le procès qu'il a intenté à l'ICANN pour obstruction à l'accès des archives en violation du règlement de l'ICANN et de la loi sur les associations. Bien sûr l'ICANN a été condamnée mais l'establishment a considéré qu'il était vraiment trop dangereux d'avoir des élus du peuple en son sein et a voté une réforme profonde de son fonctionnement pour expulser les représentants des internautes. Ils sont passés de 5 membres au Conseil d'Administration, avec plus du quart des voix, à 1 membre sans droit de vote.

Le bilan

Ce qui aurait dû être un exemple de fonctionnement coopératif et transparent dans la plus pure tradition d'Internet est, malheureusement, devenu une machine opaque

qui semble surtout penser à elle et à servir certains intérêts. La refonte des statuts de l'association voulue par Stuart Lynn en 2002, qui a retiré les représentants des internautes du CA et cherché à impliquer d'avantage les États dans le fonctionnement de l'association a confirmé cette vision.

L'année suivant la réforme des statuts, le budget de l'ICANN a augmenté de 33% pour atteindre 8 millions de dollars, puis doublé en 2004-2005 pour atteindre 15 millions et s'élève pour 2005-2006 à 23 millions. En 2012 on était à 160 millions en incluant les nouveaux TLD. Il est difficile de justifier un tel budget. Les organismes techniques, l'IETF, l'IAB et l'éditeur des RFC, disposaient en 2005, à eux trois, d'un budget 10 fois plus faible avec une dotation de 1,4 million de dollars versée par l'ISOC. Mais l'ICANN peut lever autant d'argent qu'elle le désire sur les noms de domaine, alors comment résister ?

Si la méthode ne convainc pas, les résultats ne sont guère plus convainquants. Certes quelques TLD ont été créés, mais ils restent peu nombreux. Pire, lorsque l'ICANN choisit enfin, en 2006, de créer le TLD `.xxx` pour les sites à caractère pornographique, le gouvernement de Etats-Unis la rappelle à l'ordre et la force à abandonner cette idée. Le domaine n'a finalement été approuvé qu'en 2011.

Bref, l'ICANN a le pouvoir, elle est riche, mais sa crédibilité et sa réputation sont désastreuses. De nombreux pays ont déjà demandé à ce que sa mission lui soit retirée pour être donnée à l'ONU, cf partie sur le SMSI. Il est probable qu'ils reviendront à la charge.

La vision de l'ICANN d'un ancien de l'Internet

```
Date: Tue, 6 May 2003 16:23:57 +0200 (MEST)
From: Louis Pouzin <pouzin@well.com>
To: <forum@isocfrance.org>
Subject: [forum isoc] Re: TLD non americains/ .eu et réforme ICANN

Ces discussions sont les bienvenues.

L'Icann gouverne, au sens américain, c.a.d. organise. Quoi en effet ?

D'abord des réunions internationales. Tous les 3 mois environ, les
habitués se retrouvent en des lieux sympathiques, à travers le monde. On
sait très bien qu'il ne s'y décidera rien car l'araignée a construit une
toile épaisse de comités pare-débat. Mais tout de même, Shangaï, Rio,
Montréal (en été), c'est moins banal que Genève, Genève, Genève. Et ça
entretient une fidélité à l'institution.

En plus de ce rôle de tour opérateur, il y a aussi celui de créer des
top domaines. Il faut faire piaffer les foules pendant quelques années
pour qu'elles se précipitent sur les nouvelles particules. Il importe en
effet de ne pas se faire coiffer au poteau par un gêneur accaparant le
nom de votre société. Le fait de créer ce risque est très bénéfique, car
on crée en même temps les compagnies d'assurance (registreurs) qui
couvrent ce risque pour $30 l'an. Multiplions par 300000 assurés, cela
fait un revenu de $9M. Il est bien naturel que l'Icann soit rétribué
convenablement pour ce petit geste.

Au delà de ce portefeuille d'assurances contre chaînes de caractères
nocifs, il ne reste plus grand chose. Les numéros IP ? En IPv4 l'Icann
(sous couvert IANA) a déjà bien rempli sa mission. Selon la liste
<www.iana.org/assignments/ipv4-address-space> 84% des adresses allouées
ont été attribuées à des sociétés américaines. Difficile de faire
beaucoup plus.

Oh, on allait oublier quelque chose, la Racine (root), la mère des
tables de correspondance entre noms et adresses. C'est pourtant
impressionnant: 250 noms (TLD + ccTLD), et la sauce associée, cela doit
bien faire pas loin de 100K octets. C'est là qu'on vient chercher où
trouver les autres tables des susdits domaines. Comme elles ne changent
guère souvent, tous les serveurs de la planète pourraient s'en faire une
copie, et pourquoi pas une dans chaque PC ?

Avec de tels propos iconoclastes on pourrait finir par imaginer que la
racine ne servirait à pas beaucoup plus que rien. Mais ce serait une
erreur. Elle permet à l'organisation qui contrôle la racine de
surveiller tout le trafic de l'Internet, noter qui parle à qui, placer
des bretelles sur les échanges, détourner les messages ou en fabriquer,
et même rayer des noms (ou ccTLD) de la liste. Mais ce ne serait sans
doute pas convenable de s'attarder sur ce sujet.
```

3.3 Le pouvoir économique

Internet n'est plus le réseau universitaire qu'il a été. Il s'agit aujourd'hui d'une union de réseaux pour la grande majorité privés. Les plus grands de ces réseaux appartiennent à des opérateurs Internet spécialisés dans le déploiement et la gestion des réseaux. L'accès à ces réseaux est ensuite loué aux entreprises ou aux fournisseurs d'accès, ces derniers étant les techniciens de l'Internet les plus visibles. En amont des opérateurs Internet, on trouve les constructeurs de matériel réseau dont le plus connu est Cisco.

L'influence des techniciens sur l'Internet est celle des personnes qui font les choses. Le réseau fonctionne grâce à eux, comme ils le désirent même si pour des raisons d'interopérabilité ils suivent les directives techniques de l'IETF et des autres organismes techniques. Que les plus gros opérateurs Internet et constructeurs décident de développer ensemble leurs protocoles en dehors de l'IETF et cette dernière perdra bien la moitié de sa raison d'être.

Le pouvoir des propriétaires est celui de permettre l'utilisation de leur réseau. On en a le témoignage actuellement dans le débat sur la neutralité des réseaux, cf page 116. Le coût d'un réseau continental étant de plusieurs milliards d'euros [15], les propriétaires des grands réseaux savent qu'ils sont difficilement contournables.

De l'autre coté du miroir, se trouve la puissance économique la plus visible du grand public dont les étoiles actuelles sont Google, Facebook, Apple et toujours Microsoft. Ces entreprise, en relation directe avec les internautes, font régulièrement les unes des journaux et modèlent l'utilisation de l'Internet. On peut les séparer en deux catégories, les entreprises de service et celles qui "contrôlent" l'ordinateur des internautes.

Dans la première catégorie les entreprises qui forment le paysage de l'Internet, celui que parcourt l'internaute. Ce sont Google, Facebook, Yahoo, eBay et bien sûr les commerçants, Amazon, Pixmania en France…

Dans la seconde catégorie on trouve en position d'empereur Microsoft et son système d'exploitation Windows. Avec un quasi monopole Microsoft disposerait d'un pouvoir immense sur l'Internet sans la crainte de procès pour situation de monopole ou pour entrave à la concurrence, procès qu'il a néanmoins régulièrement. Au sommet dans les années 90, force est de constaté qu'il n'a pas su profiter de la vague Internet comme son ancien et de nouveau concurrent Apple.

Apple l'ancien, moribond durant les décennies 80 et 90 a su rebondir en créant de nouveaux usages avec ses iPods, iPhones et iTabs. Son succès lui a permis de dépasser Microsoft en terme de capitalisation boursière en 2010i et de devenir l'entreprise qui dégage le plus de bénécices, et de loin, en 2015.

Une façon de regarder le poids économique des entreprises est de comparer leurs chiffres d'affaire et bénéfices [16], ce que fait la figure 3.12 pour les entreprises phares de l'Internet.

On note le changement brutal des 20 dernières années. Dans les années 90 et encore en 2005,

15. estimation de ce qu'il en coûterait à Google pour se construire un réseau national.
16. avant imposition, operating income en anglais

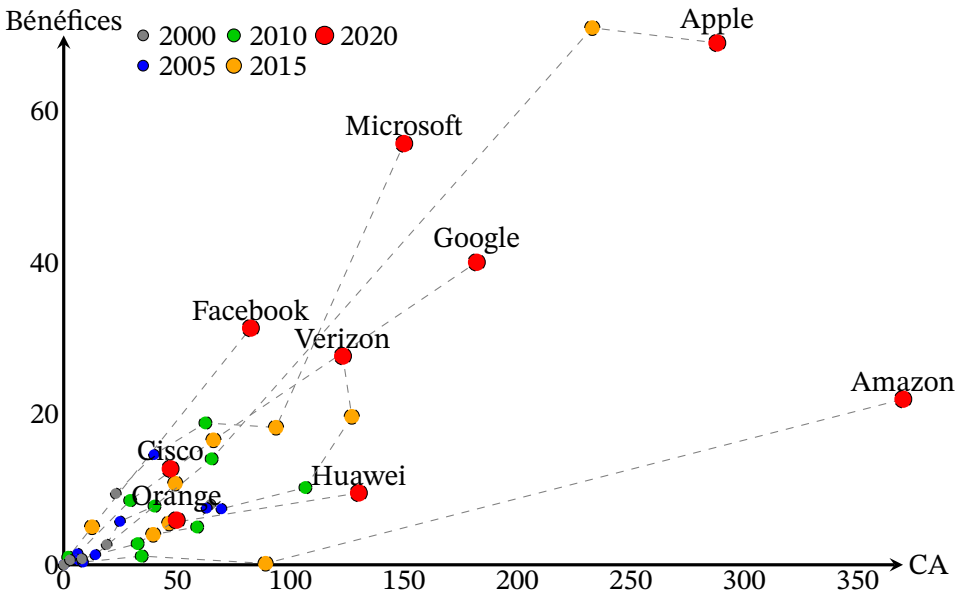


FIGURE 3.11 – Bénéfices et CA en milliards de dollars des grandes entreprises du net
source : Rapport annuel des entreprises (cf http://www.sec.gov/ pour les entreprises US)

les “télécoms” ne jouaient pas dans la même cours que les “informaticiennes”. En 2010 la différences de bénéfices entre Google et Verizon est devenue ridicule alors que le CA de Verizon [17] est 3 fois plus gros que celui de Google. Pour les autres cablo-opérateurs comme France Telecom, la pilule est encore plus amère. En 2015 si Verizon a réussi à doubler ses bénéfices On comprend leur volonté de casser la neutralité du réseau et faire payer Google.

L’opérateur Level3, qui est le plus gros opérateur Internet mais pas un opérateur téléphonique, est tout petit comparé aux autres avec ses 8 milliards de CA (en 2015). Idem pour Free avec un CA d’5.2 G$ et des bénéfices de 0,36 G$ (2014) même s’il est aussi opérateur téléphonique.

Une très grande entreprise comme Total qui a un CA de 128 G$ ne génère que 6 G$ de bénéfices en 2016. BNP Paribas [18] de son coté a un CA de 43 G$ en 2016 et génère 11 G$ de bénéfice. Les puissances économiques de l’Internet qui étaient encore relativement petites en 2000, sont devenues des puissances absolues avec l’omniprésence de l’Internet dans nos sociétés.

3.3.1 La puissance économique des techniciens de l’Internet

Les opérateurs Internet et les fournisseurs d’accès

Les grands opérateurs Internet, souvent les grandes compagnies de téléphonie, gèrent les flux de transit comme les flux internationaux et les réseaux sous-marins. Les plus gros, ceux qu’on appelle les Tier-1, niveau 1, forment l’épine dorsale de l’Intenet. Ils ont des points d’accès à

17. Une des baby Bell, Bell Atlantic
18. la plus grande banque français en terme d’avoirs et la 8e mondiale

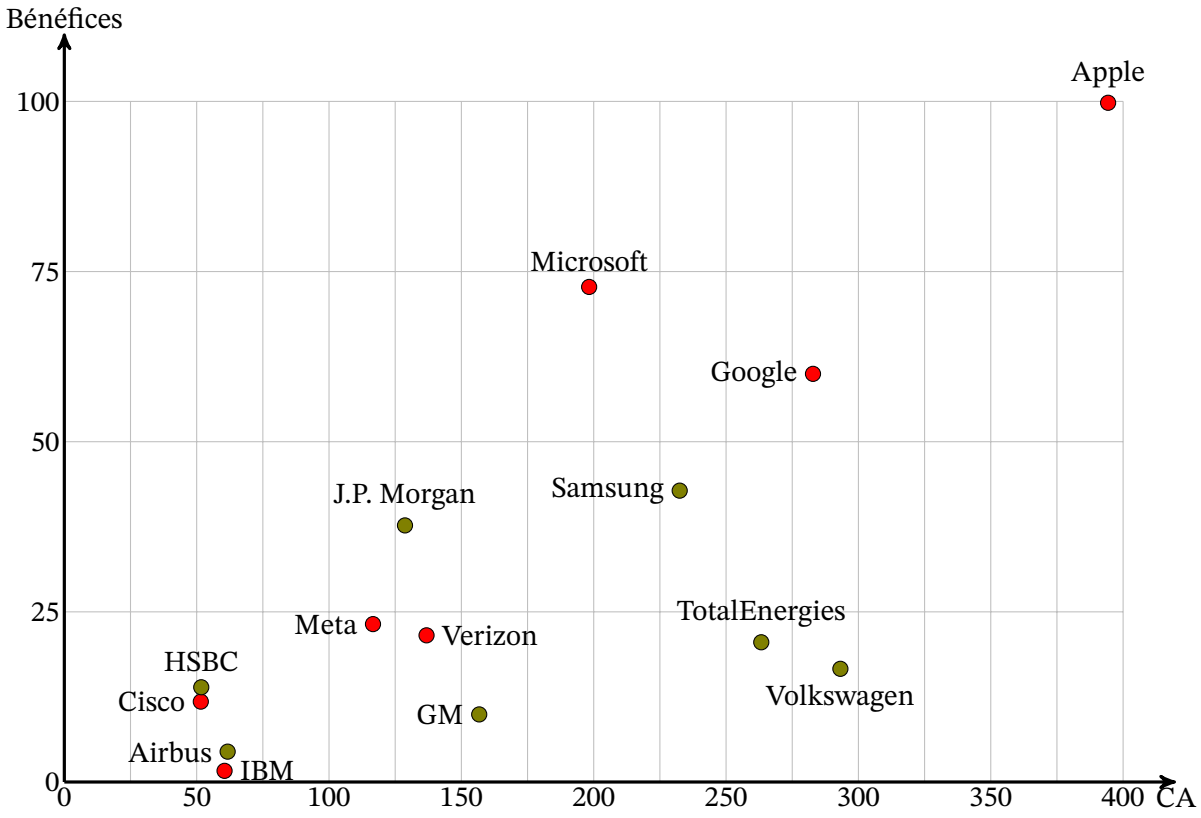


FIGURE 3.12 – Comparaison bénéfices et CA de grandes entreprises (en G$, 2022)
Note : Amazon a 500 G$ de CA pour 0 de bénéfices

travers le monde et louent leurs infrastructures, aux fournisseurs d'accès locaux ainsi qu'aux entreprises.

Les principaux opérateurs sont aux États-Unis et tirent avantage de la position centrale de leur pays dans l'Internet. Dans les années 90, il n'était pas rare qu'une connexion entre deux ordinateurs français passe par les États-Unis simplement car il était plus rentable pour les fournisseurs d'accès français de se raccorder à un réseau américain. En 2005, on estimait que 94% des communications intercontinentales passaient par les États-Unis [19]. En 2012, 9 des 10 plus gros opérateurs Internet sont toujours états-uniens, cf tableau **??**.

La force des gros opérateurs tient dans leur réseau mondial dont le coût de déploiement, en dizaines voire centaines de milliards de dollars, rend l'arrivée d'un nouveau concurrent difficile. Ces réseaux à très grande capacité leur permettent aussi de réduire les coûts de communication et donc forcer économiquement les plus petits réseaux à se connecter à eux. Ainsi, même si aucun des gros opérateurs Internet n'atteint directement 100 % de l'Internet (cf tableau **??**), ses accords de peering entre avec ses pairs [20] garanti un accès global à Internet à un rapport qualité/prix intéressant.

19. cf http://news.com.com/2100-1028_3-6035910.html
20. entre les membres du club Tier 1, les accord de peering sont gratuit généralement.

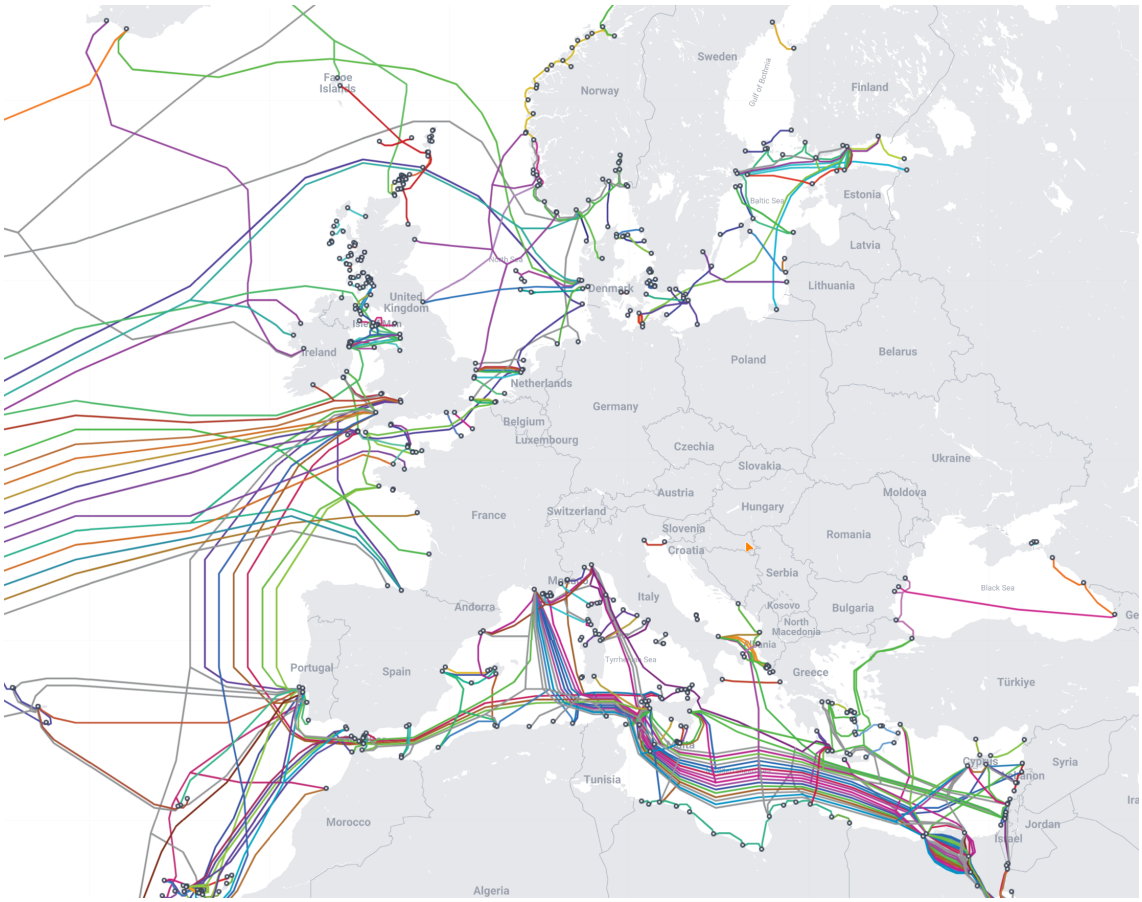


FIGURE 3.13 – Câbles de télécommunication sous-marins – partie Europe
source : TeleGeography 2024, http://www.submarinecablemap.com/

De plus en tant que propriétaire des tuyaux les opérateurs ont techniquement le pouvoir de filtrer ou privilégier les contenus qui transitent suivant des critères arbitraires. La neutralité du réseau consiste justement à ne pas le faire. C'est la position historique des fondateurs de l'Internet. C'est aussi la condition nécessaire pour que le clients final ait accès aux contenus de son choix et qu'Internet ne devienne pas un super Minitel où la valeur des fournisseurs de contenu ne vient plus du contenu mais de leurs accords commerciaux avec les opérateurs. Aujourd'hui les propriétaires des tuyaux aimeraient récupérer une part des bénéfices des fournisseurs de contenu et donc ont déclaré la guerre contre la neutralité du réseau, cf encart page 116. Aux États-Unis, c'est fait depuis 2017 sous l'administration Trump. A l'inverse la neutralité du net est toujours garantie en Europe (en 2024).

Les fournisseurs d'accès sont souvent des opérateurs Internet plus petits, du niveau 2 ou 3. Ainsi le plus gros opérateur français, France Telecom, qui est aussi le plus gros fournisseur d'accès français via sa filiale Orange, dispose aussi d'une entité à part pour son réseau international à savoir OpenTransit qui ne couvre 6 % des adresses IPv4 ce qui le classe au 26e rang en 2016 (cf table **??**). À un niveau moindre, le fournisseur d'accès Free utilise son réseau Proxad qui couvre la France et dispose de connexions à l'international.

Rang	Numéro AS	Organisation	Pays	Taille Cone (ASes)
1	3356	Level 3 Parent, LLC	USA	54757
2	1299	Arelion Sweden AB	SWE	41781
3	174	Cogent Communications	USA	37340
4	2914	NTT America, Inc.	USA	24935
5	6762	Telecom Italia S.p.A.	ITA	23578
6	6939	Hurricane Electric LLC	USA	22707
7	3257	GTT Communications Inc.	USA	20203
8	6453	TATA Communications (AMERICA)	USA	19519
9	6461	Zayo Bandwidth	USA	18819
10	3491	PCCW Global, Inc.	USA	11032
11	9002	RETN Limited	GBR	9938
12	5511	Orange S.A.	FRA	9057
13	1273	Vodafone Group PLC	EUR	7520
14	12956	Telefonica Global Solutions SL	ESP	6214
15	4637	Telstra International Limited	HKG	5440
16	7473	Singapore Telecommunications	SGP	4350
17	7195	EDGEUNO SAS	COL	4092
18	3320	Deutsche Telekom AG	DEU	4043
19	12389	PJSC Rostelecom	RUS	3912
20	52320	GlobeNet Cabos Submarinos	COL	3674

TABLE 3.4 – Principaux opérateurs Internet
La taille du cone représente les clients directs et indirects
source : Caida 2024, http://as-rank.caida.org/

Les constructeurs de matériel réseau

Si l'internaute a besoin du fournisseur d'accès pour se connecter, le fournisseur d'accès a besoin de l'opérateur Internet pour transmettre les données et l'opérateur a besoin des fabricants de matériel réseau pour construire son réseau (nous parlons ici des dorsales d'Internet, des réseaux nationaux, régionaux voire à l'échelle d'une ville, WAN [21] et MAN [22]).

Avec le développement de la 4G, puis de la 5G, il devient de plus en plus facile de surfer sur Internet au point que la majorité des connexions à Internet viennent d'ordiphones. Aussi il devient difficile de séparer les réseaux de télécommunications des réseaux informatiques lorsqu'on pense Internet globalement. Ajoutons que les services qui utilisaient différents réseaux ont généralement basculé vers IP (le téléphone, les vidéo-conférences, le système bancaire...) ce qui fait que télécom et réseau forment un grand réseau IP.

Initialement le marché était largement dominé par Cisco pour l'informatique mais plus par-

21. wide area network
22. metropolitan area network

La neutralité des réseaux

Un fournisseur d'accès à Internet, FAI, peut techniquement privilégier ou réduire les débits vers un site web ou d'une application, la radio en ligne par exemple. La neutralité des réseaux consiste à ne pas le faire, c'est la position historique.

Pourtant, les fournisseurs d'accès et opérateurs Internet aux États-Unis aimeraient changer les règles. Voici le point de vue du directeur de SBC Telecommunications qui répond à la question «*En quoi êtes vous concerné par les startups de l'Internet comme Google, MSN, Vonage et autres ?*» (interview de Business Week) :

> *How do you think they're going to get to customers ? Through a broadband pipe. Cable companies have them. We have them. Now what they would like to do is use my pipes free, but I ain't going to let them do that because we have spent this capital and we have to have a return on it. So there's going to have to be some mechanism for these people who use these pipes to pay for the portion they're using. Why should they be allowed to use my pipes ?*
>
> *The Internet can't be free in that sense, because we and the cable companies have made an investment and for a Google or Yahoo ! or Vonage or anybody to expect to use these pipes [for] free is nuts !*

Vilain Google ! D'un autre coté, sans Google et les autres fournisseurs de services et de contenus, Internet serait nettement moins attrayant et les FAI auraient probablement peu de clients. Alors qui à besoin de qui ?

Les FAI pensent avoir l'avantage et veulent offrir un meilleur accès aux fournisseurs de contenu et de service qui les payent. Il s'agit du système dit à deux niveaux, "two-tier Internet".

Vinton Cerf, vice-président chez Google mais aussi co-auteur de TCP/IP, considère que les FAI sortent de leur rôle en voulant privilégier tel ou tel accès. Pour lui, si les FAI ne respectent pas une véritable neutralité, l'avenir d'Internet est menacé :

> *Nothing less than the future of the Internet is at stake in these discussions. We must preserve neutrality in the system in order to allow the new Googles of the world, the new Yahoo !s, the new Amazons to form. We risk losing the Internet as catalyst for consumer choice, for economic growth, for technological innovation, and for global competitiveness..*

Il a été rejoint dans ce sens par Lawrence Lessig, professeur de droit à Stanford, pour qui l'innovation vient de l'extérieur.

Le "deux niveaux" risque donc de tuer l'innovation en privilégiant le commercial, j'accède à tel service non pas pour son innovation et son efficacité mais car il est bien connecté, le service ayant payé mon FAI pour avoir une bonne connexion.

Prenons un cas pratique. Ayant la fibre, mon fournisseur me propose des vidéos à la demande en 4K. Netflix me propose la même chose. Il y aura donc une concurrence et grande sera la tentation pour mon fournisseur d'indiquer que ses connexions vers Netflix sont saturées et donc qu'il devient impossible d'accéder à la vidéo en 4K.

C'est malheureusement déjà arrivé. En 2009 Free a fait payer DailyMotion pour que ses vidéos restent accessibles à ses clients. En 2012, Free essaie de faire la même chose avec YouTube en refusant de mettre à jour son interconnexion ce qui se traduit par un accès quasi impossible à YouTube le soir. La réponse du PDG de Free était «*J'invite les gens qui ont des problèmes avec YouTube de s'apercevoir que sur Dailymotion souvent il y a les mêmes vidéos*».

En 2017, l'administration Trump a cassé la neutralité du net aux États-Unis.

m.à.j. sur http://www.ricou.eu.org/e-politique.html

tagé pour les télécommunications avec Ericsson, Alcatel et Lucent (rachetés tous les deux en 2016 par Nokia) mais aussi Nortel et Siemens. Huawei est devenu le géant que l'on connait durant les années 2000.

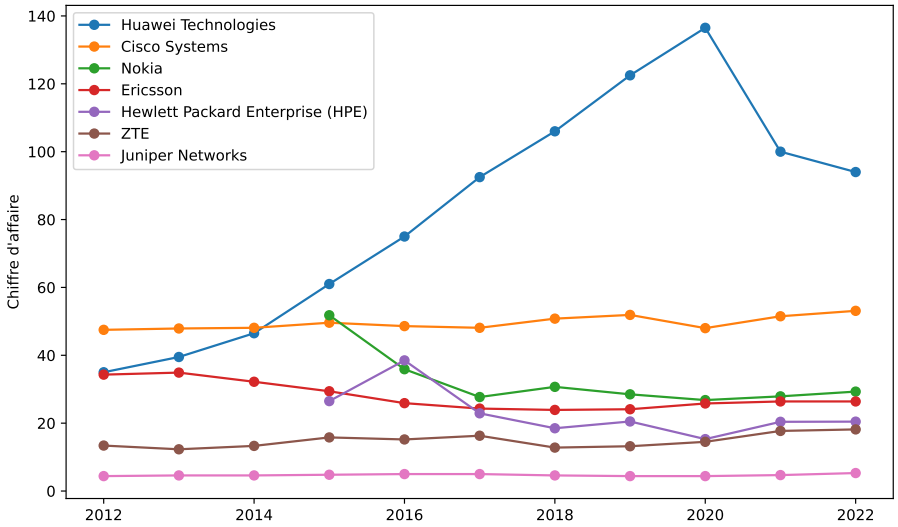


FIGURE 3.14 – Chiffre d'affaire des principaux fabricants de matériel réseau.
source : https://companiesmarketcap.com/ sauf pour Hauwei

La sécurité des réseaux est stratégique Le fait que le réseau soit devenu tellement important pour nos sociétés soulève des problèmes de sécurité en particulier au niveau des États.

Ainsi celui qui contrôle des routeurs et autres équipements réseaux a un véritable pouvoir d'espionnage voire de blocage. Dès lors qu'il s'agit d'entreprises locales, c'est un risque contrôlé mais l'affaire se corse lorsque le risque vient d'équipementiers situés dans des pays tierces. Il est tout à fait possible pour ces fabricants d'introduire des portes dérobées ou des failles dans leur matériel pour espionner ou casser le réseau. Notons aussi que de simples failles de sécurité sont aussi largement utilisé par les agences étatiques pour prendre le contrôle à distance de ces appareils. La NSA [23] a utilsé ainsi des portes dérobées sur du matériel Cisco sans qu'on sache si Cisco l'a aidé ou pas.

Avec les révélations de Snowden en 2013 sur l'espionnage pratiqué par les États-Unis contre des dirigeants européens, les États ont pris plus conscience de ce risque et l'importance d'avoir des équipementiers nationaux est apparue.

Le risque se trouve aussi au niveau des composants utilisés pour construire ce matériel réseau, composants essentiellement chinois. Un rapport du congrès des États-Unis [24] souligne le risque à utiliser du matériel étranger qui peut servir à espionner le réseau voir générer des attaques. Ce rapport visant directement des entreprises chinoises, l'une d'elle fait justement

23. National Security Agency, agence américaine en charge de l'espionnage des moyens de télécommunications, donc aussi Internet.
24. Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE, Octobre 2012

remarquer que le risque se pose aussi bien pour les entreprises occidentales qui achètent leur composants en Chine, à savoir presque toutes.

Cisco Cisco System a été fondée en 1984 par des chercheurs de Stanford. Elle est rapidement devenu le leader pour les équipements réseaux pour Internet et a pu l'accompagner dans sa croissance. Durant le siècle passé, Cisco était l'acteur majeur dans le monde des réseaux informatiques. Depuis la concurrence pousse et en 2023 on estime que Cisco n'a plus que 40 % du marché des commutateurs réseau et 30 % de celui des routeurs (contre 60 et 70 % respectivement en 2015).

Cisco a joué un rôle crucial dans le développement de nombreuses technologies utilisées sur Internet. On en trouve des traces dans les nombreuses RFCs auxquelles Cisco a participé. Puis l'intégration des nouvelles RFCs dans son matériel a poussé l'adoption de ces nouvelles normes et fait avancer Internet.

Huawei Cette entreprise chinoise crée en 1988 est devenue en 2012 le premier fournisseur mondial en réseaux télécommunications, devant Ericsson. Si Huawei est très bon dans les réseaux télécom, en particulier sur la 5G, c'est seulement récemment que Huawei est arrivé au niveau de Cisco pour les routeur (30 % du marché en 2023 mais seulement 10 % pour les commutateurs).

Huawei est typiquement l'entreprise qui fait peur pour les raisons d'espionnage et de cyberguerre citées ci-dessus. Cette entreprise, proche de l'armée et du gouvernement chinois, pourrait en effet servir les desseins de ces derniers. Aussi les sanctions tombent :

2019 les sous-traitant américain de Huawei doivent demander une autorisation pour la fournir et ainsi Huawei ne peut plus installer Android sur ses téléphones.
2020 il est interdit de vendre des composant américains à Huawei (en 2023 Huawei déclare avoir remplacé 13 000 composants qui étaient ainsi bloqués).
2022 les États-Unis interdissent la vente de leur produit télécom sur le sol américain (ainsi que pour ZTE et d'autres entreprises chinoises dans le domaine de la surveillance et de la radio).

Les sociétés au service du réseau

Verisign L'entreprise la plus importante liée à l'aspect administratif du réseau est probablement VeriSign. Elle est

— le bureau d'enregistrement des TLD `.com`, `.net`, `.name`, `.cc` et `.tv` (les deux dernier pour les Iles Coco et Tuvalu)
— l'opérateur technique des gTLD `.edu` et `.jobs`
— les gestionnaire de deux serveurs racine (A et J).

En tant que responsable de la gestion de `.com` et `.net`, VeriSign contrôle plus de 50 millions de noms de domaine (en 2005) ce qui en fait de loin le plus gros bureau d'enregistrement.

VeriSign défie l'Internet

Le 15 septembre 2003, VeriSign a mis en place dans le DNS deux jokers `*.com` et `*.net` qui renvoyaient les adresses inexistantes finissant par `.com` ou `.net` sur son moteur de recherche SiteFinder au lieu de retourner un message d'erreur. Cette modification était clairement une violation des règles implicites.

Un article du Washington Post du 15 septembre indique que VeriSign devrait ainsi obtenir un profit de plus 100 millions de dollars. Il faut dire que d'après VeriSign elle même, il y a plus de 20 millions d'erreurs par jour. Durant les jours d'activité de SiteFinder, le site de VeriSign est passé de la 1559e place à la 19e place en terme de fréquentation.

Mais le problème n'est pas que là. Le DNS ne sert pas que pour surfer sur le Web, il est utilisé par presque toutes les applications qui communiquent sur Internet. Par exemple il permet à un mail d'arriver à bon port et si l'adresse du mail est fausse, il l'indique immédiatement ce qui annule l'envoi et avertit l'émetteur. Avec le système de joker mis en place, l'erreur DNS n'existe plus, puisque VeriSign redirige sur son serveur, ce qui lui permet d'intercepter tous les mails envoyés à une adresse erronée finissant en `.com` ou `.net`.

Du point de vue de la gouvernance, cet acte a été intéressant puisqu'il a permis de voir le poids des différents protagonistes. En théorie l'ICANN peut retirer à VeriSign la gestion des domaines `.com` et `.net` :

- le 19 septembre, 4 jours après, l'ICANN annonce que suite à l'émotion suscitée dans la communauté de l'Internet, elle étudie le problème et demande en attendant à VeriSign de retirer les jokers.
- le même jour l'IAB annonce que l'utilisation de ces jokers viole les règles de bon fonctionnement,
- le 21 septembre VeriSign répond à l'ICANN que d'après ses études il serait prématuré de décider de retirer les jokers et donc rejete la demande de l'ICANN.
- le 22 le comité de sécurité et de stabilité de l'ICANN indique que l'action de VeriSign a considérablement réduit la stabilité d'Internet. Le comité demande à l'IAB et à l'IETF de donner des règles précises sur l'usage des jokers dans le DNS.
- le 3 octobre l'ICANN somme VeriSign d'obéir :

  > *Given the magnitude of the issues that have been raised, and their potential impact on the security and stability of the Internet, the DNS and the .com and .net top level domains, VeriSign must suspend the changes to the .com and .net top-level domains introduced on 15 September 2003 by 6 :00 PM PDT on 4 October 2003. Failure to comply with this demand by that time will leave ICANN with no choice but to seek promptly to enforce VeriSign's contractual obligations.*

- le jour même, VeriSign annonce qu'elle va obéir mais elle se plaint et se réserve la possibilité de faire un procès à l'ICANN :

  > *VeriSign considers ICANN's action today a groundless interference with VeriSign's business.*

On note donc que VeriSign n'a cédé qu'après avoir tenu tête 15 jours et que l'ICANN n'a bougé que poussé par la communauté. Depuis l'ICANN a fait un joli cadeau à VeriSign en lui renouvelant sa délégation du `.com` jusqu'en 2012 avec des conditions qui ont globalement été jugées comme trop favorables à VeriSign.

Tout cela lui permet de discuter avec l'ICANN en position de force.

Verisign a aussi été la plus grande autorité de certification, secteur qu'elle a revendu à Symantec en 2010.

Les autres Il existe de nombreuses entreprises qui gèrent les noms de domaines en tant que registre, comme Go Daddy ou Gandi en France, ou en tant que bureau d'enregistrement. Si chacune de ces entreprises n'a pas de pouvoir sur l'Internet, leur existence collective est vitale pour le fonctionnement du DNS. Leur multiplicité est aussi un gage de stabilité, l'ICANN pouvant toujours retirer l'accréditation de l'une pour la donner à une autre.

On a le même schéma avec les autorités de certification.

3.3.2 La puissance économique grand public

La puissance de la nouvelle économie

La nouvelle économie devait tout ravager sur son passage. L'ancienne n'allait pas s'en remettre et voila que le krach de l'an 2000 a remis les pendules à l'heure. Sauf que finalement, krach n'a été qu'un incident de parcours. Aujourd'hui les entreprises de l'économie numérique ont pris tant d'importance tant économiquement, que socialement, qu'elles sont devenus les plus grosses capitalisations mondiale [25] avec une forte accélération autour des années 2020 qui souligne le changement profond de notre monde (cf figure 3.15).

Aujourd'hui ces entreprises ont un impact significatif sur nos sociétés.

Le pouvoir de ceux qui contrôlent nos ordinateurs

Microsoft Si l'Internet s'est ouvert au grand public durant les années 90 ce n'est pas dû à une certaine volonté politique mais au fait qu'il devenait techniquement possible de connecter les micro-ordinateurs du grand public à l'Internet. Auparavant les ordinateurs utilisés sur l'Internet étaient des machines très coûteuses, que ce soit les stations de travail posées sur les bureaux des chercheurs, ou les super-ordinateurs pour les très gros calculs.

Or durant les années 90 les micro-ordinateurs, dont la puissance augmentait plus rapidement que celle des stations de travail, sont devenus assez puissants et assez complets pour être connectés au réseau [26]. Et comme le système d'exploitation des micro-ordinateurs était presque toujours Windows, Microsoft a pu profiter pleinement de l'arrivée du grand public sur Internet pour devenir un des poids lourds de l'Internet.

En 1995 Microsoft est devenu un acteur majeur du web avec son Internet Explorer avant de se faire dépasser par Chrome dans les années 2010 et devenir marginal en 2020.

25. la capitalisation étant la valeur des actions multipliée par leur nombre, elle prend en compte la valeur actuelle de l'entreprise mais aussi ce que les actionnaires imaginent qu'elle va devenir.
26. aujourd'hui les stations de travail n'existent plus, elles ont été remplacées par des micro-ordinateurs.

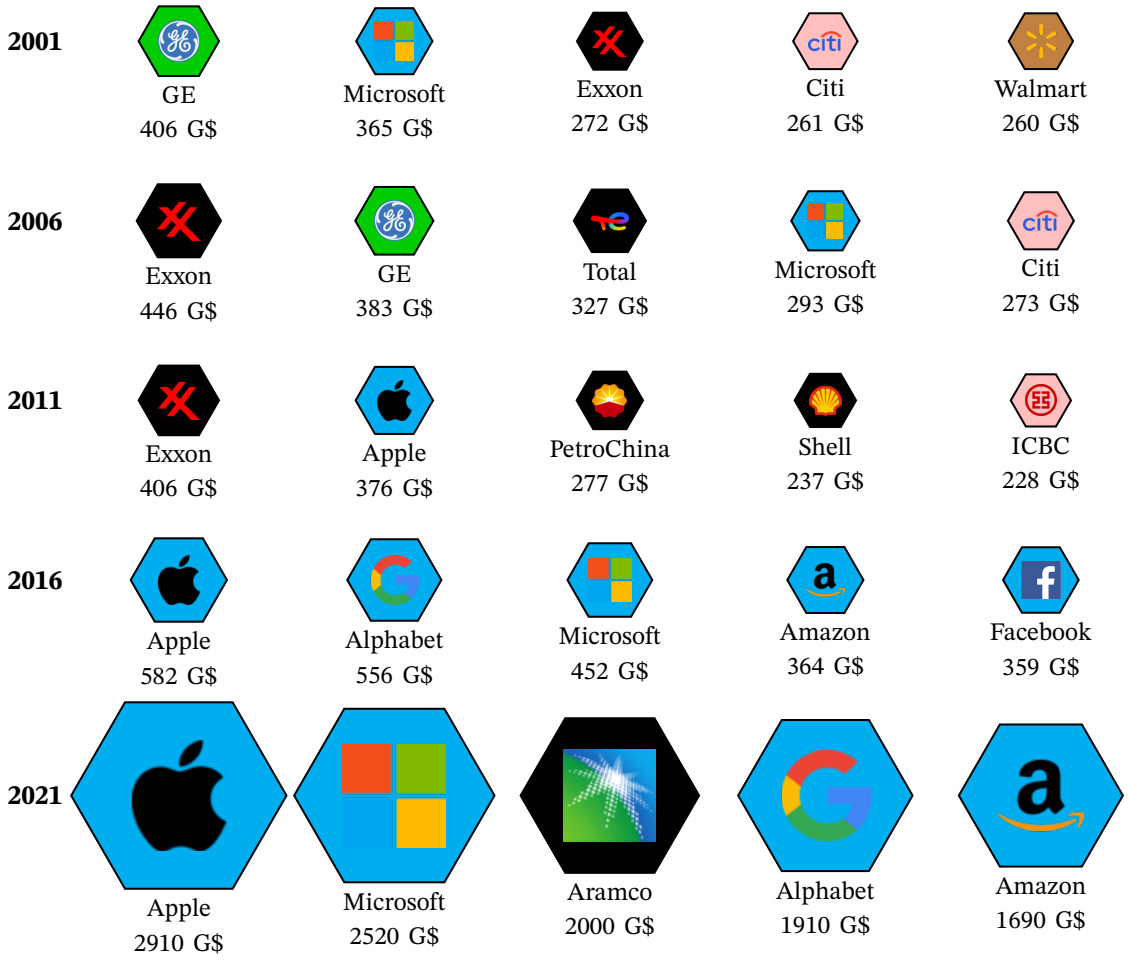


FIGURE 3.15 – Plus grosses capitalisations boursières ou quand Internet remplace le pétrole
En 2024 NVidia a remplacé Aramco (créée en 2019)
Plus d'entreprises sur https://companiesmarketcap.com/

On avait donc une entreprise, en quasi situation de monopole dans le monde industriel et du grand public, qui comprend l'importance d'Internet et mise dessus. Fort heureusement Internet était encore un réseau essentiellement sous Unix, contrôlé techniquement par les académiques et des entreprises réseaux et dont l'importance n'échappait plus aux gouvernements, donc un trop gros morceau à avaler, même pour Microsoft.

Cela a pu se confirmer lorsque de la guerre qu'a menée Microsoft en ajoutant ses balises à HTML et ainsi casser en deux le web avec le web Microsoft et le web historique. Le créateur de web, Tim Berners-Lee a réagit avec l'aide d'université pour créer le W3C et forcer Microsoft à l'intégrer pour gérer ensemble l'évolution du protocole HTML.

La puissance de Microsoft était aussi un risque vis à vis de la loi anti-monopole. L'entrrpise risquait d'être divisé en sous-entreprises ce qui forçait Microsoft à faire profil bas voire à aider la concurrence à survivre (par exemple Apple).

Microsoft n'a donc pas pu profiter pleinement d'Internet. Elle a aussi raté le virage des or-

diphones et doit finalement son retour au premier plan grâce au nuage (*cloud*) avec Azur et grâce à l'IA avec sa participation dans OpenAI (ChatGPT).

Apple À l'inverse de Microsoft, Apple a pleinement profité de la vague Internet pour renaitre. Le premier pas d'Apple a été l'abandon de son ancien système d'exploitation pour en reconstruire un basé les système d'exploitation libre FreeBDS et NetBSD, des UNIX. Mais le renouveau d'Apple est surtout dû à ses appareils portables qui ont générer de nouveaux usages : l'iPod, l'iPhone et l'iPad. Non seulement Apple a créé les appareils mais surtout il a su mettre en place les services associés à savoir l'iTune pour la musique et l'App Store pour les applications iPhone et iTab.

La force d'Apple aura été de créer l'outil que tout le monde attendait depuis les Palms des années 90, à savoir l'appareil qui fusionne avec succès l'ordinateur et le téléphone. L'explosion d'Internet et son accès par la 3G a clairement aidé, mais le génie ne doit pas être sous estimé. Cela faisait des années que les concurrents essayaient cette fusion et ni Palm, ni Microsoft avec Windows Mobile n'y été aussi bien arrivé. Mais l'iPhone tout seul n'aurait pas eu son succès sans les milliers d'applications dédiées qui ont été développées pour lui via un écosystème très bien contrôlé par Apple. Ainsi début 2013, 40 milliards de téléchargement d'applications avaient eu lieu sur l'App Store ce qui a généré un revenu estimé à 7 milliards de dollars pour Apple [27].

Aujourd'hui Apple est en position de force, toute la question étant de savoir si Apple pourra continuer son chemin avec autant de succès sans son fondateur Steve Jobs, mort en 2011.

Linux et les logiciels libres Les logiciels libres et Linux sont à l'opposé de la philosophie de Microsoft et d'Apple. Au modèle économique de développement d'un logiciel pour le vendre ou pour vendre des produits dérivés, les logiciels libres répondent par des produits collaboratifs gratuits et librement ré-utilisables. Ainsi dans le monde du Web, Firefox et Apache sont devenus des références dans le monde des navigateurs pour le premier et dans celui des serveur web pour le second. Dans le développement informatique et en particulier dans les langages de codage, là encore la notion de libre est usuelle en particulier pour les compilateurs.

Les logiciels libres, qui sont développés et diffusés sur Internet grâce à un travail collaboratif à l'échelle de la planète, sont un commun [28] qui a cassé l'idée que les communs ne sont pas viables. En cela, les logiciels libres ont participé au retour de la nation de communs dans notre société.

Le pouvoir des usages

Google (Alphabet) L'étoile de la nouvelle économie qui brille le plus fort est bien sûr Google. Créé 25 ans après Apple et Microsoft, elle joue les tout premiers rôle sur Internet et ce depuis

27. Apple prend 30% sur les ventes d'applications pour iPhone ou iTab et interdit les ventes directes
28. Les communs sont une notion juridique qui décrit la possession qui n'est ni privée, ni publique mais qui appartient à un groupe, lequel fonctionne suivant des règles ouvertes. Voir les travaux d'Elinor Ostrom à ce sujet.

l'arrivée de son moteur de recherche à la fin des années 90 (entre 80 et 90% des parts de marché des moteurs de recherche en 2024 suivant les instituts de sondage).

Son second succès notable est le système Android utilisé par la grande majorité des ordiphones.

Troisième point fort est son navigateur Chrome qui est devenu hégémonique.

N'oublions pas que Google c'est aussi YouTube, la plateforme de référence pour la diffusion de vidéos.

Tout ces points façonnent directement les usages des internautes et font l'importance de Google pour Internet.

Facebook (Meta) Facebook est la référence dans les réseaux sociaux même si les nouvelles générations lui préfère d'autres réseau sociaux. Avec ses 3 milliards d'utilisateurs, Facebook arrive à exercer une influence sur Internet et le monde réel.

Dans le monde réel la révolution du Printemps arabe de 2010 est probablement le meilleur exemple de l'impact de Facebook (mais aussi de Twitter). La Tunisie qui était un modèle de censure et de contrôle de l'Internet n'a pas pu bloquer Facebook et Twitter pour éteindre l'incendie. Cela étant il semblerait que les régimes autoritaires soient nettement plus efficace dix ans plus tard et qu'au contraire, les réseaux sociaux soient devenu plus une aide à la surveillance qu'un outil d'émancipation.

Un autre exemple de l'influence de Facebook se retrouve dans les élections américaines, tant pour celles d'Obama qui a su utiliser les relations entre utilisateurs de Facebook pour que ses supporters aillent convaincre leurs amis hésitants, que pour celle de Trump qui a profité de l'aide de la Russie avec ses *fake news* ciblées sur Facebook

Amazon Il est évident que cette entreprise de vente par correspondance a gagné sont pari, les internautes achètent sur Internet et les catalogues quasi-infinis d'Amazon et de ses concurrents ont changé les habitudes des consommateurs et obliger les magasins physiques à s'adapter.

3.4 Le pouvoir politique

Les gouvernements ne sont pas impuissants face à l'Internet, loin de là. Ils disposent de lois pour imposer leur volonté dans leur pays et des accords internationaux pour l'imposer sur l'ensemble de l'Internet. Suivant les pays, les gouvernements ont d'autres leviers nationaux comme la censure, les contraintes techniques comme un passage unique pour sortir du pays, les incitations financières, la pression sur les entreprises…

Les Etats-Unis disposent en plus, du contrôle de l'ICANN [29], donc du DNS, et d'une surrepré-

29. car l'indépendance de l'ICANN est toute relative.

sentation dans l'ensemble des organismes de gestion de l'Internet.

A côté des gouvernements, certaines associations disposent d'un poids politique important sur l'Internet, en particulier l'Internet Society, qui chapeaute l'IAB, l'IETF et l'IRTF.

3.4.1 Les pouvoirs nationaux

Les lois

Si l'Internet a profondément modifié notre société et a rendu des lois dépassées, les gouvernements suivent attentivement ces modifications et adaptent les lois régulièrement afin de préserver l'État de droit sur l'Internet. Ainsi les lois françaises encadrent :

— la liberté d'expression,
— la protection de la vie privée,
— le piratage,
— la vente en ligne,
— le téléchargement dont le pair à pair, P2P,
— la cryptographie,
— ...

Dans certains cas, comme dans le cas récent en France de la loi DADVSI sur les droits d'auteur, les lois nationales sont l'application d'accord internationaux.

En France, il n'y a guère de domaines de l'Internet non couverts par la loi.

Les organismes nationaux

Les organismes nationaux sont le plus souvent le résultat de la loi, par exemple la CNIL a été créée suite à la loi "Informatique et liberté" de 1978. Ces organismes ont pour mission d'encadrer l'exécution de la loi en définissant les vides laissés par la loi afin de pouvoir s'adapter aux évolutions, en gérant les aspects d'enregistrement lorsque la loi le prévoit, en avertissant le gouvernement des changements du paysage et de la nécessiter de faire évoluer la loi, etc.

Ces organismes ont un rôle très important puisqu'ils représentent l'État et construisent l'environnement permettant l'application de la loi. Lorsque la loi est en relation directe avec le fonctionnement de l'Internet, ces organismes deviennent des acteurs majeurs de l'Internet national.

Les organismes français en charge de l'Internet français

Les organismes français les plus importants de l'Internet français sont l'ARCEP, la CNIL, l'AFNIC et le forum de l'Internet. Avec la démocratisation de l'Internet, d'autres organismes

Censure sur Internet

La censure sur Internet est l'application des lois locales ou des usages. Ainsi en France, la loi interdit de faire l'apologie du nazisme et plus généralement l'incitation à la haine raciale. British Telecom, en application de la loi anglaise, bloque les sites répertoriés comme pédophiles par l'Internet Watch Foundation, censure que l'on retrouve dans d'autres pays. En Corée du Sud sont bloqués les sites pro-Nord-Coréen...

Suivant les pays, les techniques ne sont pas les mêmes. La France censure a posteriori par saisine de la justice sur constatation. Dans d'autres pays la censure est en amont, que soit avec des parefeux qui bloquent tout sauf autorisation ou avec une administration en charge de la censure.

D'un point de vue technique, la mise en œuvre de cette censure dans les pays les plus radicaux est le plus souvent le fait d'entreprises occidentales. Les ténors de l'Internet à savoir Google, Yahoo, Cisco, Microsoft ont déjà fait les unes des journaux lors de signature de contrats avec ces pays.

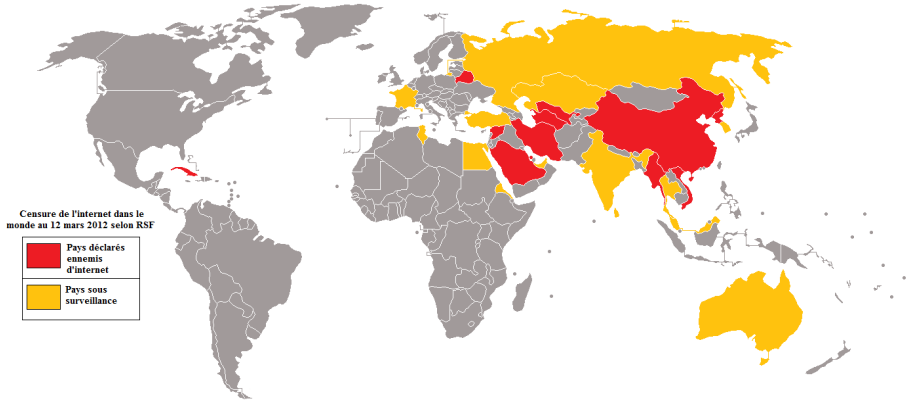


FIGURE 3.16 – La censure sur Internet par pays
source : Données : Reporter sans Frontière 2012, Carte : Wikipedia

Cette censure est semblable à celle de la presse pour les pays qui en ont les moyens techniques :

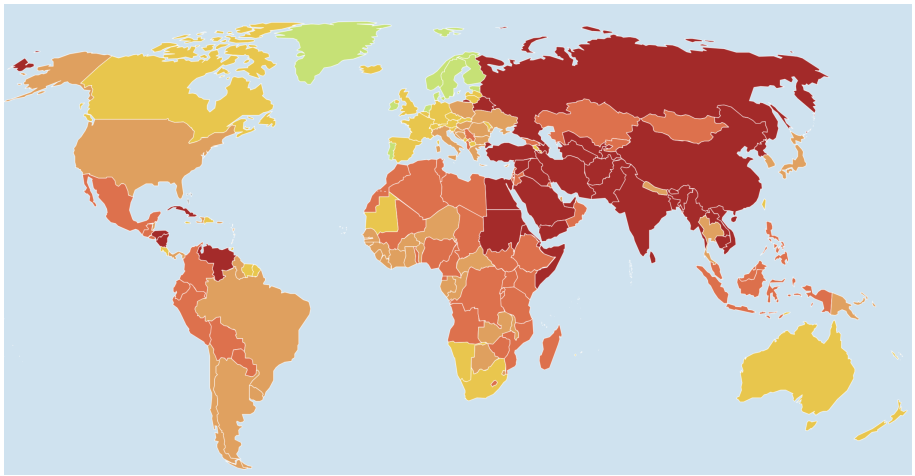


FIGURE 3.17 – La liberté de la presse par pays
source : Reporter sans Frontière 2024

entrent en jeu comme le Conseil de la Concurrence, le Conseil économique et social, le Conseil Général des Technologies de l'Information…

L'ARCEP Anciennement l'ART, l'Autorité de Régulation des Communications électroniques et des Postes a été créée en 1996 par la loi 96-659 de réglementation des télécommunications, loi définissant les conditions de mise en place, d'ouverture à la concurrence et d'exploitation de réseaux de télécommunication. En 2002 sa mission a été élargie, principalement à la régulation de l'ouverture à la concurrence de la poste.

Concernant Internet, les dossiers de l'ARCEP sont :

— le dégroupage, à savoir le changement d'opérateur pour gérer la ligne téléphonique,
— l'offre ADSL, avec un travail sur la concurrence loyale entre les opérateurs,
— la boucle locale radio, qui permet de se connecter à Internet via la radio en mode Wimax,
— le déploiement de la fibre.

Dans tous les cas l'ARCEP fait office d'observateur et de régulateur. Les observatoires et les publications de l'ARCEP sont en général riches d'informations. En tant que régulateur, l'ARCEP attribue les ressources limitées comme les fréquences radio, émet des avis, prend des décisions pour garantir une concurrence loyale entre les opérateurs.

Les lois à la source de l'ARCEP étant les transpositions des directives européennes ouvrant à la concurrence le marché des télécommunications, on retrouve des "ARCEP" dans les différents pays de l'Union Européenne. Elles ont créé au niveau européen l'Independent Regulators Group.

L'AFNIC L'Association Française pour le Nommage Internet en Coopération est en charge de la zone `.fr` et `.re`, respectivement pour la France et la Réunion. Elle a été créée en 1997 pour remplacer l'INRIA [30] qui n'avait plus vocation à s'occuper de cette zone à partir du moment où Internet n'était plus un outil essentiellement universitaire. Son mandat a été renouvelé en 2012 suite à un appel d'offre du gouvernement pour la gestion des ccTLD appartenant à la France.

Chargée de définir une politique de classement au sein de `.fr`, l'AFNIC a fait preuve d'originalité en réservant pendant des années la terminaison `.fr` aux sociétés et en ouvrant `.com.fr` à tous, ou en créant un espace `.tm.fr` pour les marques, *trademark*, tout en acceptant ensuite `pagesjaunes.fr` puis en indiquant que finalement `.fr` est aussi possible pour les marques. L'AFNIC a aussi mis en place des espaces sectoriels comme `.experts-comptables.fr` ou `.geometre-expert.fr` qui peuvent muter comme l'a fait `.barreau.fr` pour devenir `.avocats.fr`. Bref, l'AFNIC n'a pas su définir une politique de nommage cohérente et s'y tenir.

En même temps l'AFNIC a mis en place une politique de réservation très lourde administrativement ce qui a nettement freiné l'enregistrement de domaines en `.fr`. Il s'agissait de garantir un *espace de confiance*. Elle a finalement simplifié les procédures en 2004 pour les entreprises et en 2006 pour les particuliers. Le résultat a été immédiat. En 2008 le cap du million de

30. Institut National de Recherche en Informatique et en Automatique

domaines a été atteint.

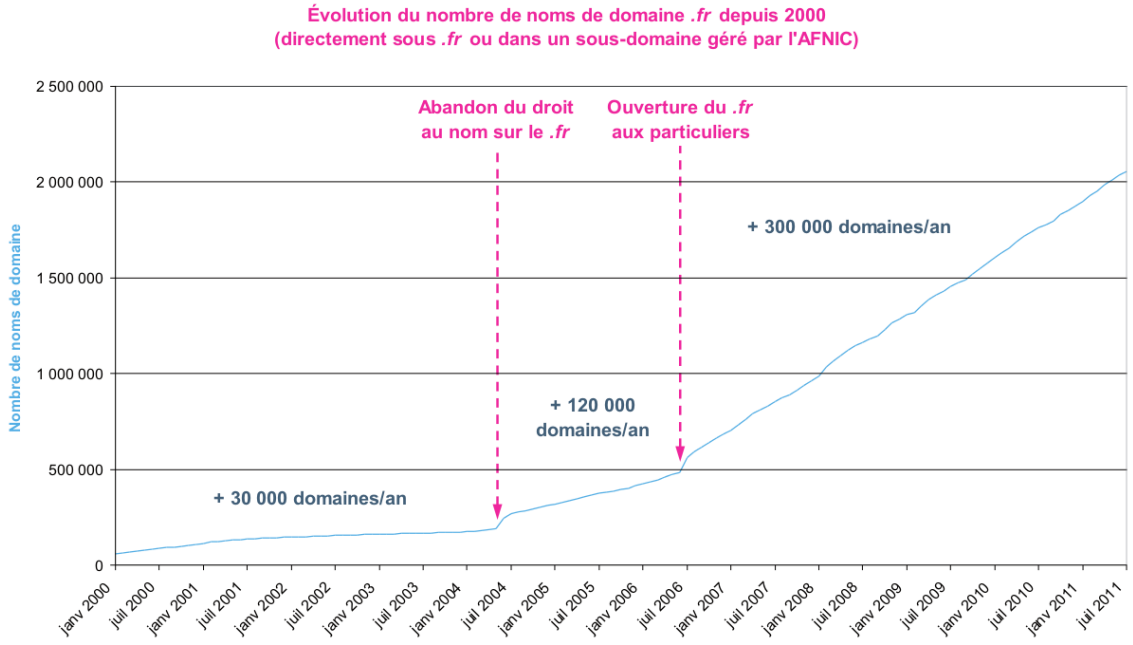


FIGURE 3.18 – Evolution du nombre de domaines en `.fr`
source : AFNIC, Observatoire 2011

A titre de comparaison, le `.de` allemand avait dépassé le million de domaines en 2000 contre 2008 pour le `.fr`. En 2011 il y avait 7 fois plus de domaines en `.de` qu'en `.fr`. Certes l'Allemagne est le champion des noms de domaines nationaux, mais toujours en 2011 le `.uk` du Royaume Uni était 4,5 fois plus grand que le `.fr` et l'Italie et la Pologne avaient aussi plus de domaines nationaux que la France.

Aujourd'hui tout résident en France peut réserver un domaine en `.fr` à condition que le domaine ne soit pas déjà pris et qu'il ne soit pas sur la liste noire. Cette liste noire, appelée la liste des termes fondamentaux non enregistrables, contient les communes, des organismes, des sigles et une liste à la Prévert pas vraiment cohérente [31].

La CNIL La Commission Nationale Informatique et Liberté est probablement l'organisme lié à l'informatique et à Internet le plus connu du grand public. Sa mission est de veiller au respect de la loi informatique et liberté, à savoir protéger la vie privée et les libertés individuelles ou publiques face aux risques de fichage informatique.

La CNIL est une autorité morale consultée lorsqu'un texte de loi est en discussion et qu'il y a des risques concernant la vie privée, lorsqu'un projet local ou régional porte les mêmes risques, etc. Elle a aussi un devoir de surveillance des fichiers informatiques nominatifs, en particulier de vérifier leur conformité avec la loi, avec possibilité de saisir la justice. Enfin,

31. Jeu : `canon.fr`, `fusil.fr`, `pistolet.fr`, `revolver.fr`. Parmi ces 4 domaines, 2 sont autorisés et 2 ne le sont pas, trouvez lesquels.

depuis la révision en 2004 de la loi informatique et liberté, la CNIL dispose d'un pouvoir de sanction.

Le terrain d'action de la CNIL dépasse l'Internet, elle était néanmoins très attendue sur ce média informatique. Force est de constater que la CNIL a déçu, sa mécrompréhension de ce média a été constatée à plusieur reprises. Mais la CNIL déçoit aussi globalement, cf encart.

Des prix pour la CNIL soulignant la déception…

Prix Spécial du Jury Bug Brother 2000 «*Pour son incapacité à utiliser avec pertinence tous les contre-pouvoirs que lui donne la loi pour protéger le citoyen contre la montée du fichage accru (contribuables, salariés ou assurés sociaux). Ou pour sa trop grande prudence à se déclarer publiquement contre certains projets sensibles.*».

Nominé au Big Brother Awards France 2005 pour l'ensemble de son œuvre, Alex Türk, alors président de la CNIL, il a obtenue le prix spécial du jury 2010 « pour tromperie et dissimulation » avec la précision «*Alex Türk endosse les habits du défenseur tout terrain de la vie privée et des libertés alors qu'il en est parfois le fossoyeur et souvent le facilitateur.*»

Madame Isabelle Falque-Pierrotin nomée présidente en 2011 avait déjà nominée aux Big Brother Awards 2007 dans le cadre de son travail au Forum des Droits de l'Internet.

Le cas des États-Unis

Les États-Unis ayant créé l'Internet, ils en ont eu le contrôle absolu. Depuis que l'Internet est devenu international, ce contrôle a diminué mais reste assez important. Il faut dire que les États-Unis contrôlent

— le DNS à travers l'ICANN,
— le plus gros du réseau et en particulier la majorité du transit intercontinental (pour certains pays cela peut être plus, 84 % du trafic international pour le Brésil [32]).
— les entreprises les plus importantes de l'Internet.

Si les deux derniers points sont difficilement mesurables, le contrôle du DNS a montré ce qu'on peut en faire :

— fermeture des domaines `.af` et `.iq` au moment des guerres des États-Unis contre l'Afghanistan et l'Iraq,
— refus de la création du TLD `.xxx` pour les sites pornographiques qui a repoussé de 5 ans sa création.

À cela on peut ajouter que les États-Unis sont surreprésenté dans l'ensemble des organismes qui gèrent l'Internet (IETF, ISOC…).

Tout ces points font que les Etats-Unis ont toujours un contrôle important sur Internet.

32. Chiffres extraits des travaux d'Anne Edmundson en 2018.

3.4.2 Le pouvoir international

Poussée par les États qui supportent mal la mainmise des Etats-Unis sur l'Internet, poussée par l'Union Internationale des Télécommunications, UIT, qui rêve de gouverner l'Internet, l'ONU se penche de plus en plus sur les aspects de gouvernance de l'Internet. Elle a ainsi lancé des sommets ouverts, invitant les universitaires, les entreprises et la société civile à participer afin d'ouvrir un dialogue entre tous les acteurs, ceux qui représentent les citoyens et ceux qui ont fait et font l'Internet.

Le sommet mondial sur la société de l'information, SMSI

La première manifestation a été le Sommet Mondial sur la Société de l'Information, SMSI, tenu en deux partie, en 2003 et en 2005, sous l'égide de l'UIT, en tant qu'organisation des Nations Unies. Les objectifs officiels de ce sommet était la lutte contre la fracture numérique nord-sud et la gouvernance de l'Internet.

Si ce sommet a bien réuni un nombre impressionnant de personnalités et a permis d'aborder les problèmes de gouvernance, force est de constater que peu de choses ont changé dans le fond. Ainsi le principal, le contrôle des Etats-Unis sur le DNS, n'est pas remis en question.

Cependant l'accord obtenu à la fin de la seconde partie en 2005, dit l'agenda de Tunis, a permis certaines avancées :

art. 35 a) *en ce qui concerne les questions d'intérêt général qui se rapportent à l'Internet, le pouvoir décisionnel relève de la souveraineté nationale des États, lesquels ont des droits et des responsabilités en la matière;*

La suite de l'article souligne l'importance du secteur privé, de la société civile, des organisations intergouvernementales et internationales. L'article suivant souligne la précieuse contribution du milieu universitaire. Mais la page est tournée, les États revendiquent le contrôle de l'Internet, ce qui ne fait qu'officialiser une réalité de plus en plus nette.

art. 38 *Nous appelons au renforcement d'institutions régionales spécialisées dans la gestion des ressources Internet afin de garantir les intérêts et les droits nationaux des pays de cette région quant à la gestion de leurs propres ressources Internet, tout en assurant une coordination au niveau mondial dans ce domaine.*

art. 63 *Les pays ne devraient pas intervenir dans des décisions relatives au domaine de premier niveau correspondant au code de pays (ccTLD) d'un autre pays. Les intérêts légitimes nationaux, tels qu'ils sont exprimés et définis par chaque pays, de diverses manières, en ce qui concerne les décisions relatives à leurs ccTLD doivent être respectés, défendus et traités dans un cadre et au moyen de mécanismes souples et améliorés.*

art. 68 *Nous reconnaissons que tous les gouvernements devraient avoir égalité de rôle et de même responsabilité dans la gouvernance internationale de l'Internet ainsi que dans le maintien de la stabilité, de la sécurité et de la continuité de ce réseau. Nous reconnaissons également la nécessité pour les gouvernements d'élaborer des politiques publiques en consultation avec toutes les parties prenantes.*

Quelques vœux pieux ont donc été dirigés contre les États-Unis qui ont été obligés de céder officiellement mais sans rien perdre de leur pouvoir.

L'autre point fort du SMSI concernant la gouvernance de l'Internet et la création d'un forum de la gouvernance de l'Internet où seront abordés les aspects politiques de cette gouvernance. Cela exclu donc les aspects techniques comme la gestion du DNS.

Le Forum sur la gouvernance d'Internet

Le poids de ce forum dépend essentiellement de ses participants, et donc de ses relations avec les autres organismes de l'Internet et du monde physique. À l'usage l'impact de ce forum sur le fonctionnement de l'Internet n'est pas bien visible.

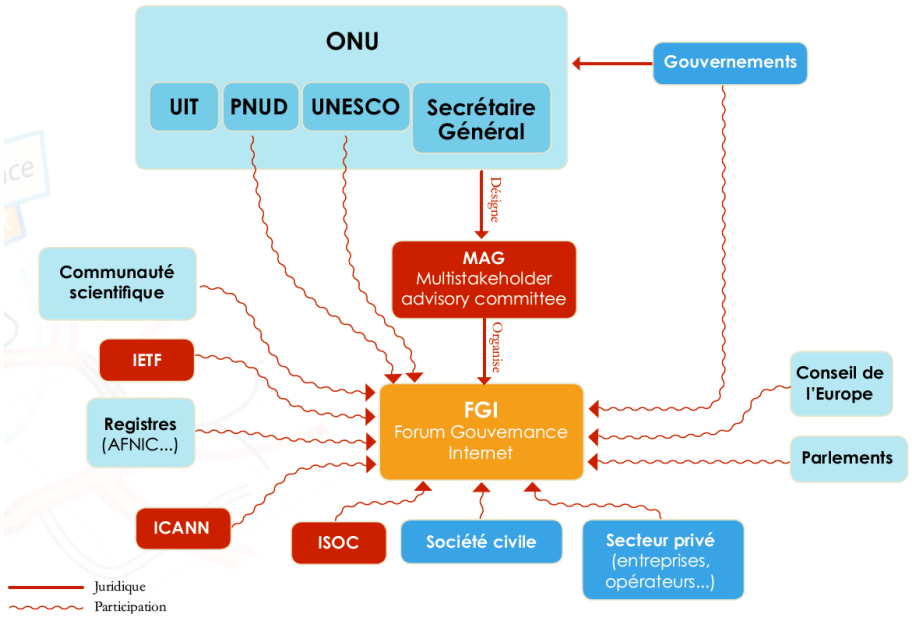


FIGURE 3.19 – L'univers du FGI
source : AFNIC, 2008

La première édition de ce forum a eu lieu à Athènes en octobre 2006. Là encore la volonté d'un processus multipartite engageant les États, les universitaires, les entreprises et la société civile a permis à chacun de comprendre le point de vue des autres. Il semble qu'il s'agisse du principal succès de ce sommet qui n'avait pas vocation à prendre des décisions.

La deuxième édition a eu lieu en novembre 2007 à Rio de Janeiro, la troisième à Hyderabad fin 2008. En 2014 le forum a eu lieu en Turquie ce qui est piquant sachant que le gouvernement a censuré Twitter l'année même.

3.4.3 Le monde associatif

L'ISOC, l'association des internautes

Créée en 1991, les mission de l'Internet Society sont :

— Promouvoir un Internet ouvert et accessible

L'ISOC milite pour un Internet libre et ouvert à tous, sans barrières économiques, géographiques ou politiques. Elle travaille pour assurer que l'Internet reste un bien public mondial, accessible à tous, sans discrimination.

— Défendre l'innovation et l'évolution d'Internet

Ce point technique est essentiellement dévolu à l'IETF qui travaille à la standardisation des protocoles Internet via les RFC.

— Développer la capacité et la gouvernance de l'Internet

L'organisation s'efforce d'éduquer et de renforcer les compétences des gouvernements, des entreprises, des ONG, et des utilisateurs dans le domaine de l'Internet. Elle offre des formations, des programmes de développement communautaire, et participe aux débats sur la gouvernance d'Internet.

— Assurer la sécurité, la confiance et la résilience de l'Internet

Ici le but est double, défendre une sécurité accrue sur Internet en soutenant des politiques et des technologies qui renforcent la confiance des utilisateurs et travailler à la résilience des infrastructures d'Internet face aux menaces telles que les cyberattaques ou les catastrophes naturelles.

— Favoriser l'inclusion numérique

Il s'agit de réduire la fracture numérique en travaillant avec des communautés sous-représentées ou mal desservies pour les connecter à Internet. Elle participe à l'extension des infrastructures Internet dans les régions éloignées ou en développement.

— Soutenir les droits numériques et la vie privée

La défense des droits de l'homme en ligne, notamment en matière de liberté d'expression et de protection de la vie privée, est un combat politique mené auprès des politiques. Aux États-Unis où la protection des données personnelles n'existe pas vu d'Europe, ce combat est d'autant plus important.

On retrouve ces différentes missions dans la répartition des dépenses de l'association en 2023 :

6,2 M$	pour aider les personnes à utiliser Internet
6,9 M$	pour participer à la croissance d'Internet,
7,0 M$	pour renforcer Internet
0,3 M§	pour l'IETF
1,0 M$	pour sa fondation
11,5 M$	en frais de fonctionnement
0,4 M$	de marketing et communication

Les rentrées d'argent propore sont dues en bonne partie à la gestion du TLD `.org` qui lui a été attribué par l'ICANN en 2002. Cela lui a apporté 28 millions de dollars en 2023, soit les 3/4 de son financement.

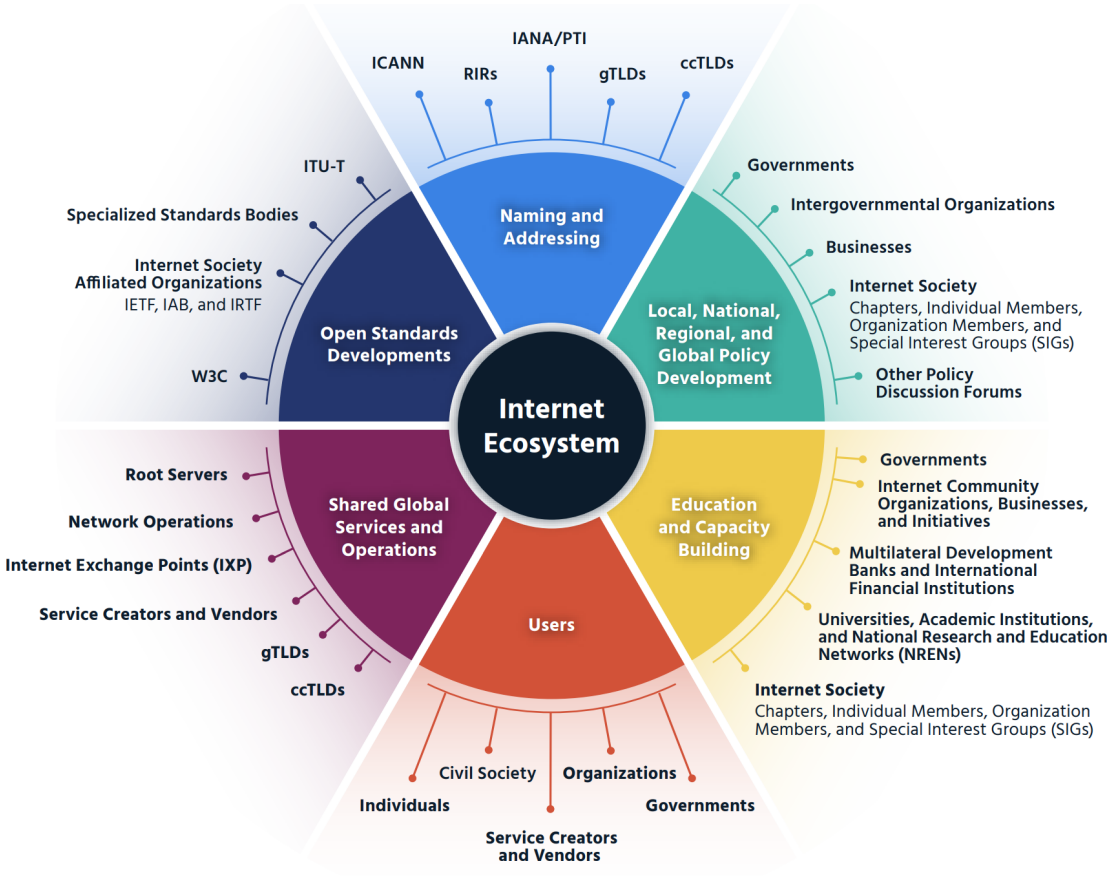


FIGURE 3.20 – Écosystème Internet vu par l'ISOC avec ses interventions
source : The Internet Ecosystem, ISOC, 2022

The Electronic Frontier Foundation

L'EFF est une association américaine dont le but est la défense de la liberté de parole et la protection de la vie privée sur l'Internet. Née en 1990, ses actions en justice sont une trace de l'histoire de l'Internet. Citons parmi ces procès gagnés par l'EFF :

- 1990 Affirmation de la protection de la correspondance privée sur Internet,
- 1995 Protection du code source par le 1er amendement défendant la liberté d'expression et donc l'interdiction faite au gouvernement des Etats-Unis de bloquer la diffusion de codes de cryptographie,
- 1996 Pas de différence légale entre Internet et le monde "réel" : abrogation d'une loi qui interdisait la publication de certains contenus sur Internet alors que les mêmes contenus pouvaient être légalement publiés en dehors de l'Internet,
- 2002 Procès de Karl Auerbach contre l'ICANN, cf page 109,

- 2004 la défense de deux développeurs du code de déchiffrage des DVD, DeCSS, afin de pouvoir les lire sous Linux. Le plaignant a finalement retiré sa plainte.
- 2005 Lutte contre le logiciel de surveillance (*spyware*) de DirectRevenu afin de connaitre les sites web visité par internautes pour leur proposé des publicités ciblées.
- 2011, 2014 Deux procès contre la surveillance étatique, contre le FBI et contre le département américain de la justice. Dans les deux cas l'État américain a du permettre plus de transparence et donner des documents sur la surveillance d'État.

Dans les procès perdus, notons celui de 2011 de Sony contre Hotz (soutenu par l'EFF) qui avait cassé la sécurité de sa PlayStation 3 pour y faire tourner son code et diffusé comment faire. Sony a utilisé avec succès le DMCA [33] et montré ainsi aux utilisateurs qu'ils ne peuvent pas utiliser librement leur machine.

L'EFF s'est aussi fait connaitre en développant la machine à casser le système de chiffrage DES, remplacé depuis par l'AES. Plus récemment, toujours dans le domaine de la sécurité, l'EFF a développé Certbot pour aider à la mise en place de certificats HTTP certifiés par Let's Encrypt.

Plus

Des sites sur la gouvernance :

— CercleID, http://www.circleid.com/
— Ars Technica http://arstechnica.com/tech-policy/
— ICANN Watch, http://www.icannwatch.org/

33. Digital Millennium Copyright Act, loi interdisant de contourner les protections informatiques d'un système (DRM).

Deuxième partie

Changement de monde

Chapitre 4

La communication

Internet est un média au moins aussi important que la radio ou la télévision, probablement plus si on pense au niveau mondial. En fait l'impact d'Internet sur notre société est tel qu'il est le plus souvent comparé à l'imprimerie. On parle de la révolution d'Internet comme on parle de la révolution de l'imprimerie qui a tué les moines copistes.

Avec Internet, tout citoyen dispose d'un mass média au bout des doigts. Avec Internet, l'article 19 de la déclaration universelle des droits de l'homme prend tout son sens :

> *Tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit.*

Internet redistribue les cartes de la communication.

4.1 Le Web

Le Web est l'application de référence sur Internet.

C'est une application tellement importante qu'il est fréquemment confondu avec Internet : "Cherche sur Internet", "J'ai ma page sur Internet". L'ironie est que le Web est probablement moins utilisé que le mail, mais le mail c'est le mail alors que le Web est Internet. La preuve : Google a fait fortune en permettant aux internautes de se retrouver dans le web. Qui a fait fortune avec le mail qui ne soit pas du mail via le web ?

Lorsque Tim Berners-Lee a inventé le web pour des besoins scientifiques il n'imaginait probablement pas le succès qu'aurait son invention. Aujourd'hui il s'agit non seulement de la plus grande source d'information mondiale, et de loin, mais aussi de l'outil qui a permis entre autres la liberté de *mass*-communication, les réseaux sociaux, les tweets, les wikis, ironiquement les web-services et demain d'autres applications totalement inattendues. Le web est non seulement une application mais aussi un support à la création.

Aussi regarder le web permet d'avoir une vision de l'importance d'Internet dans notre société, tant par l'information diffusée que par les nouveaux modes de communications qui s'imposent au monde physique [1]. Certains voient dans ce nouveau média un 5e pouvoir qui complète voire remplace le 4e pouvoir, la presse, aujourd'hui fortement affaibli.

Contrairement à ce que l'on peut supposer le Web n'est pas le même suivant l'endroit où l'on se trouve, même si l'ensemble du Web est accessible à tous (ou presque sachant que certains pays censurent des sites). Voici le classement des sites suivant différents pays (sites classés en fonction du nombre de visiteur unique) :

	France	Etats-Unis	Japon	Chine	Russie	Monde
1	Google Fr	Google	Google Jp	Baidu	V Kontakte	Google
2	YouTube	YouTube	YouTube	QQ	Google Ru	YouTube
3	Google	Facebook	Google	Taobao	YouTube	Facebook
4	Facebook	Reddit	Yahoo !	Tmall	Yandex	Baidu
5	Amazon	Amazon	Amazon	Sohu	mail.ru	Wikipedia
6	Wikipedia	Wikipedia	Facebook	Sina	OK	Reddit
7	leboncoin.fr	Yahoo !	Twitter	JD	Google	Yahoo !
8	Live	Twitter	Nicovideo	Weibo	Avito	Google Inde
9	Yahoo !	Netflix	Wikipedia	360	Aliexpress	QQ
10	Orange	Ebay	Rakuten	list.tmall	Wikipedia	Amazon

TABLE 4.1 – Classement des sites web les plus consultés
source : Alexa.com 01/2018

Parmi les moins connus pour un français

— Baidu et Yandex sont des moteurs de recherche,
— QQ est un système de messagerie instantanée,
— Sina, Sohu et mail.ru sont des portails,
— V Kontakte et OK sont des réseaux sociaux,
— Tmall, JD, Rakuten et Taobao sont des sites de commerce en ligne,
— Weibo un site de micro-blogging,
— 360 un site de sécurité informatique,
— Avito est un site de vente d'occasion.

On voit que notre vision du Web est très occidentale et qu'en Orient, l'Orient commençant à Moscou, les poids lourds du Web ne sont pas obligatoirement les mêmes. Ces pays du fait de leur marché économique important, leur différences culturelles et la volonté étatique [2], arrivent à contrer les références mondiales chez eux ainsi que dans leurs pays voisins, où on trouve un mélange de site occidentaux et de sites provenant du grand frère (Taïwan, Corée du Sud, les anciens états soviétiques).

Au niveau de la fréquentation mensuel, les 3 premiers mondiaux dépassent le milliard de

1. par exemple les politiques se plient à l'exercice du tweet et du blog.
2. En Chine ou en Iran l'État censure et ainsi favorise les sites nationaux

visiteurs uniques par mois. Ensuite cela baisse vite. Des chiffres de 2011 [3] de Google indiquait que le taux de pénétration d'un site web baisse très rapidement :

— le 20e site ne touche que 7,7% des internautes,
— le 100e touche 2%
— le 1000e seulement 0,3%.

Cet aspect est très important pour les revenus publicitaires et ce d'autant plus qu'un site web important peut imposer des tarifs plus élevés.

4.2 L'information traditionnelle ébranlée

Tout comme l'imprimerie en son temps, Internet a démultiplié la diffusion de l'information. Réservée avant aux journalistes et aux élites, la diffusion en masse est devenue à la portée de tous avec Internet. Les coûts d'une publication sont devenu très modestes puisqu'un un simple accès au web est suffisant. Les compétences techniques nécessaires ont été largement réduites au fil du temps pour qu'elles ne soient plus un obstacle. La seule difficulté reste le contenu qui doit être à la hauteur des attentes de son public. Si on se focalise sur le contenu de type journalistique, il est remarquable de noter le grand nombre d'internautes qui propose des articles de très bonne qualité. Aussi il n'est pas surprenant que les médias traditionnels se fassent du mouron, la concurrence est devenue rude et surtout gratuite. Ainsi je peux lire sans intermédiaire le blog d'un ministre, d'un procureur, d'un scientifique, d'un artiste et même découvrir les pensées d'un ado, d'un ouvrier, d'un militant... Je peux aussi lire des journaux collaboratifs, regarder des vidéos sur Youtube, suivre les événements en direct sur Twitter... Enfin je peux accéder à l'information où qu'elle soit, sans limitation de frontières.

Aujourd'hui l'information vient autant d'Internet que des médias traditionnels ce qui oblige ces dernier à exister sur Internet sous peine d'être marginalisés. Comme l'information y est traditionnellement gratuite et qu'il est difficile de faire payer l'internaute, les médias classique proposent gratuitement leur contenu ce qui les met en porte à faux vis à vis de leurs éditions papier payantes [4].

L'arrivée de l'imprimerie a été la fin des moines copistes pour le meilleur, on peut donc espérer le meilleur pour l'avenir avec de nouveaux types de journalisme plus libres et plus pertinents qu'avant.

4.2.1 La presse en ligne

Si Médiamétrie publie l'audience mensuel des sites web en France, ses résultats basés sur les sondages ont été contesté par des sites web qui ne retrouvaient pas les chiffres annoncés dans leurs logs (Slate en particulier). Depuis 2012 MediaMétrie et OJD ont signé un accord pour mélanger les données provenant de sondages aux données numériques de mesure des sites

3. cela n'a pas dû changer
4. En France, seul le vilain petit canard résiste et refuse de barboter sur le net.

web. Cela étant il n'est pas toujours très clair de savoir à quoi correspondent exactement les chiffres et leur solidité.

Les chiffres de l'ACPM [5] donnés ci-dessous proviennent des déclarations sur l'honneur des différents médias qui a aussi probablement ses limites.

Rang	Sites	Visites totales	Visites site web fixe	Visites site web mobile	Pages vues totales	Pages vues par visites
1	Orange	330521032	330521032		2768140340	8,4
2	LeFigaro	110358424	51083957	59274467	271596114	2,5
3	LeMonde	101450829	49457823	51993006	298231256	2,9
4	Tele-Loisirs	83120677	41495787	41624890	200018805	2,4
5	L'Equipe	77586002	40657125	36928877	402080410	5,2
6	Bfmtv	76331192	15783527	60547665	141839523	1,9
7	20minutes	74933786	26125329	48808457	178221884	2,4
8	Franceinfo	60382776	28395397	31987379	101627348	1,7
9	LeParisien	57363901	27024255	30339646	108454903	1,9
10	Gentside	48827742	5498757	43328985	95213132	2,0
11	Ouest-france	47611848	24838467	22773381	199321079	4,2
12	Ohmymag	47098111	4542614	42555497	91932580	2,0
13	Huffingtonpost	45179093	13439056	31740037	67770660	1,5
14	Doctissimo	36953145	10220415	26732730	79921415	2,2
15	Femmeactuelle	36085050	20178446	15906604	129868924	3,6
16	Gala	34253160	14297938	19955222	123638342	3,6
17	Voici	32364362	12719387	19644975	93092835	2,9
18	L'Obs	31471000	15884422	15586578	73158368	2,3
19	Footmercato	30736447	7811550	22924897	94566510	3,1
20	Lexpress	30234596	14588268	15646328	59436130	2,0

TABLE 4.2 – Classement des sites de presse grand public en France en décembre 2017
source : APCM

Si en général la fréquentation des sites web est donnée en visiteurs uniques et donc qu'on ne compte qu'une fois le visiteur qui est venu 5 fois sur le site dans le mois, le tableau 4.2 compte les visites simples ce qui rend tout comparaison avec les autres sites web impossible. Par contre on peut comparer avec la presse traditionnelle.

Orange est en tête avec 330 millions de visite dans le mois. Si on veut bien croire qu'il ne s'agit que de la partie information et non pas les connections pour gérer son abonnement, cela fait environ 10 millions de visites par jours. Pour le Figaro et le Monde on est à 3 millions de visites par jours. Le nombre de page par visite laisse penser qu'une visite est un article lu [6]

5. Alliance pour les chiffres de la presse et des médias

6. Le nombre de pages vues est une information délicate à prendre en compte car un site mal fait qui passe son temps à vous rediriger augmentera le nombre de pages vues par visite (le chiffre important pour Orange de pages vues par visite laisse craindre qu'il s'agisse de tout son site, y compris les pages liées à son abonnements qui sont toujours incompréhensibles et vous renvoient à d'autres pages).

Comparaison des différents canaux Voici les chiffres pour les quotidiens nationaux :

Titre	Diffusion payée	Évolution en %
Le Parisien + Aujourd'hui en France	334226	-2.89
Le Figaro	306737	0.44
Le Monde	278790	5.38
L'Equipe	233131	1.92
Les Echos	128215	0.58
La Croix	91095	-1.06
Libération	75824	-1.66
L'Humanité	34877	-4.37
The New York Times	14212	-7.12

TABLE 4.3 – Classement de la diffusion des quotidiens en France – 2016-2017
source : APCM

Si on considère qu'un lecteur qui achète son journal va lire 10 articles, on trouve quasiment le même chiffre pour la lecture via le support papier ou via le site web pour le Figaro et le Monde.

Pour comparer nos chiffres à la télévision, regardons les journaux télévisés (JT). Un JT de 20h fait entre 5 et 6 millions de téléspectateurs pour chacune des deux premières chaines soit environ 11 millions de téléspectateurs à elles deux. Si on estime qu'un JT correspond à la lecture de 10 articles alors un JT est nettement plus vu que les sites web ou les journaux papier.

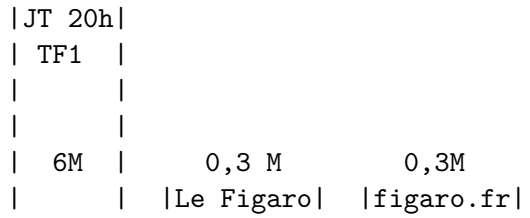


FIGURE 4.1 – Comparaison à la louche des *lecteurs* quotidiens entre la TV, le papier et le web

Donc pour les grands quotidiens papier, leur diffusion papier ou par le web est équivalente et reste largement en dessous de la diffusion de l'information par la télévision.

Internet vs la télévision Il semble donc que la télévision reste le principal canal d'information. En fait le temps moyen passé devant la télévision est tellement important qu'il est difficile d'imaginer qu'Internet puisse la dépasser. Et pourtant...

Un français de plus de 4 ans passe en moyenne 4 heures devant la télévision par jour (un jeune entre 15 et 34 ans regarde 2h10 par jour alors qu'une personne de plus de 50 ans regarde 5h44

par jour en moyenne)[7]. On constate que la télévision est un truc de personnes agées et que les jeunes y sont nettement moins accrochés que leurs ainés.

Si on compare la fréquentation de ces deux supports on voit qu'Internet devient aussi important que la télévision, cf figure 4.2.

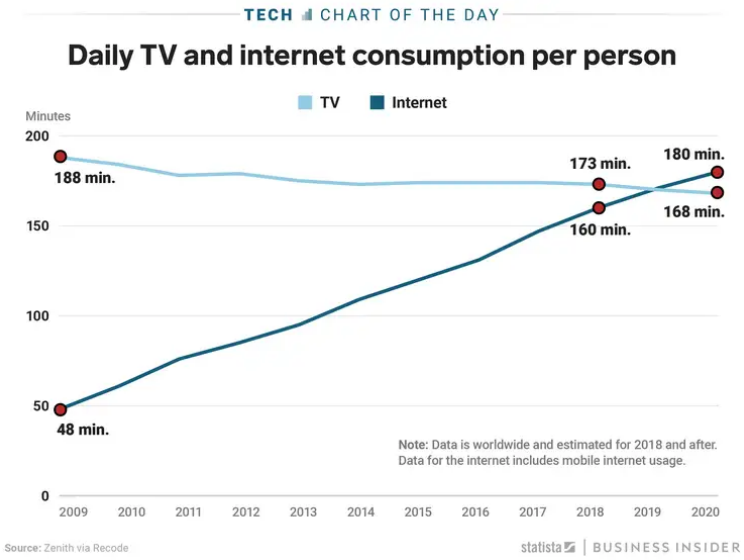


FIGURE 4.2 – Temps passé devant la TV vs Internet en tant que spectateur

Si on regarde par âge (figure 4.3) on retrouve le décalage générationnel de consultation de la télévision et on comprend que non seulement les téléspectateurs deviennent aussi des internautes[8] mais aussi que les jeunes générations sont principalement sur Internet et y reste en vieillissant. Ainsi tout doucement Internet prend de plus en plus de place et va devenir la source d'information principale.

Le décalage que l'on voit entre le JT qui surclasse largement le site web du Figaro et cette figure qui souligne l'importance d'Internet pour s'informer chez les jeunes, vient des canaux d'information qui dépassent largement ceux de la presse traditionnelle. Ainsi le site d'information collaborative Reddit est en 2018 le 6e site le plus visité aux États-Unis, très loin devant le premier site de presse.

Avec Internet, il ne s'agit pas seulement d'un changement de support mais aussi d'un changement de sources d'information.

La presse papier

Il n'y a plus de doute que la presse papier souffre de la concurrence d'Internet, concurrence qui devient de plus en plus rude avec les nouveaux modes d'information.

7. chiffres janvier 2018 de MédiaMetrie
8. la progression nette de l'utilisation d'Internet pour s'informer pour les personnes de plus de 65 ans en est le

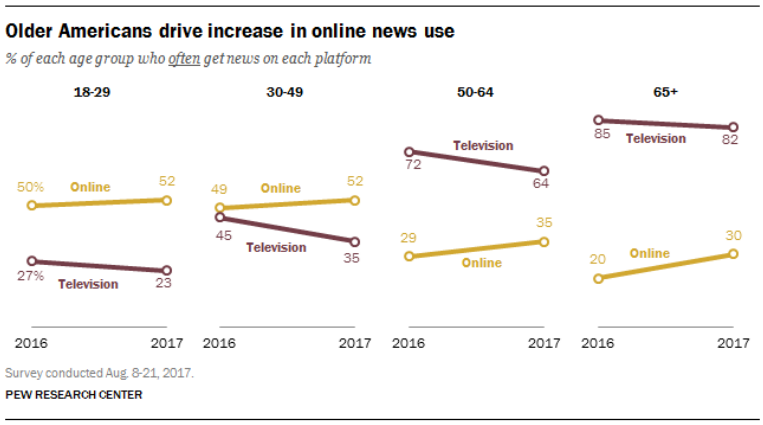


FIGURE 4.3 – Fréquence d'utilisation de la TV et d'Internet pour s'informer aux EU

La première faiblesse de la presse traditionnelle est son prix. Alors que le journal papier est payant, l'information est gratuite sur Internet et le journal qui oserait de ne pas diffuser son information gratuitement sur son site web, prendrait le risque d'une perte de visibilité importante.

De plus qualité des journaux est le plus souvent insuffisante pour lutter contre l'information sur Internet. On y retrouve la même chose voire plus intéressant comme le souligne le journaliste Éric Scherer dans son livre *A-t-on encore besoin des journaliste ?* :

> *Les causes de cette accélération de la défiance [vis à vis des médias d'information] sont multiples. Citons en quelques unes : le public voit bien désormais, via Internet, le manque de sérieux des exclusivités, et parfois des expertises, s'aperçoit que les informations, qui viennent le plus souvent des agences de presse ou de communiqués de presse, sont à peu prêt partout les mêmes, se désole de la pauvreté, du manque de courage et de suivi dans les questions posées aux grands de ce monde.*

Enfin un journal est statique et rigide. Il offre la même sélection d'articles à tous ses lecteurs. À l'inverse Internet offre la possibilité de créer son propre journal à l'aide d'agrégateurs où l'on peut combiner des articles de journaux traditionnels à des articles de blogs, des tweets, des photos... suivant la mise en page de son choix.

Ainsi, pour un effort ridicule, il est possible d'avoir mieux pour moins cher.

Un cas intéressant dans le domaine des agrégateurs et celui de Google News. Ce site aspire les articles des différents journaux et les présente tous dans l'ordre chronologique après avoir permis à l'utilisateur de filtrer les articles par sa recherche. Pour les journaux c'est un bien et un mal. Un bien car leurs articles sont mis en avant et un bon article va ramener des lecteurs sur le site du journal, un mal car les lecteurs risquent de négliger les pages web des journaux avec les publicités et aller seulement lire l'article et quitter le site ensuite. Comme Google a mis son service en ligne sans demander l'avis des journaux cela lui a valu des procès suite à quoi Google n'aspire plus les journaux qui ne le désirent pas. Cela ne convient pas non plus à ces journaux qui disparaissent par la même occasion du moteur de recherche de Google ce qui est lourd en terme de visibilité et donc de revenus publicitaires.

signe le plus clair

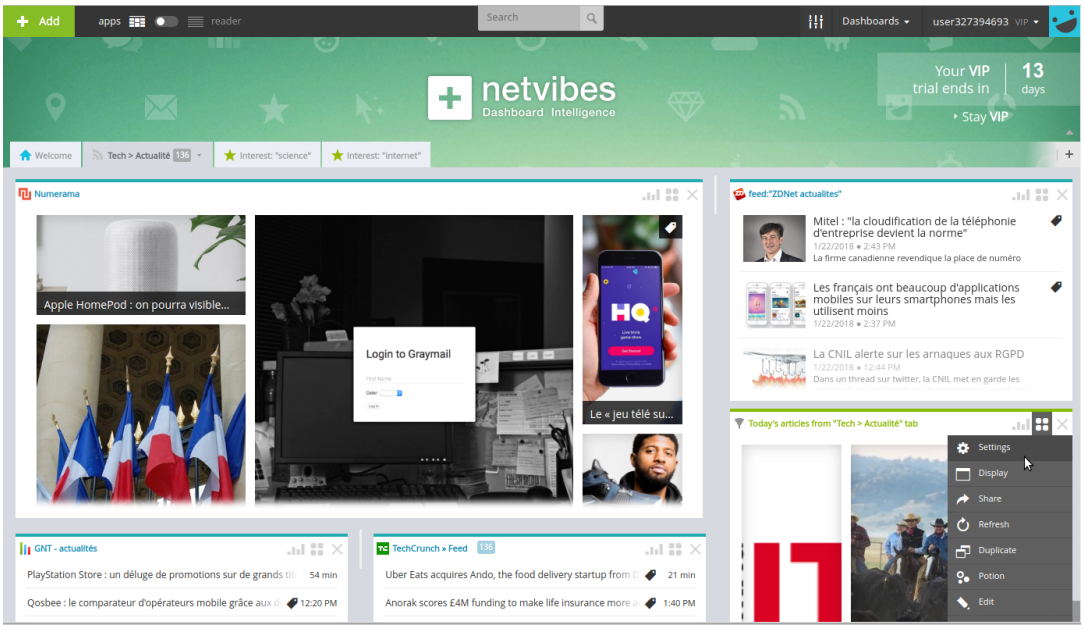


FIGURE 4.4 – Netvibes, un exemple d'agrégateur
L'utilisateur choisit et met en page ses flux

Finalement la solution a été technique. Aujourd'hui les journaux ne laissent visible que le début de leurs articles [9] entièrement lisibles, ce qui suffit pour qu'ils soient référencés mais ce qui pousse le lecteur à s'abonner pour lire l'article en entier.

Vers un nouveau journalisme

In fine il n'est pas impossible que demain les journalistes deviennent des fournisseurs de flux, le travail du journaliste étant alors alors d'extraire de la surabondance d'information actuelle des articles éclairés, vérifiés qui aident le lecteur internaute à gagner du temps. Quelques journalistes iront encore chercher l'information mais le monde étant connecté et le moindre téléphone étant un témoin, leur rôle ne sera pas aussi important qu'il l'a été.

On aura ainsi les blogueurs gratuits, les blogs actuels, et les blogueurs payants ou professionnels, les journalistes d'aujourd'hui reconvertis et des blogueurs qui franchiront le pas. Parfois ces nouveaux journalistes se filment ou s'enregistrent et on regarde et écoute à la carte. Tout cela donne de nouveau modèles économiques dit *pure player* qui n'existe que sur Internet et vivent des abonnements.

En France on a ainsi Daniel Schneidermann, licencié de France 5, qui a monté en 2007 @rret sur images, [illegible]ctualité accessible en petite partie librement et complètement sur abonnement. En 2016 le site a dégagé un bénéfice 137 k€ avec 28000 abonnés à 40 euros

9. parfois des articles sont entièrement lisibles pour découvrir le journal.

par an [10],
— Edwy Plenel, ancien du Monde, a créé Mediapart en 2008 avec une formule exclusivement d'abonnement. À l'équilibre début 2011 avec 47 500 abonnés à 9 euros par mois [11], en 2017 Médiapart a eu un CA de 11 M€ pour 130 000 abonnés et 74 salariés.

4.2.2 Les blogs

Le blog est le descendant direct de la page personnelle, réservée à l'époque à ceux qui comprenaient un minimum l'informatique. Avec les blogs et des sites spécialisés [12] pour permettre à n'importe qui peut facilement publier, tout le monde peut écrire son journal ou ses pensées. Non seulement il n'est nul besoin d'être informaticien mais en plus le coût est gratuit, pas de serveur à acheter ou louer, pas de copain informaticien à implorer pour faire marcher la mécanique.

C'est donc sans surprise que le nombre de blogs a explosé. On estimait à 170 millions le nombre de blogs en 2011 [13], en 2018 il est probable que les 500 millions soient atteint.

Si parmi ces blogs un grand nombre sont inactifs, si une énorme majorité est de qualité médiocre ou destinée à une diffusion restreinte, si un bon morceau est correct sans toute fois atteindre un niveau journalistique, un petit pourcentage est de très bonne qualité, supérieure à bien des journaux. Que ce petit pourcentage soit de 0,1 % et cela donne 500 000 blogs intéressants à lire. Si on considère que tous les sujets ne nous intéressent pas, si on ne lit pas toutes les langues de notre planète [14], il reste quand même largement de quoi remplir ses journées.

Nous ne présenterons pas ici une sélection de blogs qui de toute façon serait incomplète, partiale et donc sujette à discussion. D'autres s'y hasardent comme le montre une recherche avec les termes "Best blog" ou "Meilleurs blogs" ce qui peut permettre de commencer à construire sa liste. On peut néanmoins citer quelques blogs connus qui ont assez de lecteurs pour les considérer comme importants voire influents :

— **538**, http://fivethirtyeight.com/, le blog de Nate Silver, dont le modèle mathématique avait prédit correctement les votes dans 49 et 50 états lors de l'élection du président des États-Unis en 2008, a prédit correctement les votes des 50 états en 2012. Son succès est d'autant plus remarquable que grand nombres d'experts et de journalistes politiques se sont lourdement trompés. Le site a eu environ 6 millions de visiteurs chaque jour dans les derniers jours de la campagne. En 2016 il s'est trompé et n'avait pas prévu que Trump gagne, comme tout le monde.
— **Blog del Narco**. http://www.blogdelnarco.com/, publie des informations sur la guerre menée contre les narco-trafficants au Mexique. Les deux auteurs ont voulu publier ce que les médias n'osaient pas publier par peur des représailles. Fin 2010 il avait 3 millions de visiteurs mensuel, en 2012 il était le site le plus consulté au Mexique (le 208e site

10. formule principale, d'autres types d'abonnement existent.
11. là aussi d'autres formules existent
12. Blogger, Wordpress, OverBlog, Tumblr...
13. http://www.nielsen.com/us/en/insights/news/2012/buzz-in-the-blogosphere-millions-more-bloggers-and-blog-readers.html
14. même si les traducteurs automatiques ont fait des progrès impressionnants ces dernières années.

mondial d'après Alexa fin 2012).

— **Il blog di Beppe Grillo** , http://www.beppegrillo.it/, est le blog d'un comique, acteur, activiste, politicien italien. Ce blog, ouvert en 2005, est devenu une référence en Italie où il a été le 82e site web le plus vu en Italie. En 2008 le Guardian l'a classé dans les 10 blogs les plus puissants [15]. En 2013 le parti de Beppe Grillo, le mouvement 5 étoiles, est crédité de plus de 15 % des voix aux législatives alors même qu'il ignore la télévision. En 2016 le parti remporte les villes de Rome et de Milan. Fin 2017 Beppe Grillo pert la direction de son parti.

— **Mashable** , http://mashable.com/, fondé par Pete Cashmore en tant que blog spécialisé dans la culture numérique, les réseaux sociaux et la technologie est devenu avec le temps un média de référence ses 45 millions de visiteurs uniques fin 2017 date à laquelle il a été vendu pour 50 M$ au groupe de presse Ziff Davis.

Enfin notons qu'un blog peut être très rentable :

Site	Revenus mensuels en $
Huffington Post	14 000 000
Engaget	5 500 000
Moz	4 250 000
TechCrunch	2 500 000
Mashable	2 000 000
CopyBlogger	1 000 000
Perez Hilton	575 000
Gizmodo	325 000
Smashing Magazine	215 000
Tuts+	175 000

TABLE 4.4 – Classement des blogs les plus lucratifs
source : Forbes 2017

Des agrégateurs de blogs tout prêt

Certains sites web font un tri des articles qu'ils apprécient pour les servir. Il effectue donc un travail éditorialiste tel que pourraient le faire les journaux de demain. Voici deux sites connus dans le domaine.

Global Voices propose une sélection d'articles de blogs qui parlent de ce que les médias traditionnels taisent. Pour cela Global Voices s'appuie sur des volontaires qui rabattent les articles et surtout traduisent les meilleurs. Ce choix permet d'avoir dans sa langue le point de vue de différents blogueurs à travers la planète et pas des seuls anglophones ou francophones. Ainsi un blogueur russe parle de l'exil des élites de Russie, un libanais présente sa vision des sur les événements en Syrie, un angolais rapporte une manifestation locale...

15. http ://www.guardian.co.uk/technology/2008/mar/09/blogs

FIGURE 4.5 – Global Voices en français

Le Drudge Report, créé en 1997 pour sa version web, est probablement le premier agrégateur d'articles de presse, cf figure 4.6. Il publie parfois des articles, son article le plus important étant probablement l'annonce que le journal Newsweek bloquait un article sur les relations entre le président Clinton et une stagiaire. Suite à cette annonce, Newsweek a publié l'affaire Lewinsky.

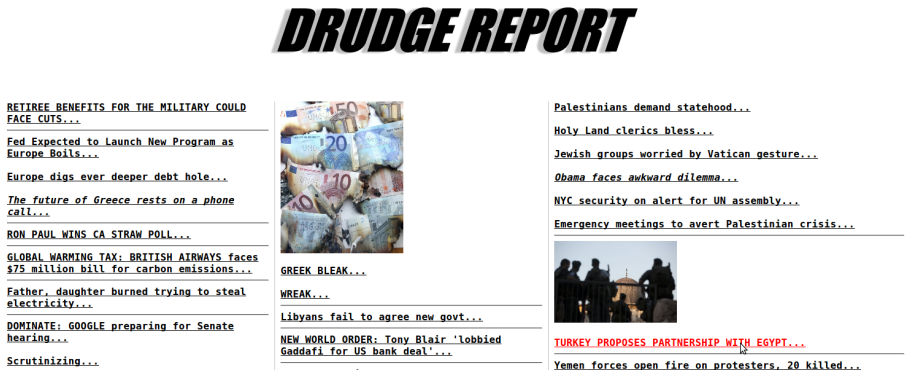


FIGURE 4.6 – Le Drudge Report

Cet assemblage de blogs existe aussi sur les sites web des quotidiens papiers avec des articles

en plus de la rédaction ou de proche de la rédaction. Ainsi Le Monde enrichit son site web avec des blogs de journalistes, d'amis des journaliste et de candidats journalistes. Libération fait de même avec sa sélection de blogs. Libération et Les échos présentent les blogs de leurs journalistes.

4.2.3 Les journaux collaboratifs

La révolution Internet ayant déjà bouleversé le monde journalistique, il n'est pas surprenant que des journalistes aient tenté de nouveaux modèles. Mediapart et @rret sur image sont des journaux virtuels par abonnement avec de petites équipes de journaliste. Certains blogs sont devenus des sources d'information importante que convoitent les journaux traditionnels. Ainsi Médiapart à une version dite Le Club qui héberge des blogs des abonnés.

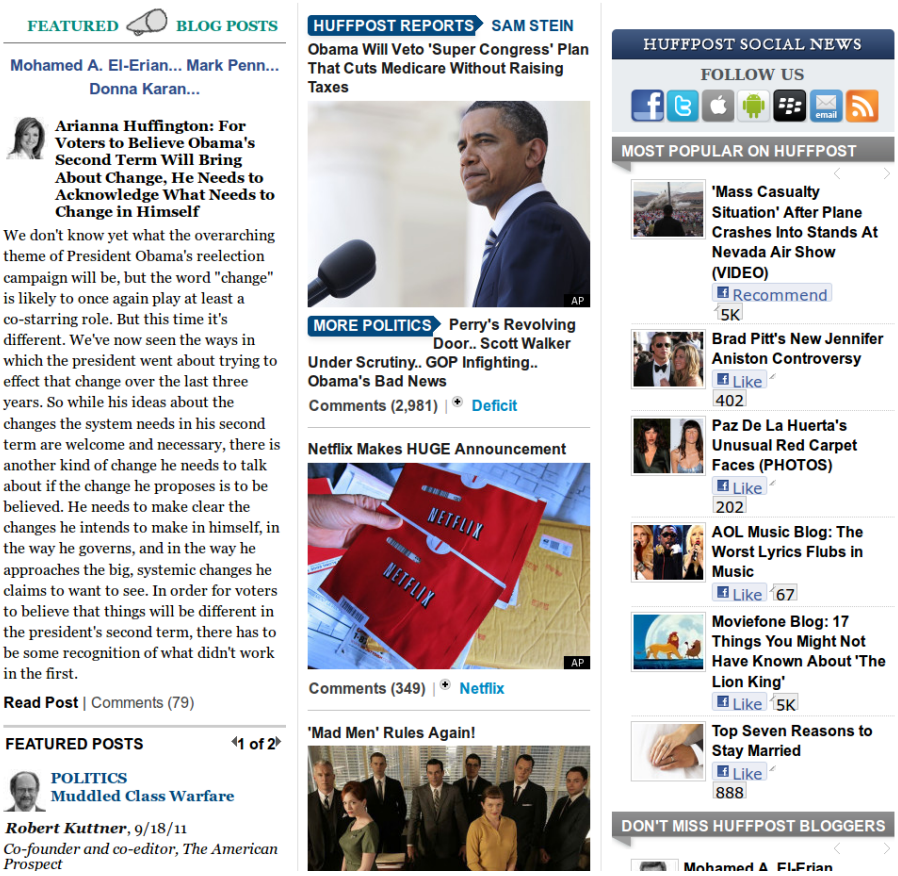


FIGURE 4.7 – Le Huffington Post avec l'édito de sa fondatrice

En 2007, des anciens de Libération ont été plus loin puisqu'ils mélangent les articles de blogs et de journalistes pour créer le journal virtuel Rue89. Il s'agit d'ajouter aux articles des journalistes des articles proposés à la rédaction par qui veut. Ainsi chacun peut devenir un journaliste bénévole et profiter de l'audience d'un journal reconnu.

Un cran plus loin, Agoravox est un journal entièrement basé sur le volontariat, tant pour l'écriture des articles que pour leur sélection avant publication. En 2011, soit 6 ans après sa création,

Agoravox comptait 70 000 rédacteurs et 1 900 modérateurs.

Bien sûr ces expériences françaises ont leur sources dans des expériences anglo-saxonnes de plus grande échelle. L'exemple de référence étant le Huffington Post.

Le Huffington Post créé en 2005 propose ses articles, des articles d'autres journaux ainsi que ceux de milliers de blogueurs, cf figure 4.7. Son succès lui a permis d'avoir des versions locales à certaines grandes villes américaine et d'avoir en plus de la version etats-uniennes, une version Canadienne et une version Anglaise. En 2011, soit après 6 années d'activité, ce journal a été acheté pour 315 millions de dollars par AOL.

4.3 L'éducation

Un bon formateur a ce souci constant : enseigner à se passer de lui.

André Gide

L'éducation est surtout de la communication dans le but de transmettre le savoir. Avec Internet cette transmission du savoir prend de nouvelles formes.

L'éducation à distance est bien antérieure à l'Internet, le CNED [16] existe depuis 1939, quand à l'auto-apprentissage il existe au moins depuis que les bibliothèques existent. La spécificité de l'Internet dans ce domaine est de coupler les connaissances en ligne avec la communauté des forum toujours prête à donner un coup de main. Il n'y a plus de professeurs qui guident mais des centaines de pairs qui aident.

Le premier domaine à avoir pleinement profité de l'apprentissage en ligne est naturellement l'informatique. N'importe quel jeune désirant apprendre pouvait, et peut toujours, non seulement trouver tous les cours possibles en ligne mais aussi de l'aide et, cerise sur le gâteau, des projets libres où mettre en pratique son apprentissage guidé par les mentors des projets. Les logiciels libres ont montré qu'ils sont une très bonne école à tel point qu'inscrire dans son CV une participation significative à un projet libre vaut bien des diplômes aux yeux des recruteurs du domaine.

Aujourd'hui la connaissance est disponible dans tous les domaines, les centres d'*e-learning* sont pléthore. Des universités, dont le célèbre MIT et le non moins célèbre Collège de France, mettent en ligne leurs cours. TED diffuse ses conférences mais les organisateurs de conférences diffusent de plus en plus souvent les interventions des orateurs, parfois en direct. Des individus expliquent leur domaine à travers des vidéos, des blogs, des forums spécifiques, et bien sûr Wikipedia est toujours plus riche.

Là encore le monde change, rien ne garantit que les cours en amphi ont encore de l'avenir, peut-être que les universités les plus prestigieuses vont récupérer l'élite mondiale via leurs enseignements en ligne, peut-être qu'un étudiant validera différents modules dans différentes université à travers le monde, peut-être que les entreprises offriront des modules dans leurs spécialités. Quoi qu'il en soit, l'enseignant de demain fera probablement un métier différent de celui d'aujourd'hui.

16. Centre National d'Enseignement à Distance

4.3.1 L'université en ligne

Le monde de l'enseignement supérieur est en effervescence pour ne pas dire en pleine révolution. Avec Internet l'enseignement à distance devient de plus en plus confortable et si on peut apprendre à distance dans de bonnes conditions, pourquoi aller dans l'université minable à coté de chez soi alors que les plus grandes université à l'autre bout du monde nous ouvrent leurs portes ?

La compétition entre les universités a toujours existé, pour accueillir les meilleurs étudiants, les meilleurs chercheurs, les meilleurs enseignants. Avec Internet deux paramètres changent :

— la couverture d'une université n'est plus locale mais mondiale,
— le numérique permet d'accepter un nombre infini d'étudiants pour un surcout faible.

Dans cette compétition mondiale la langue de référence est l'anglais ce qui apporte un avantage certain aux universités anglo-saxonne qui sont aussi les plus réputées.

Les projets

OCW Le MIT, Massachusetts Institute of Technology, a proposé le premier ses cours en ligne gratuitement avec la volonté affichée d'offrir tous ses cours en ligne. Le MIT Open Courseware, OCW, lancé en 2001 a été depuis rejoint par Harvard, ParisTech, l'université de Pékin et l'université de Kyoto.

D'autres projets ont vu le jours par la suite dans le but de partager la connaissance et d'offrir un accès libre aux cours à tous.

Khan Academy En 2004 Salman Khan a expliqué à distance les maths à ses cousins via des vidéos qu'il a posté sur YouTube. Rapidement ses vidéos sont devenues populaires et ce succès l'a poussé à créer la Khan Academy en 2006. Il s'agit là de courtes leçons de l'enseignement secondaire et qui tirent partie des possibilités qu'offrent l'informatique en mélangeant les vidéos aux exercices interactifs.

En 2013, Salman Khan a publié plus de 4000 petites leçons dans un grand nombre de disciplines. Il est soutenu par la fondation Gates et par Google. La traduction des leçons dans les langues les plus connues est en cours.

Coursera Créé par Andrew Ng et Daphne Koller de l'Université de Stanford, Coursera a pour but d'offrir le plus largement possible des cours de qualité. Pour cela, elle regroupe regroupe 62 universités à travers le monde [17], plus de 200 cours et presque 3 millions d'étudiants [18] début 2013.

Coursera a levé 16 millions de dollars en 2012. Son plan d'affaire est en cours de définition.

17. l'école Polytechnique pour la France
18. avec une progression supérieure à celle de Facebook

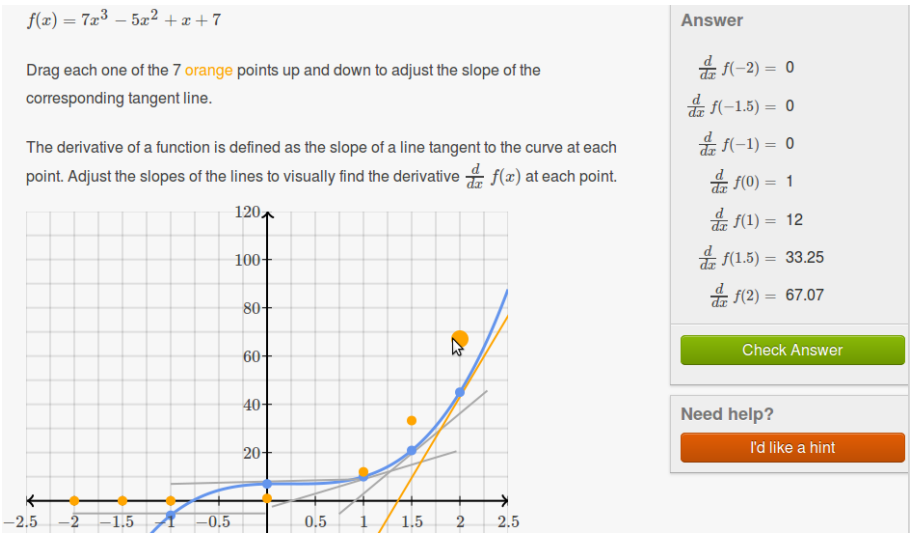


FIGURE 4.8 – Khan Academy - leçon interactive sur les dérivées

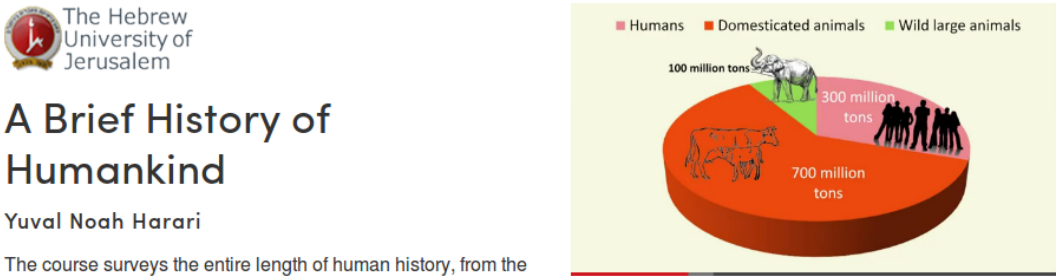


FIGURE 4.9 – Coursera – un cours sur l'histoire de l'humanité

EdX est un projet créé par Harvard et le Massachusetts Institute of Technology en 2012. Le MIT avait déjà mis en ligne certains de ses cours et inscrit des étudiants en ligne. Le cours d'électronique de décembre 2011 a accueilli 150 000 étudiants dont 10 000 ont passé l'examen final. Début 2013, le projet a accueilli 6 universités tout aussi célèbres, cf figure 4.10. Avec de tels noms, le potentiel de ce projet semble très important.

FIGURE 4.10 – EdX « *Explore free courses from leading universities* »

Les deux universités fondatrices ont investi 60 millions de dollars dans le projet avec de grandes ambitions :

> *"I Want to Teach Engineering to a Billion"*
> Anant Agarwal, président d'EdX

FIGURE 4.11 – EdX – un cours de philosophie d'Harvard

L'éducation ouverte

Le bon coté de la chose est que les cours de ces différents projets sont librement accessibles [19]. Les fondateurs de Coursera soulignent l'injustice du modèle classique où seuls les favorisés (au niveau planétaire) ont accès à une éducation supérieure de qualité. Avec l'enseignement en ligne, non seulement on peut faire des cours pour des centaines de milliers d'étudiants à travers le monde, mais en plus on peut proposer les meilleurs cours des meilleures universités.

Ainsi des étudiants des pays en développement peuvent suivre de tels cours avec un simple accès Internet. Des personnes entrées dans la vie professionnelles peuvent se remettre à étudier. Des personnes qui ne peuvent pas se déplacer physiquement, là encore peuvent apprendre. Le plus intéressant est que ces cours se valident et permettent d'obtenir des emplois et d'entrer dans des universités classiques. Il est probable qu'ils permettront d'obtenir des équivalences de diplômes via la VAE [20].

Enfin notons que le passage à l'échelle offre des opportunités pédagogiques. Avec une classe de 100 000 étudiants répartis à travers le monde, les forums associés au cours ont des intervenants 24h/24 qui peuvent répondre aux questions des autres. De plus, comme le système est informatisé, il est possible de suivre le comportement de chaque étudiant, ses clics, ses réponses aux différents exercices, ses interventions dans les forums, sa façon de suivre les vidéos, etc. Toutes ces données transforment fondamentalement la recherche en pédagogie et permettent de comprendre des comportements, des biais, qui ne sont pas visibles à petite échelle. On peut donc s'attendre à des évolutions prochaines dans l'enseignement, le but ultime étant le précepteur numérique pour chacun.

19. il existe des projets payant comme Udemy par exemple
20. la validation des acquis de l'expérience

4.3.2 Conférences en ligne : TED

Les conférences en ligne sont arrivées naturellement lorsque les tuyaux de l'Internet l'ont permis. Cela a commencé par des conférences académiques filmées puis rapidement sont arrivées les conférences dédiées [21] à Internet. La référence dans ce domaine est TED [22].

Si TED a été créée en 1984 dans le monde réel, elle a explosé avec son arrivée sur Internet et la mise à libre disposition de ces exposés en 2006. Ces exposés de 18 minutes sont présentés par des célébrités politiques, scientifiques, culturelles, associatives... Ce format permet de faire des exposés coup de poing où des grandes idées, projets ou innovations sont présentés pour le grand public. En 2013 TED offre un catalogue de 1400 exposés.

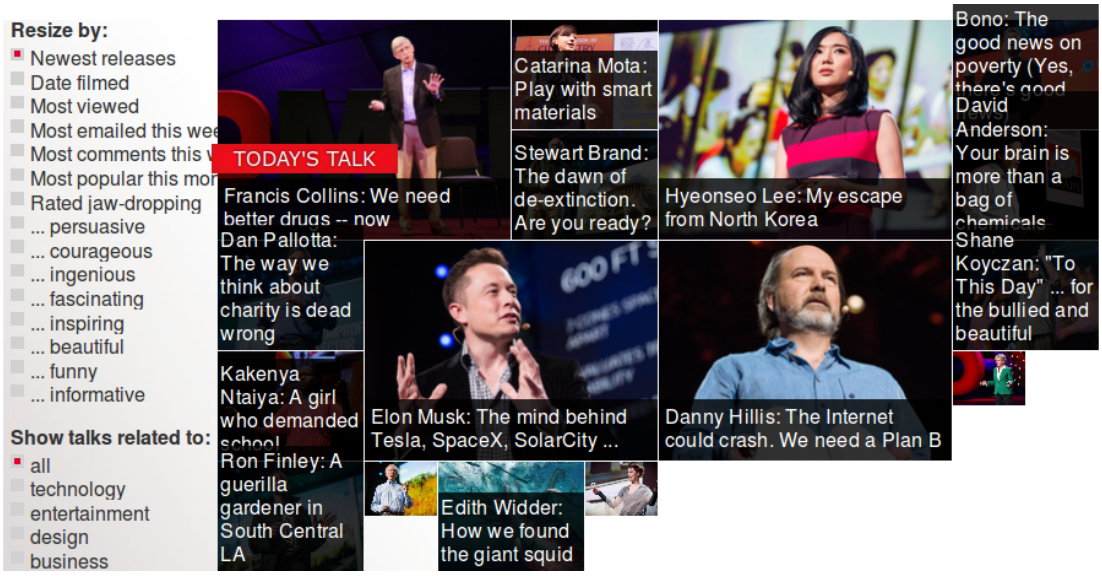


FIGURE 4.12 – TED – Ideas worth spreading

La mise en ligne des conférences de TED diffuse auprès du grand public ce qui était réservé à un public restreint.

La mise en ligne des conférences académiques et des séminaires de recherche, comme les Google Tech Talks, permet aux chercheurs, étudiants et passionnés, de multiplier les possibilités de suivre ce qui se fait en temps réel. Il ne s'agit pas d'un changement aussi important que celui de l'enseignement en ligne, mais ce changement améliore notablement la transmission d'information et donc l'efficacité de la recherche.

Avec ces nouveautés, toutes les briques de la connaissance sont présentes, de la vulgarisation, TED, jusqu'à la recherche en passant par l'enseignement en ligne. Le site Open Culture répertorie tout ce matériel et bien d'autres sur son site en y ajoutant des libres et films librement accessibles.

21. dédiées ou pour lesquelles Internet est la cible principale
22. Technology, Entertainment and Design, http://www.ted.com/

4.3.3 L'encyclopédie : Wikipedia

On pourrait l'oublier tellement elle est entrée dans les meurs. Wikipedia est le second exemple réussi de création commune à très large échelle d'une œuvre intellectuelle, le premier étant les logiciels libres. Elle est devenu l'encyclopédie de référence à travers le monde, ayant dépassé les autres en nombre d'articles depuis des années. Elle a surtout permis à tous les publics d'accéder à des articles de qualité régulièrement mis à jour et enrichis.

La spécificité de la Wikipedia est qu'elle a été créée ex nihilo sur Internet par les internautes. Il ne s'agit pas comme pour la presse ou l'enseignement de l'adaptation de quelque chose qui existait dans le monde physique d'avant. Bien sûr les encyclopédies existaient, et là encore Internet les a obligées à évoluer et les fera peut-être disparaitre. Mais la Wikipedia n'est pas lié à ces anciennes encyclopédies, elle a redéfini le genre et propose la base de connaissance commune de l'humanité. Avec l'explosion de personnes instruites que va générer l'enseignement en ligne, il est probable que Wikipedia gagnera encore en qualité et en volume.

4.4 Les réseaux sociaux

Une vieille source d'information très appréciée est le bouche à oreille. Avec les réseaux sociaux on peut largement développer ce concept en touchant des millions de personnes tout en conservant le lien direct du bouche à oreille. Je te connais, tu me plais, je te fais confiance donc je te suis, je t'écoute, j'amplifie, le tout à une telle échelle que le monde entier est devenu un bistro.

Ce nouveau mode de communication est tellement répandu, plus de deux milliards d'utilisateurs de Facebook, qu'il exerce une influence sensible sur notre monde physique. Ainsi on a parlé parlé de la Révolution Facebook, de la Révolution 2.0, de la Révolution Twitter lors du printemps arabe afin de souligner l'importance de ces moyens de communication instantanés adaptés à l'action. Des études analysent l'impact des réseaux sociaux sur notre économie, lors du lancement d'un film, d'un jeu vidéo... Les politiciens et plus globalement les communiquants ont adopté ce nouveau canal. Facebook est devenu la source d'information principale des électeurs américains lors des présidentielles.

Si les réseaux sociaux sont largement utilisés, ils couvrent aussi un spectre large comme le montre la figure 4.14 [23]. Dans cette section, nous nous concentrons sur le cœur des réseaux sociaux à savoir Facebook et Twitter, mais on va aussi regarder YouTube dont l'influence sur notre vie est tout aussi importante. Ces exemples ne doivent pas faire oublier la diversité et

23. On peut discuter sur le fait que tout ces services soient réellement des réseaux sociaux

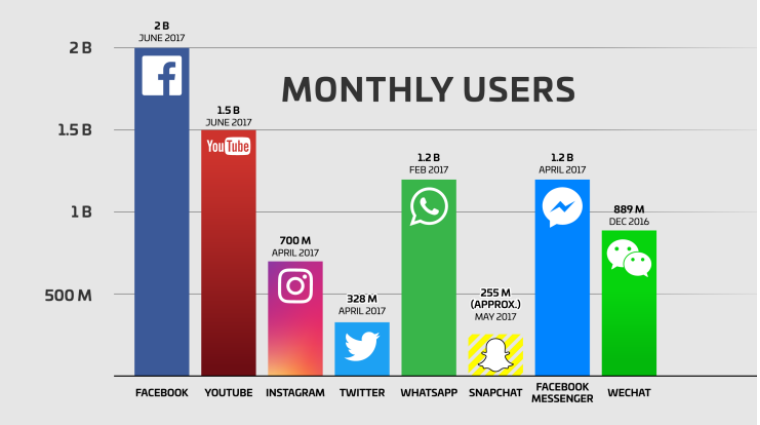


FIGURE 4.13 – Nombre d'utilisateur des principaux réseaux sociaux
source : Techcrunch 2017

.

les réseaux spécialisés comme Flickr pour les photos, LinkedIn pour les relations professionnelles, Foursquare pour la géolocalisation...

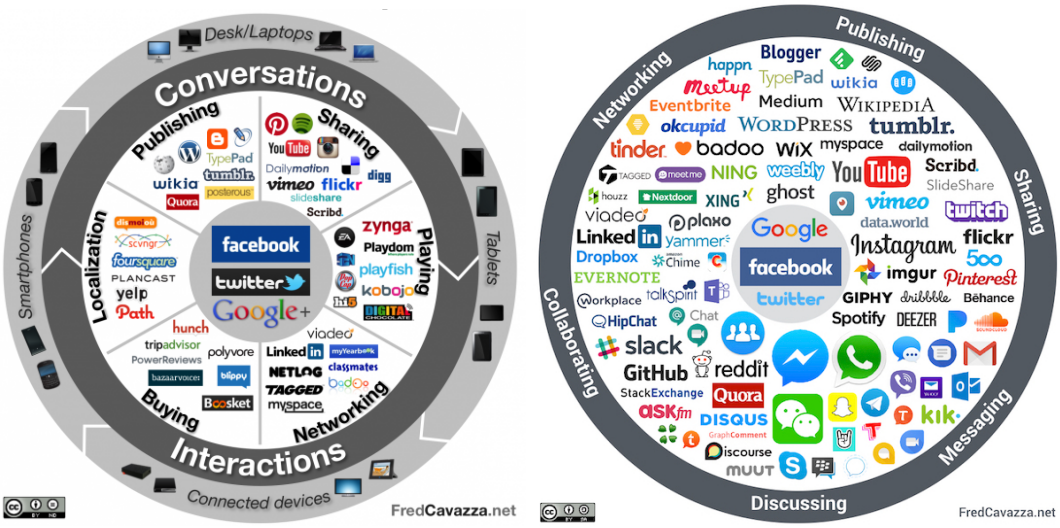


FIGURE 4.14 – Panorama 2012 et 2017 des réseaux sociaux *source : Fred Cavazza*

.

4.4.1 Twitter

Il n'était pas évident d'imaginer que la remise en marche du télégramme aurait un succès planétaire et pourrait générer des centaines de millions de dollars de revenus annuels. Dans une société abreuvée d'information où la phrase choc remplace l'analyse, Twitter est devenu le messie.

Un tweet est donc un message de 140, oups 280, caractères maximum qui sera diffusé immé-

diatement aux abonnés du flux ainsi qu'à ceux qui iront sur la page web de l'émetteur. Les lecteurs peuvent répondre et ainsi lancer une discussion. Il est également possible de faire suivre les messages d'autres sur son canal ce qui permet à l'information de littéralement exploser, en moyenne n'importe quel utilisateur Twitter est à 5 rebonds d'un autre [24]. Ainsi grace à Twitter tout utilisateur est très rapidement au courant des événements, parfois même d'un tremblement de terre avant que l'onde sismique arrive, voir la publicité de Twitter à ce sujet.

La force de Twitter est donc l'immédiateté du message concis. Comme son protocole a été porté sur de nombreuses plateformes, intégré dans des applications dédiées ou pas, agrégé dans des sites web... les tweets sont devenus accessibles partout. Une étude [25] faite en 2009 a calculé la répartition de 2000 tweets américains : 40,55% de blabla inintéressant, 37,55% de discussions, 8,70% de messages relayés, 5,85% d'autopromotion, 3,75% de spam, 3,60% d'information.

Pour les amateurs de chiffres, Twitter c'est [26] en 2016

— 330 millions d'utilisateurs actifs mensuel (dont 69 M aux USA)
— 110 millions d'utilisateurs actifs quotidien
— 500 millions de tweets envoyés chaque jour
— 300 milliards de tweets envoyés depuis le 21 mars 2006
— 170 minutes par utilisateur par mois
— 208 suiveurs en moyenne
— 20 millions de « faux comptes »
— 1 million de sites qui intègrent des tweets.

Malgré ces chiffres Twitter a du mal à dégager des bénéfices. Son influence et son poids restent limité et il n'est pas évident de savoir quel sera le modèle économique qui lui permettra de bien vivre. Inclure une publicité dans un tweet étant impossible et l'inclure dans un flux est délicat si on ne veut pas perdre ses abonnés.

24. voir analyse d'Alex Cheng d'avril 2010, http://www.sysomos.com/insidetwitter/sixdegrees/.
25. Twitter Study par Ryan Kelly chez Pear Analytics (12 août 2009)
26. d'après https://www.blogdumoderateur.com/chiffres-twitter/

4.4.2 Facebook

Dans le monde des réseaux sociaux, le poids lourd est Facebook. Avec le cap du milliard d'utilisateur [27] franchit fin 2012, il représente presque la moitié de l'Internet ou tout l'Internet de 2006. Il est le numéro 2 en terme de visiteurs pas si loin de Google. Année après année il écrase la concurrence et devient numéro un dans de plus en plus de pays.

Cette progression en fait l'étoile montante actuelle du web d'autant qu'il affiche clairement sa volonté de s'approprier les clients des concurrents, et les revenus publicitaires associés, avec comme première cible : Google.

Du point de vue fonctionnel, Facebook offre les fonctionnalités usuelles d'un réseau social ce qui implique beaucoup de choses et probablement encore plus dans le futur puisque le but est que l'utilisateur ait tout sur place pour communiquer avec ses amis ou relations, suivre leur activité, organiser sa vie et bien sûr faire dire ce qu'il fait, ce qu'il pense, ce qu'il aime... ce qu'il vit.

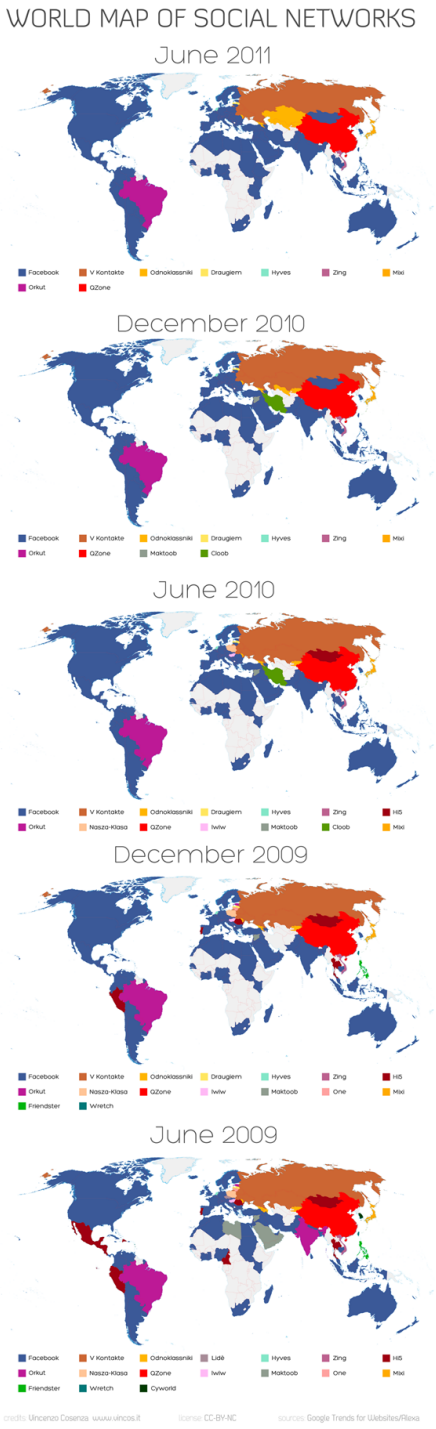


FIGURE 4.15 – Réseaux sociaux leaders par pays - *source : www.vincos.it*

Login Facebook

Facebook, ainsi que Twitter dans une moindre mesure, a réussi en devenant le plus gros hébergeur d'internautes identifiés à vendre sa capacité d'identification à tous les sites qui ont besoin de ce service, sachant que les internautes ont trop de comptes et désirent se simplifier la vie. Ainsi de très nombreux sites proposent de s'identifier avec son compte Facebook ce qui permet à ce dernier de suivre l'activité de ses membres en dehors de son site, information valorisable.

Jeux Facebook

Puisqu'on fait tout sur Facebook, il est normal qu'on y joue, en tout cas pour le joueur occasionnel, le véritable joueur ayant un PC taillé sur mesure pour cela et non un simple navigateur. Mais le

27. utilisateur = personne connectée durant le mois

joueur occasionnel est nettement plus nombreux que le passionné et cela se retrouve dans les chiffres impressionnants de la fréquentation des jeux sur Facebook :

03/12	Nom	Joueurs/jour	03/14	Nom	Joueurs/jour
1.	World With Friends	8 900 000	1.	Candy Crush Saga	57 036 000
2.	CityVille	8 700 000	2.	Farm Heroes Saga	16 755 000
3.	Hidden Chronicles	7 200 000	3.	Pet Rescue Saga	11 546 000
4.	CastleVille	7 000 000	4.	Hay Day	6 806 000
5.	Texas HoldEm Poker	6 800 000	5.	Criminal Case	4 924 000
6.	FarmVille	5 700 000	6.	Dragon City	4 828 000
7.	Bubble With Saga	5 300 000	7.	Top Eleven	4 689 000
8.	Diamond Dash	6 600 000	8.	Farm Ville 2	4 172 000
9.	The Sim Social	3 700 000	9.	Cash of Clans	4 104 000
10.	Tetris Battle	3 700 000	10.	Papa Pear Saga	3 475 000

TABLE 4.5 – Jeux les plus populaires sur Facebook en mars 2012 et 2014 - *source AppData*

Avec un tel nombre de joueurs, un tout petit bénéfice par joueur peut générer des revenus conséquents. Aussi le principe du *Free to play* est appliqué avec des jeux gratuits mais la possibilité d'acheter des objets virtuels pour améliorer l'expérience du jeu. Le miracle est que les joueurs achètent et même beaucoup. Ainsi les achats en se chiffre en milliards de dollars, 1,65 milliards seulement pour les États-Unis en 2012 [28].

4.4.3 YouTube

YouTube, Vimeo et d'autres équivalents, ont au moins 3 usages différents de la part de ceux qui ajoutent des vidéos :

1. témoigner,
2. promouvoir leurs œuvres ou leur produits commerciaux,
3. partager ce qu'ils aiment.

Le premier point, rendu possible grâce aux ordiphones et plus généralement grâce aux évolutions technologiques qui permettent d'acheter du matériel vidéo de qualité à des prix accessibles, nous transforment tous en reporter potentiel. Il est en effet devenu simple de créer des vidéos de qualité correcte qui vont du simple témoignage de la fête d'anniversaire du petit dernier à l'exclusivité présentée au journal télévisé d'un événement dont vous avez été le témoin. Cela permet aussi de faire apparaitre des événements dont les médias traditionnels ne parlent pas voire que les gouvernements, entreprises et autres organisations préfèreraient voir passer sous silence, cf http://fr.globalvoicesonline.org/category/type/video/ pour de tels exemples.

Le second point met Internet au service des créatifs. Sur YouTube cela va de la prestation filmée, un concert, une danse, un exploit, jusqu'à l'œuvre cinématographique comme le film

28. source : le rapport "Inside Virtual Goods" de Inside Network

Home de Yann Arthus-Bertrand. Ainsi tout artiste en herbe peut se promouvoir voire toucher directement son public sans intermédiaire.

Le gros succès de YouTube dans ce domaine est clairement musical. Des artistes inconnus y sont devenus des stars mondiales. La vidéo ”Gangnam Style” du musicien Psy a été vu plus d'un milliard de fois en 6 mois ce qui lui a apporté une notoriété mondiale. D'autres exemples impliquent des agents ou des groupes de musique qui découvrent des chanteurs sur YouTube et les mènes à la gloire (Justin Bieber, Soulja Boy, Tay Zonday, Arnel Pineda...). Pour bien mesurer le poids de ces vidéos, notons que Justin Bieber avait 31 millions de suiveurs sur Twitter fin 2012 et a été classé comme le 3e star la plus puissante du monde en 2011 et 2012 par le magasine Forbes [29].

Ces deux vidéos ont été le phénomène initial de l'explosion de vues sur YouTube. Jusqu'à juin 2015 Psy et Bieber étaient les seuls a avoir dépasser le milliards de vues. En 2018 le record est à 4,7 milliards de vue pour la vidéo musicale “Despacito”, les vidéos à plus d'un milliards de vue s'approchant de 100 avec seulement 5 vidéos qui ne sont pas des vidéos musicales.

FIGURE 4.16 – Psy et Bieber
source : http://mashable.com/2012/12/21/psy-gangnam-style-billion-vs-bieber/

Mais ce second point ne touche pas que les artistes, les entreprises, les politiciens, aussi utilisent YouTube pour s'offrir de la publicité à moindre coût, le coût étant de faire la vidéo qui plaira assez pour générer de l'audience voire le buzz [30].

Le troisième point est le plus sensible puisqu'il peut impliquer du matériel protégé par le droit d'auteur. A priori la situation est simple, il est illégal de déposer une vidéo protégée dont on n'a pas les droits. Le problème est alors de savoir si la vidéo est protégée et si elle l'est, ce qu'en pense l'ayant droit. Dans de nombreux cas, la vidéo est diffusée sans les droits mais avec la bénédiction des ayant-droits qui peuvent y trouver des avantages marketing, qui approuvent la diffusion massive de leurs œuvres ou qui considèrent que ces œuvres n'ont plus de valeur marchande. Ainsi YouTube propose de nombreux extraits d'émissions de télévision d'antan et il est peu probablement que cela soit sans l'accord implicite des chaînes de télévision. Dans ce cas YouTube sert de mémoire du monde.

Le problème est lorsque les ayant-droits ne sont pas d'accord. Notons que ce problème n'est pas toujours dans le sens qu'on imagine. Il arrive en effet que des personnes mettent leurs vidéos

29. https://en.wikipedia.org/wiki/Forbes_Celebrity_100
30. qui peut aussi être désastreux comme l'a vécu Cuisinella fin 2012 avec sa vidéo funeste.

sur YouTube dans un but de promotion et les retrouvent diffusées par une télévision sans en avoir été averties et bien sûr sans être rémunérées.

Sur YouTube les ayant-droits peuvent faire retirer les vidéos déposées contre leur volonté. Étant donné la quantité d'œuvres disponibles dont un grand nombre sont a priori protégées, il semble que l'état actuel arrange tout le monde.

4.4.4 L'impact des réseaux sociaux

Avec la communication directe de masse on change les règles du jeu.

En politique les candidats on compris l'importance de ces réseaux, bien sûr comme outil de travail pour avoir une communication directe avec leurs supporters, mais aussi pour favoriser la communication directe avec l'idée que la caisse de résonance de ces réseaux est devenue plus importante que les médias traditionnels, qui de toute façon reproduiront l'information. Depuis la première élection d'Obama il est devenu clair qu'une présidentielle américaine ne peut pas se faire sans les réseaux sociaux. Aussi il n'est pas surprenant que Barack Obama ait délaissé les médias traditionnels pour remercier directement ses électeurs sur Twitter, tweet relayé des centaines de milliers de fois, avec en prime une photo qui a fait le tour du monde, cf figure 4.17.

FIGURE 4.17 – Tweets d'Obama lors de sa réélection du 6/11/12

L'élection de Donald Trump a amplifiée le phénomène. Ce candidat anti-establishment a déclaré rapidement la guerre aux médias traditionnels et a privilégié une relation directe avec ses électeurs via un flux de tweets mémorable.

Globalement les leaders américains sont nettement plus présents sur les réseaux sociaux que les européens mais ils ne sont pas les seuls comme le montre le tableau 4.6.

Nom	Twitter	Facebook
Barrack Obama (EU)	99,3	53,4
Donald Trump (EU)	47,0	24,3
Narendra Modi (Inde)	39,6	42,7
Pape François (Vatican)	16,4	ε
Recep Tayyip Erdoğan (Turquie)	12,3	8,7
Rania Al Abdullah (Jordanie)	9,9	15,5
Joko Widodo (Indonésie)	9,5	8,1
HH Sheikh Mohammed (Dubaï)	8,7	3,7
Enrique Peña Nieto (Mexique)	7,0	5,4
Dimitry Medvedev (Russie)	5,6	1,4
Mauricio Macri (Argentine)	4,7	4,5
Emmanuel Macron (France)	2,7	2,2

TABLE 4.6 – Suivants des leaders sur les réseaux sociaux (en millions) – janv.18

Facebook et l'élection de Trump

Le problème principal des réseau sociaux est leur impact négatif sur la démocratie. Cela s'est révélé avec Facebook durant l'élection présidentielle américaine en 2016 [31].

En 2012 on a estimé que Facebook a motivé les jeunes à voter et les jeunes étant plutôt à gauche, les Démocrates ont gagné. Faire participer plus de citoyens à une élection c'est bien donc tout va bien. Mais rapidement des études ont montrées que pour un budget minime on peut cibler des publicités qui auront un impact sensible sur le choix d'électeurs. À tel point qu'en juin 2014 le chercheur en droit de Harvard Jonathan Zittrain a écrit «*Facebook Could Decide an Election Without Anyone Ever Finding Out*» [32]

Facebook a un aspect addictif développé par le bouton *J'aime* que l'on clique mais surtout que les autres cliquent pour vous féliciter. Outre cet aspect, ce bouton permet aussi à l'intelligence artificielle de Facebook de vous comprendre et de savoir ce que vous allez aimer et donc ce qui vous fait rester sur Facebook (50 minutes en moyenne par jour, plus que la lecture ou le sport et de loin). Ainsi Facebook peut cibler de façon très efficace sa publicité et les annonceurs peuvent faire autant de publicité qu'ils visent de type de personne. Dans une campagne électoral c'est redoutablement efficace, surtout que rien n'oblige à dire toujours la même chose puisque seul le groupe A recevra la publicité A et le groupe B la publicité B. On peut donc satisfaire tout le monde et cela d'autant plus facilement qu'on se rend compte que les groupes ne communiquent pas entre eux. Facebook facilite le replis sur soi en s'entourant de personnes qui pensent comme vous.

Ce qu'on a aussi découvert lors de la dernière élection est que non seulement des publicités et des fausses nouvelles diffusées par Facebook ont un véritable impact mais qu'un pays étranger,

31. Cette section est fortement inspirée de l'article très complet de The Atlantic : https://www.theatlantic.com/technology/archive/2017/10/what-facebook-did/542502/

32. Facebook peut choisir le résultat d'une élection sans que personne ne le sache jamais.

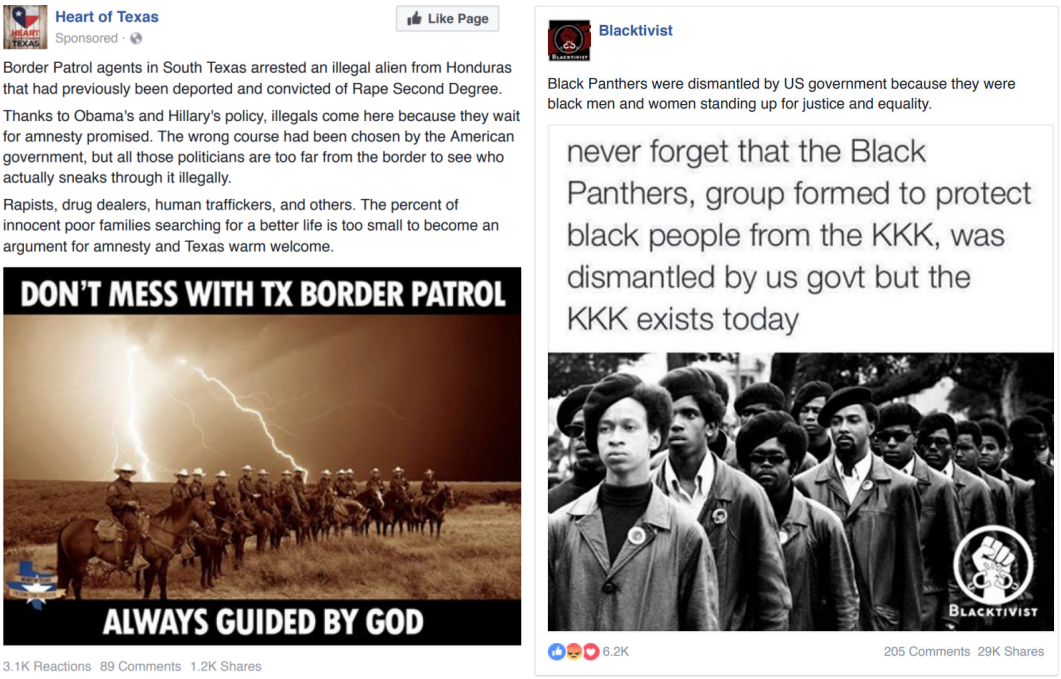


FIGURE 4.18 – Publicité et *troll* russes sur Facebook durant l'élection US 2016

la Russie en l'occurrence, peut acheter pour un prix dérisoire des publicitée ciblées qui vont lui permettre d'aider le candidat de son choix, Trump en l'occurrence, mais aussi de déstabiliser le pays en exacerbant les groupes les uns contre les autres, cf figure 7.7.

Enfin Facebook permet de se mobiliser en aimant et partageant des documents. On a ainsi vu à la fin de la campagne de l'élection de 2016 des petits groupes de la catégorie *troll* prendre de plus en plus d'importance avec des théories du complot, de fausses nouvelles au point d'être plus relayés que les articles des plus grands médias traditionnels.

Si ces différents points avaient été envisagés par les spécialistes des médias, leur combinaison et leur force a surpris tout le monde en 2106.

Suivi de politique – probablement plus dans l'e-democratie

Une étude de Twiplomacy [33] indique que les dirigeants de 125 pays étaient présents en 2012 sur Twitter. Barack Obama est le plus suivi avec 17 millions de suiveurs, Hugo Chavez arrivant second avec 3 millions de suiveurs. Si la majorité des dirigeants ont une équipe de communication pour écrire leur tweets, certains dirigeants, comme Paul Kagame du Rwanda et Amama Mbabazi de l'Ouganda, écrivent eux mêmes voire répondent. A l'inverse, certains dirigeants actifs lors de leur campagne disparaissent de l'horizon Twitter une fois élu, François Hollande et Dilma Rousseff du Brésil pour ne pas les citer.

Les campagnes électorales sont souvent un moment privilégié pour tweeter. Elles sont aussi le

33. cf. http://twiplomacy.com/twiplomacy-study-2012/

moment opportun pour interpeler les candidats. Ainsi le père de Sophia a poussé le candidat Obama à prendre position sur l'adoption par des parents homosexuels en postant sa lettre ouverte sur Facebook. Obama a répondu [34]. Plus généralement les réseaux sociaux peuvent forcer la presse et les candidats à aborder un sujet ou un point précis en générant un buzz tellement assourdissant qu'il devient impossible de l'ignorer.

L'effet collatéral de ce nouveau moyen de communication est la trace laissée. Ainsi il est possible de retrouver des anciens messages, de faire des statistiques, de les agréger comme le fait le site figure 4.19. Le politique perd immédiatement le contrôle de son message.

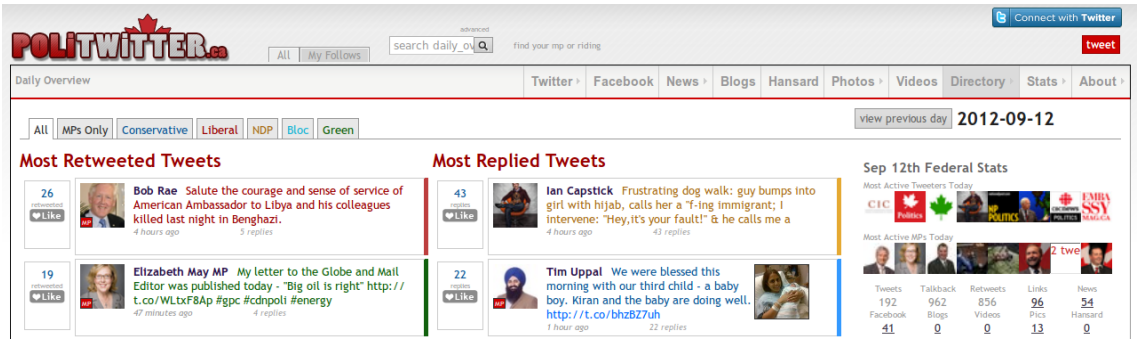


FIGURE 4.19 – PoliTwitter, un site canadien qui suit les dires de ses élus

Avec Internet, avec les blogs et encore plus avec les réseaux sociaux, l'information qui était restreinte à des cercles d'initiés se propage mondialement, rapidement et directement vers les personnes intéressées.

4.5 La désinformation

Si Internet est un merveilleux outil d'accès à la connaissance, il est aussi un outil de désinformation des plus puissants. Il permet avec peu de moyen de diffuser massivement de fausses informations. On a ainsi pu voir apparaitre des *fake-news* durant les campagnes de 2016 aux États-Unis et 2017 en Europe pour influencer les résultats. Certains y ont vu la main de Moscou, la Russie aidant les partis lui étant le plus favorable ou qui affaibliront le plus le pays visé. Mais la désinformation se fait aussi au niveau des entreprises à travers les faux avis sur les produits commerciaux, que ce soit pour encenser ses propres produits ou pour frapper la concurrence. Enfin elle se fait au niveau des individus, qu'ils soient convaincus d'avoir la véritable information ou qu'ils soient simplement cupides, la désinformations pouvant aussi rapporter.

Cet aspect sombre de l'Internet n'est pas nouveau mais je dois avouer l'avoir sous-estimé et il est probable que nombre de mes lecteurs en ait fait de même. Il est difficile d'imaginer que 9% des français pensent que la terre est plate lorsqu'on a fait des études supérieures ou simplement voyagé assez loin. On se dit qu'il est tellement simple de croiser les informations que la désinformation ne peut pas survivre. Mais on découvre que si Internet permet un accès quasi

34. cf l'article du Nouvel Observateur : Quand une fillette de 10 ans écrit à Obama sur ses parents gays

universel à la connaissance, chacun de nous se limite à sa zone de confort et ne va pas voir l'information qui le dérange [35].

4.5.1 La propagande

Les états

La limite entre communication et propagande est subtile et n'est pas notre sujet aussi regardons plus largement comment Internet est utilisé pour pousser ses idées en particulier au niveau des états.

Comme indiqué en introduction la Russie a été sous le feu des projecteurs occidentaux pour son œuvre de propagande avec des soupçons d'avoir permis à Trump de gagner l'élection présidentielle américaine grâce à des *fake-news* diffusé sur Facebook. En France Emmanuel Macron souligné, lors d'une conférence de presse avec Poutine en 2017, le poids de média russes durant la campagne présidentielle :

> *Quand des organes de presse répandent des contrevérités infamantes, ce ne sont plus des journalistes, ce sont des organes d'influence. Russia Today et Sputnik ont été des organes d' influence durant cette campagne qui, à plusieurs reprises, ont produit des contre-vérités sur ma personne et ma campagne ...*
> *ils se sont comportés comme des organes d'influence, de propagande et de propagande mensongère.*

On retrouve ces craintes d'influence russe dans un grand nombre d'élections. Il semble en effet que la Russie ait décidé d'utiliser ses organes de presse pour pousser ses idées et défendre ses intérêts de façon relativement agressive. Cette politique fait parti du *soft power*, connu pour le pouvoir qu'il confère aux des États-Unis à travers le monde tant via Hollywood que par ses médias et aujourd'hui par le poids des GAFA et autre entreprises majeures américaines sur Internet. Mais cela ne limite pas les États-Unis qui ont aussi leur canal de propagande, Voice of America, dont la radio arrosait les pays soviétiques durant la guerre froide et qui aujourd'hui vise un grand nombre de pays à travers des informations locales dans leur langue, cf https://www.voanews.com/navigation/allsites.

Mais vouloir diffuser sa vision du monde n'est pas réservé aux deux anciennes super-puissances. La chaîne Aljazeera est aussi perçu comme un outil au service d'un pays, le Qatar, pour contrer la puissance médiatique des saoudiens sur le monde arabe et plus généralement servir les intérêts de son pays. Moins connu, Xinhua, l'agence officielle de la Chine, existe en anglais, français, arabe, russe, espagnol, allemand. La France dispose de France 24, diffusé est français, anglais, arabe et espagnol, pour porter sa voix à travers le monde. Enfin la voix de Londres, la BBC, est connue à travers le monde et applique la même stratégie locale que la Voix de l'Amérique.

Tout ces canaux d'information sont disponibles sur Internet en différentes versions, écrite,

35. Je vous invite à regarde le site russe en français RT, c'est toujours un exercice intellectuel intéressant tant pour remettre en question des idées reçues que pour chercher les buts de la Russie.

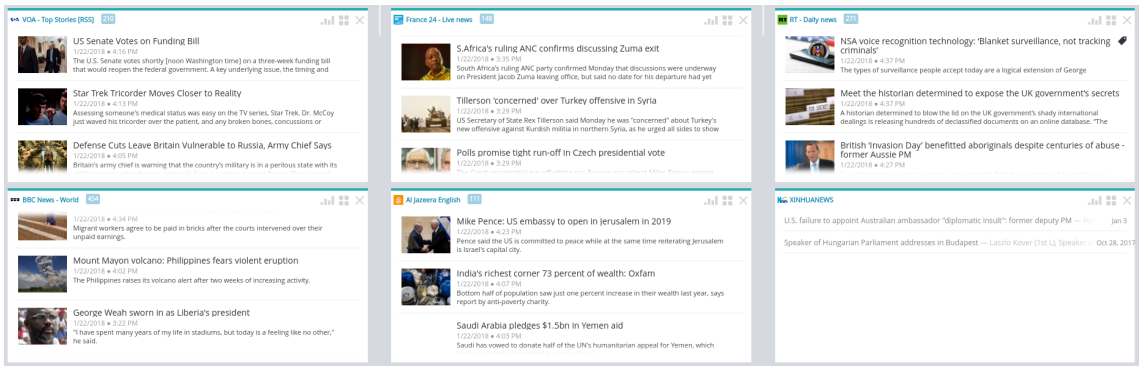


FIGURE 4.20 – Flux RSS d'agences d'information d'États

vidéo et direct télévisé et sur différents supports, site web, twitter, facebook voire plus. Certains ne sont disponible en France que par Internet, l'outil de diffusion de masse le moins cher de très loin.

On voit donc que toutes les puissances utilisent l'information [36] et Internet pour la diffuser. Bien sûr on ne veut pas que d'autre pays influencent nos concitoyens pour définir notre avenir. En même temps la mondialisation est justement la construction d'une pensée mondiale qui est très largement occidentale et due en bonne partie à la France des lumières. Les états occidentaux influencent notablement depuis des siècles le reste du monde et cette influence est encore augmentée avec Internet.

La limite acceptable de l'influence est donc dans la façon de faire. Promouvoir l'art de vivre à la russe est acceptable, souligner l'avantage à avoir de bonne relations avec la Russie est plus discutable surtout si cela implique de voter pour X, utiliser le mensonge pour défendre son candidat dans l'élection d'un pays tierce n'est pas bien (surtout si on se fait attraper ou que son candidat ne gagne pas). Quand à pirater les boites mails des candidats Emmanuel Macron et Hillary Clinton pour publier leurs mails, voire en ajouter des faux, avec une volonté évidente de vouloir influencer l'élection [37]...

Enfin soulignons que la France a des règles électorales qui encadrent strictement la communication des candidats et des médias afin de garantir une élection juste. Ces règles s'imposent à la presse écrite, radio et télévision mais plus difficilement aux plateformes ou médias étrangers sur Internet [38]. Ainsi les comptes Twitter et Facebook des candidats, de leur parti et proches associés doivent respecter les mêmes règles mais comment empêcher des supporters de communiquer, surtout s'ils sont à l'étranger? Comment bloquer les publicités ou *fake-news* qui peuvent avoir un impact fort sur une élection?

En janvier 2018 le président Macron a annoncé que l'état allait lutter contre les fausses nouvelles en période électorale.

36. plus d'excuse pour ne pas lire le point de vue de l'autre!
37. cf http://www.slate.fr/story/145221/le-macronleaks-est-une-fakenews et l'article de RT sur le sujet https://francais.rt.com/france/37940-macronleaks-equipe-den-marche-denonce-piratage-massif-ses-donnees
38. http://www.vie-publique.fr/actualite/dossier/presidentielle-2017/regles-campagne-electorale-audiovisuelle-internet.html

Le terrorisme

S'il est des groupes qui ont su profiter de l'Internet et des ses outils de communication, ce sont bien les groupes terroristes. Twitter, Facebook ou YouTube sont du pain béni pour des combattants de l'ombre qui ne peuvent pas utiliser les réseaux hertzien ou les satellites. Ainsi Deash a pu diffuser librement ses messages en mettant dans l'embarra tant les entreprises de l'Internet concernées que les pays visés. Les réponses mises en place par les états ont malheureusement abimées nos démocraties en développant une surveillance policière accrues. Quand aux réponses des plateformes qui diffusent les messages, elles sont difficiles à mettre en œuvre étant donné la quantité de données en jeu. Si la censure en directe n'est pas possible, les comptes diffusant des vidéos terroristes sont clos dès qu'ils sont repérés par les plateformes mais il est toujours possible d'en ouvrir d'autres. L'institut Brooking a ainsi estimé que les supporters d'ISIS ont utilisé 46 000 comptes twitter entre septembre et décembre 2014 (à une époque où Twitter, défenseur de la liberté d'expression, n'était pas encore trop agressif dans la fermeture de tels comptes). Un compte Twitter spécialisé dans la dénonciation de compte d'ISIS déclare en avoir fait fermer 200 000 entre 2015 et 2017.

Le problème de fond lorsqu'on affronte des groupes terroriste sur le terrain de la communication est le choix à faire entre une censure assez large pour filtrer efficacement et laisser des terroristes utiliser Internet pour promouvoir leur cause et recruter, les deux solutions étant mauvaises pour la démocratie.

Aussi la loi essaie de définir les limites. Par exemple Marine Le Pen en tweetant des images d'exécutions de Deash (pour montrer la différence entre son parti et ce groupe terroriste à un journaliste qui les assimilait) s'est vu mise en examen sous l'article de loi 227-24 du Code pénal.

> *Art. 227-24 : Le fait de diffuser (...) un message à caractère violent (...) de nature à porter gravement atteinte à la dignité humaine (...) est puni de trois ans d'emprisonnement et de 75.000 euros d'amende lorsque ce message est susceptible d'être vu ou perçu par un mineur.*

Cet article de loi ne s'applique pas aux journalistes afin que l'on soit informé.

4.5.2 Les complotistes

Internet permet aussi aux complotistes de développer leur arguments et comme personne ne peut contredire un site web sur le même site web, on peut ainsi avoir des sources d'informations farfelues présentées comme d'autres sources très sérieuses. Par exemple il existe la société savante de la terre plate qui précise bien dans sa FAQ qu'elle n'est pas une blague et pourquoi ce sont ceux de la terre sphérique qui sont dans le tort (cf figure 4.21 pour voir le pourcentage de français d'accord avec cette théorie).

Le problème est que beaucoup de personnes font plus confiance en leur intuition qu'en leur raison [39]. Une enquête de l'IFOP montre qu'en 2017 seul 1 français sur 5 ne croit pas en une

39. ou ne prenne pas la peine de faire fonctionner leur raison.

des onze théories du complot qu'il lui était présentées quand 1 sur 4 croit en 5 ou plus des ces théories, cf figures 4.21 et 4.22. On notera que deux théories arrivent à convaincre la majorité des personnes interrogées. Il faut néanmoins noter que les réponses proposées ne permettaient pas d'indiquer qu'on ne sait pas. Ainsi vous deviez savoir si la CIA est impliquée ou pas dans la mort de Kennedy. On peut penser que le nombre de complotistes aurait baissé si le doute était permis [40].

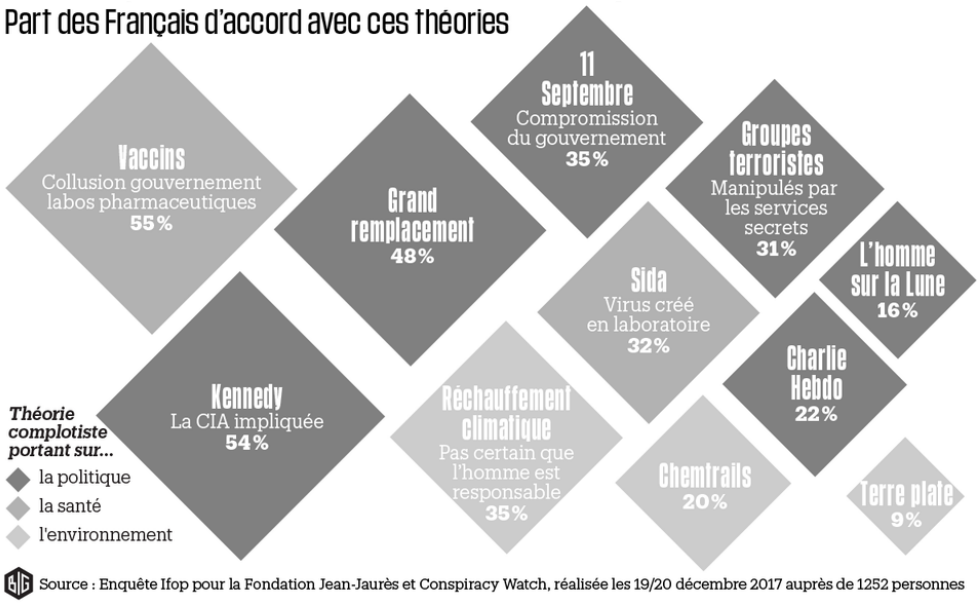


FIGURE 4.21 – Croyances des français dans les théories complotistes

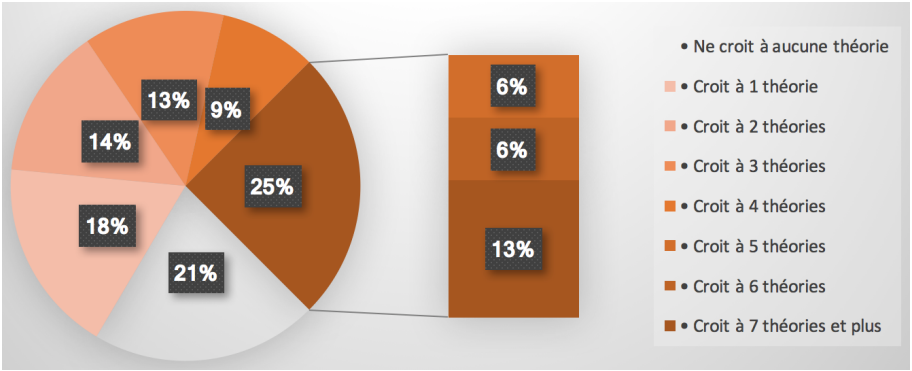


FIGURE 4.22 – Nombre de théories complotistes approuvées

Il existe des raisons pour suivre les théories du complot, une évidente est le désir de transgression et de révolte. On notera que les jeunes sont plus sujet à croire au complot que leurs ainés. L'époque, Internet et l'éducation peuvent aussi entrer en jeu. Enfin les états et les entreprises font assez de choses peu avouables en secret pour qu'on puisse porter crédit à de nombreuses rumeurs.

40. Il est intéressant de noter que seul un quart des sondés de la même enquête pensent que les journalistes font bien leur travail.

Le bon coté des théories du complot est de pousser l'autre camps a affuter ses arguments. Ainsi la page de Wikipedia «on n'a pas été sur la lune» déconstruit chacun des arguments usuels des complotistes. Malheureusement la logique ne suffit pas à contrer les théories du complot car admettre qu'on s'est trompé est toujours un exercice difficile qui peut remettre en cause son monde mental. Aussi il souvent est plus simple de trouver une autre raison qui vous conforte dans le complot lorsqu'un argumentaire peut vous faire douter.

Il sera intéressant de voir comme l'accès à toutes les connaissances, vraies et fausses, qu'offre Internet fera évoluer ou pas la croyance dans les complots.

4.5.3 Les faux avis de consommateurs

A un niveau plus mercantile, la désinformation est utilisée pour dire du bien de ses produits et critiquer ceux de la concurrence. Dire du bien de ses produits est la publicité sauf lorsqu'on ne sait pas qu'il s'agit de publicité. Ainsi écrire un avis sur Amazon d'un produit que l'on vend en se faisant passer pour un acheteur est malhonnête.

En 2016 une étude sur 40 000 avis d'hôtels de Hong-Kong sur Trip Advisor a montré que 20 % des avis étaient truqués. En 2017, la direction de la concurrence et des fraudes indiquait que 35% des avis clients en ligne ne sont pas authentiques.

Ces avis sont le plus souvent écrits par des intermédiaires. En prenant en compte la différence de niveau de vie à travers la planète, un faux avis écrit par un spécialiste peut coûter très peu cher. Certains sites, comme Fiverr, servent d'intermédiaires pour de tels services ou pour diffuser sur leurs pages des recommandations, cf propositions figure 4.23.

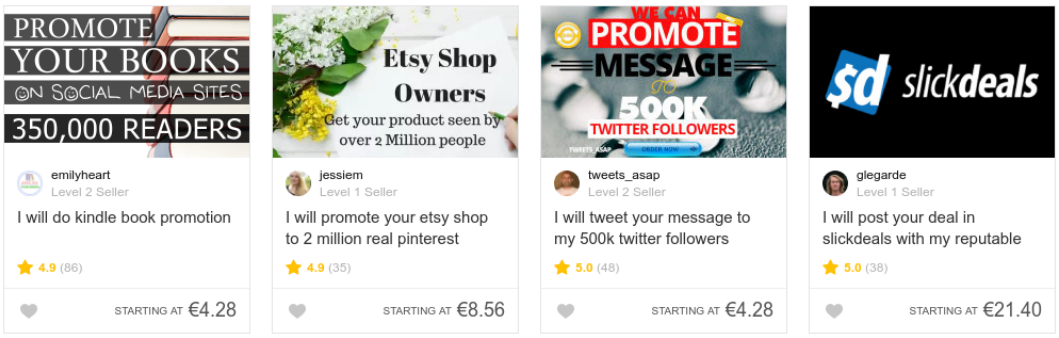


FIGURE 4.23 – Propositions faites par des membres de Fiverr – janv. 2018

On retrouve la même chose à un niveau professionnel avec des sites spécialisés dans la notations des autres entreprises. Une entreprise comme Trustpilot est régulièrement dénoncée [41] pour retirer les bons ou mauvais avis de façon suspecte, a priori en fonction de ce que paie l'entreprise visée.

Le problème est que ces faux avis, positifs ou négatifs ont un impact réel sur les consommateurs. D'après le baromètre 2014 du C to C PriceMinister-Rakuten & La Poste, 74 % des internautes ont déjà renoncé à acheter un produit à cause de commentaires ou d' avis négatifs et

41. Voir les discussion sur 60 millions de consommateurs, Reddit...

41 % ont déjà réalisé un achat spontané à la suite d' un avis positif. Une étude de Nielsen de 2017 indique que 80 % des consommateurs tiennent compte des avis pour faire leur achat.

On est donc dans un véritable système de fraude qui a un impact réel sur les achats des consommateurs. Aussi la loi pour une République numérique demande à partir du 1er janvier 2018 aux plateformes d'avis d'indiquer les procédures de contrôle qui ont été mises en place pour s'assurer que les avis postés sur leur site sont fiables. Elles devront aussi expliquer comment sont choisis les avis mis en avant et s'il y a une rémunération de la part des vendeurs pour pousser tel ou tel avis.

Chapitre 5

Le commerce électronique

A priori le commerce électronique n'a rien de vraiment révolutionnaire. Finalement il ne s'agit que de vente à distance comme le fait la Redoute depuis 1837 ou comme l'a fait le Minitel dans les années 80. La principale différence est la taille du marché qui est devenu mondial, ce qui génère des problèmes de livraison et de paiement mais procure de réels avantages économiques.

Tous les modes de commerce semblent exister aujourd'hui sur Internet. Le commerce des entreprises à destination des particuliers (B2C pour *Business to Consumers*) est le plus visible, mais le commerce inter entreprise (B2B) est nettement plus important en chiffre d'affaire et la vente entre particuliers profite aussi largement d'Internet via des sites comme eBay ou Le bon coin.

Surtout Internet est le lieu idéal pour le commerce des biens immatériels. La musique, le cinéma, les jeux vidéo, la presse, les logiciels, les services peuvent se développer sans limites avec cet outil. C'est là qu'Internet a fondamentalement changé les choses. Bien sûr le risque de piratage existe mais il a surtout touché les modèles qui n'ont pas su s'adapter ou qu'Internet a rendu désuets. L'arrivée des imprimantes 3D et des plans des objets disponibles sur le réseau va amplifier ce changement de paradigme économique.

Enfin pas de commerce sans argent, ou plus précisément sans outil de paiement. Là aussi une innovation bouleverse le paysage : le bitcoin. Cette monnaie alternative sans contrôle étatique connait un succès grandissant ce qui n'est pas sans poser problème aux États.

5.1 La vente en ligne – B2C

La vente en ligne à destination du grand public devrait dépasser les 6 billions [1] de dollars en 2023, cf figure 5.1. À titre de comparaison les exportations de marchandises des membres de l'OMC (quasiment le monde entier) représentent 19 T$ en

1. Attention, un billion est 10^{12} en français alors qu'il vaut 10^{9} en anglais, soit notre milliard. En anglais 10^{12} se dit trillion (mais attention trillion est 10^{18} en français...). Il est parfois plus simple de parler en mega, giga, tera, peta... ce qui donne des M$, G$, T$ et P$. Ainsi le B2C en ligne pèse 6 T$ en 2023.

2020 [2] (les exportations des produits agricole sont à 1,8 et le pétrole et produits miniers à 3 T$).

La répartition de ce commerce en ligne est grossièrement 20% en Europe, 30% aux États-Unis, 45% en Asie, le reste du monde prenant le reste. Ces chiffres reflètent le pouvoir d'achat des différentes zones, leur taux de pénétration d'Internet et les habitudes (la figure 5.3 montre qu'aux États-Unis la vente en ligne progresse alors que le pouvoir d'achat et le taux de pénétration d'Internet sont globalement stables).

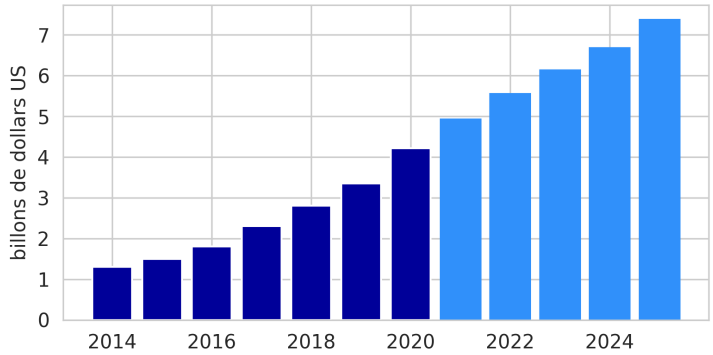


FIGURE 5.1 – Chiffres mondiaux du e-commerce (B2C)
source : eMarketer – Prévision pour 2021 et après.

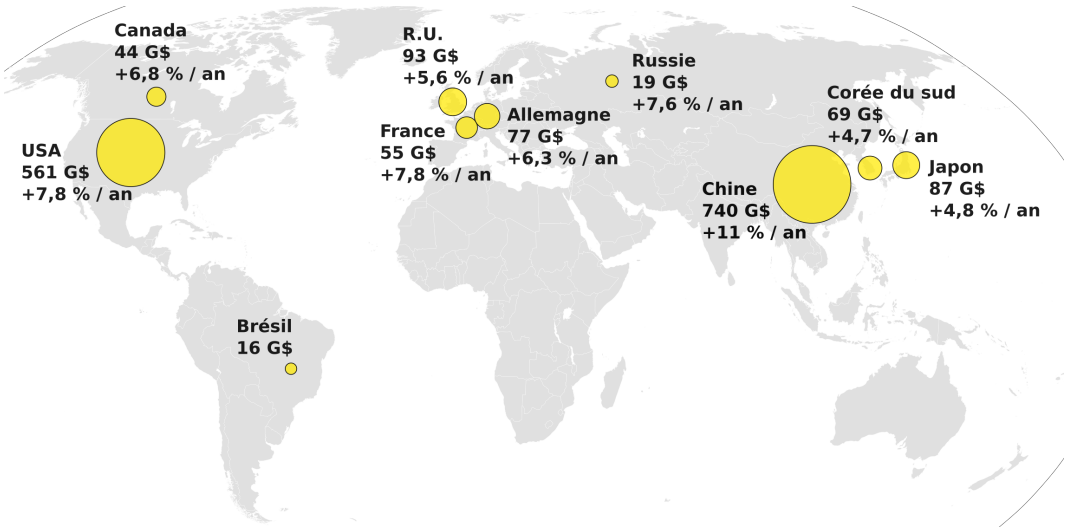


FIGURE 5.2 – B2C en ligne de pays les plus consommateurs en 2019
Vente de produits mais ne prend pas en compte les services.
Le pourcentage indique la croissance prévue entre 2018 et 2023.
source : Statista

Suivant les pays, le commerce en ligne est plus ou moins présent. En Europe, les chiffres de

2. cf https://www.wto.org/french/res_f/statis_f/wts2020_f/wts2029_f.pdf

2017 indiquent que le commerce en ligne représente pour le Royaume-Uni 18 % du commerce au détail. L'Allemagne suit avec 15 %, la France, la Suède et les Pays-Bas sont à 10 %. À l'autre bout, le commerce en ligne en Italie ne représente que 3,4 % de la vente au détail [3]. À la même date, le B2C en ligne aux États-Unis s'approchaient des 10 % du commerce de détail suivant une progression très régulière. Avec la Covid en 2020 et les confinements, les achats en ligne ont fait un bon, puis les choses se sont stabilisées, comme si on attendait de retrouver l'ancienne croissance régulière, cf figure 5.3.

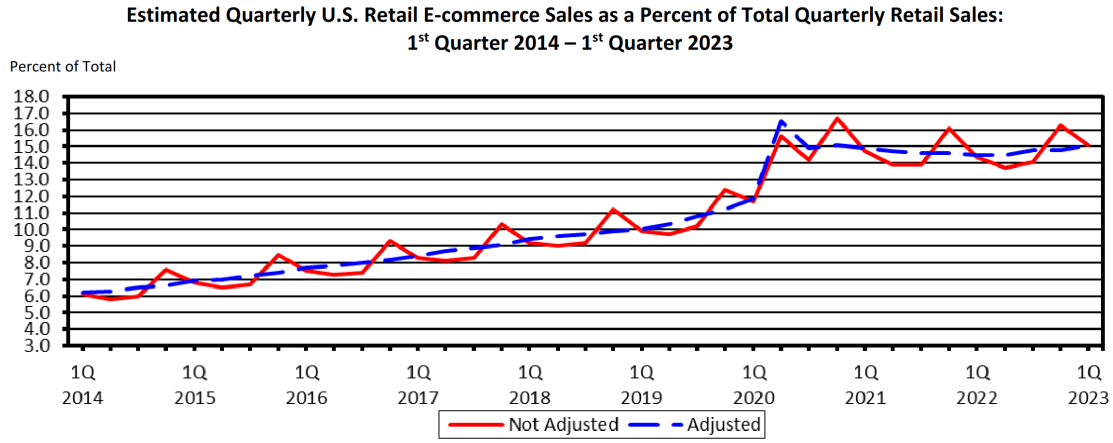


FIGURE 5.3 – part du commerce en ligne dans la vente au détail aux États-Unis
source : U.S. census bureau

Le commerce en ligne reste donc encore faible comparé au commerce physique. Certains domaines comme l'alimentaire et les carburants, qui représentent des parts importantes dans le budget des ménages, résistent. Mais la croissance du commerce en ligne et son importance lors de la crise de la Covid en font déjà un acteur majeur du commerce.

D'autre part, il faut noter qu'une présence sur Internet ne sert pas qu'à y faire des ventes. Être sur Internet permet aussi de se présenter et de promouvoir ses produits. C'est d'autant plus important que les consommateurs s'informent sur Internet que le produit soit acheté en ligne ou dans un magasin.

Enfin notons que parmi les sites marchands français, mais c'est probablement la même chose dans les autres pays, quelques sites marchands mangent le gros du gâteau. En 2019 en France, moins d'un pour cent des sites récupèrent près de 70 % des revenus du commerce en ligne. À l'opposé plus des 3/4 des sites se partagent 2,2 % des revenus, cf figure 5.4. Le principal vendeur est toujours Amazon, suivi de la Fnac et de CDiscount et Veepee, anciennement Vente-privée.

3. Données de Statista, https://fr.statista.com/statistiques/689343/e-commerce-part-vente-de-detail-pays-europe/

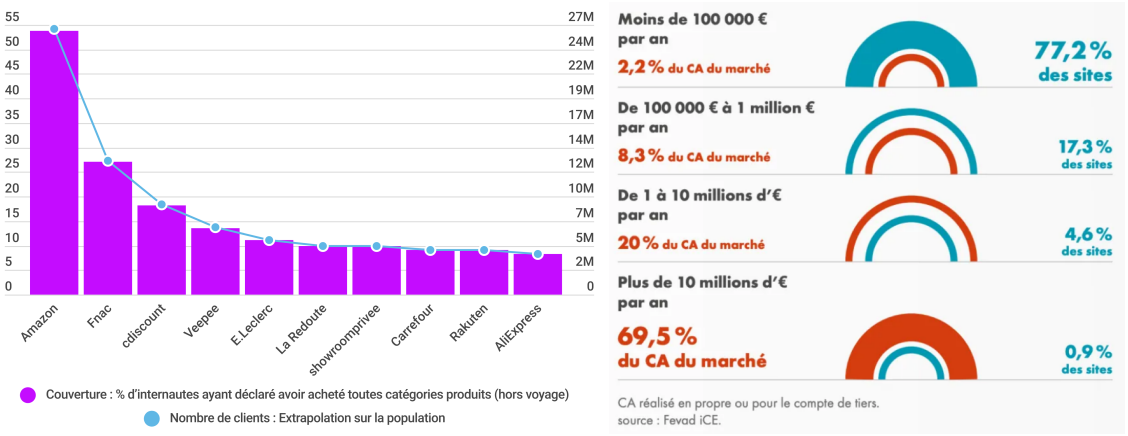


FIGURE 5.4 – Sites marchands. Top 10 2020 et répartition en fonction du CA 2019 en France
source : Fevad iCE

Attention aux chiffres

Le British Retail Consortium annonce sur son site web que le commerce de détail UK a vendu pour 373 milliards d'euros en 2012 dont 35 milliards en ligne alors que l'étude de la Fevad [a] indiquait une vente en ligne de 96 milliards d'euros pour ce même pays la même année ce qui fait presque un facteur 3 !

En France l'INSEE indique dans son rapport sur *La situation du commerce en 2015* que les ventes hors magasin (donc en ligne mais aussi par correspondance) représentent 5,3 % des ventes au détail alors que la Fevad annonce dans son rapport 2016 que les ventes en ligne pèsent 7 % soit un tiers de plus.

Au niveau mondial, en regardant les rapports successifs du site Ecommerce Europe [b], on découvre que le B2C en Amérique latine passe de 50 G$ en 2013 à 37 G$ en 2014 et 33 G$ en 2015 alors que chaque rapport indique une progression de plus de 15 % par an.

a. Fédération du e-commerce et de la vente à distance, Chiffres clefs 2013, site web : www.fedav.com
b. La fondation Ecommerce est leur structure de recherche, c'est elle maintenant qui publie les rapports sur son propre site

5.1.1 Les types de produits

Le commerce en ligne est le mieux adapté pour les produits immatériels comme les billets pour voyager ou pour aller voir un spectacle, les réservations d'hôtel ou d'autres choses, les produits culturels (musique, film, livre électronique) et les jeux. Si la vente de ces produits restent majoritaire sur Internet en chiffre d'affaire, la vente d'objets physique explose aussi. Pour s'en convaincre on peut regarder l'augmentation des livraisons à travers les chiffres d'affaires des entreprises concernées (UPS, Fedex, La Poste en France) ou en regardant les coûts de livraison pour Amazon, figure 5.5 [4]. Bien sûr la crise de la Covid-19 a amplifie le phénomène.

4. Attention, la part de marché d'Amazon dans la vente en ligne augmente aussi, mais nettement moins vite. Aux É.U. elle est passée de 34 % en 2016 à 50 % en 2021.

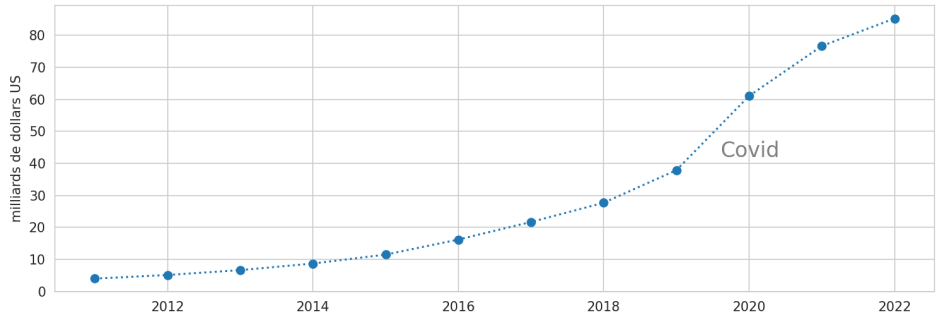


FIGURE 5.5 – Coûts de livraison d'Amazon

Au niveau européen, le commerce en ligne devrait représenter 717 milliards d'euros en 2020 [5] (110 milliards d'euros en 2012). Si on regarde les chiffres d'affaire en France on constate que le tourisme représente preque la moitié à lui seul. Si on ajoute la vente des produits culturels et d'autres services immatériels, on dépasse largement les 50 %, cf figure 5.6.

À l'opposé l'alimentation et les produits de grande consommation restent encore essentiellement des achats physiques puisque leur vente en ligne ne représente que 8% de part de marché en France en 2019.

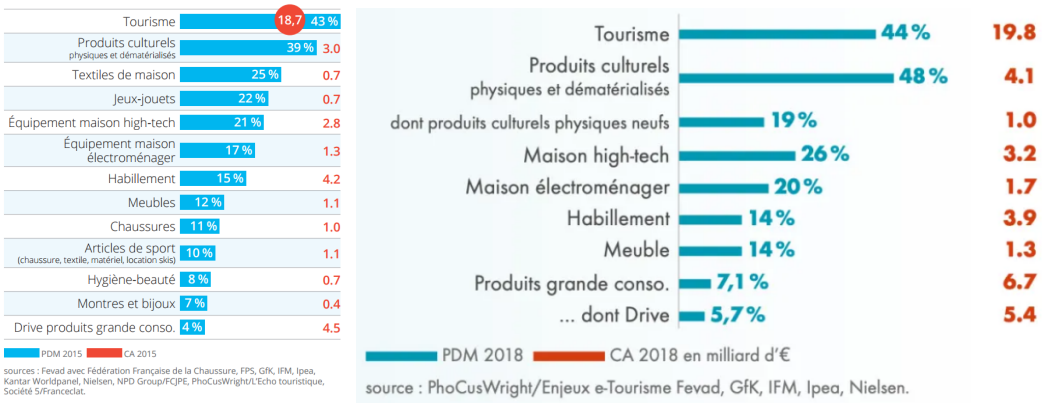


FIGURE 5.6 – Parts sectorielles du commerce en ligne en France en 2015 et 2018

Regardons la vente en ligne des produits immatériels en ligne, celle pour laquelle Internet offre une véritable valeur ajoutée.

5. estimation de Ecommerce News

5.1.2 La vente des produits immatériels

Voyages

À tout seigneur tout honneur, commençons par le monde du voyage. Avant la crise de la Covid-19, Allied Market Research avait estimé que la vente en ligne des voyages (billet de train, avion + hotel) devrait dépasser les 1 billion de dollars en 2022 (½ T$ en 2015). Ce poids s'explique par le coût des voyages, la forte concurrence du marché, la jungle des prix dans le domaine, une infrastructure de comparaison et d'achat mûre et bien sûr, le fait qu'un billet soit un produit immatériel. Notons que la vente en agence résiste car si 60 % des français on réservé au moins un voyage en ligne en 2019, la moitié du chiffre d'affaire reste aux mains des agences physiques. Il n'est pas certain que l'on retrouve cette répartition après la crise de la Covid qui favorise tout ce qui est en ligne.

Au niveau des entreprises, deux marquent les esprits : Booking qui est devenu la référence des réservations d'hôtel en ligne et AirBnB qui est la référence des réservations de logements privés. Ces deux entreprises ont profondément bouleversé le monde du tourisme, pas pour le mieux pour de nombreuses personnes. La progression du chiffre d'affaire de ces deux entreprises montre leur importance. En 2019 Booking était la plus grosse agence de voyage en ligne, juste devant Expedia.

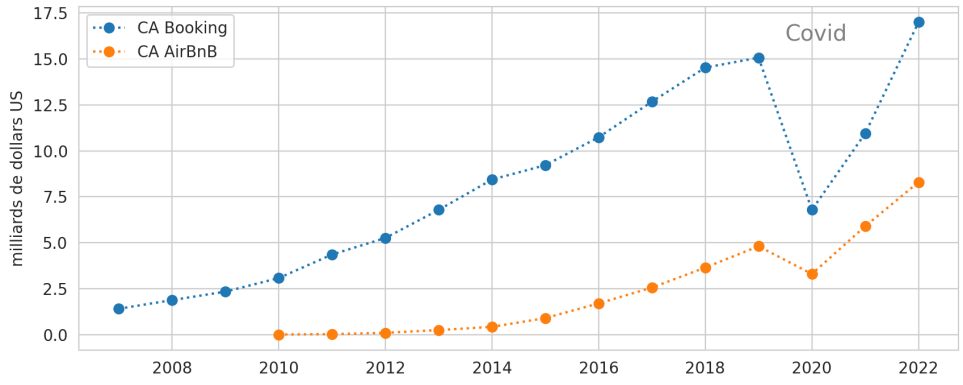


FIGURE 5.7 – Chiffre d'affaire de Booking et d'AirBnB

L'intérêt pour les consommateurs des offres de tourisme en ligne est de pouvoir facilement les comparer. Cela étant les sites marchants ont des outils pour retourner la situation à leur avantage. Le premier est le *yield management* qui fait varier le prix des places afin d'optimiser le remplissage. L'idée principale transmise aux clients est que plus on achète tôt son billet, et moins c'est cher mais c'est nettement plus compliqué [6]. À l'arrivé chacun ou presque paie un prix différent pour un même trajet ou un même hôtel dans des conditions équivalentes. Le second outil consiste à augmenter les prix au fur et à mesure de la recherche d'une personne avec l'idée que plus elle cherche, plus elle est déterminée à acheter un billet et donc plus on

6. une personne qui achète au dernier moment, peut très bien payer très cher (pas le choix) ou vraiment pas cher (promotion).

peut la faire payer. Cela est rendu possible car il est relativement simple de reconnaitre une machine sur Internet. Bref, tout votre travail de recherche du prix le plus faible est contré par le marketing qui désire justement l'inverse [7]. Cette guéguerre est à l'origine du site web, Flystein, qui propose pour une petite somme, de chercher à votre place le prix le moins cher avec des personnes qui savent contrer les pièges des compagnies.

Le poids des influenceurs

Les influenceurs sont devenus des acteurs majeurs de la publicité, pardon, du marketing d'influence sur Internet. On les retrouve dans la mode, les voyages, la santé, la cuisine, les affaires, etc. Les marques ont compris l'avantage qu'offre une recommandation par une personne suivie sur Internet. Aussi le métier d'influenceur explose, ils ont des agences, des plateformes dédiées et des tarifs directement liés au nombre de suiveurs et au réseaux social :

	NANO (0-10K)	MICRO (10-100K)	MACRO (+ de 100K)	TOP (+ de 100K)	Au-delà de 3 MILLIONS d'abonnés
Instagram					
Post	0 - 165 €	155 - 1,900 €	1,900 - 5,000 €	5,000- 25,000 €	25,000 € à plusieurs centaines de millers d'€
Live	0 - 400 €	400 - 2,500 €	2,500 - 8,000 €	8,000 - 40,000 €	40,000 € à plusieurs centaines de millers d'€
Reels	0 - 300 €	300 - 2,500 €	2,500 - 6,500 €	6,500 - 35,000 €	35,000 € à plusieurs centaines de millers d'€
Stories	0 - 90 €	90 - 1,400 €	1,400 - 5,200 €	5,200 - 24,000 €	24,000 € à plusieurs centaines de millers d'€
Twitter					
Post	0 - 40 €	40 - 400 €	400 - 800 €	800 -6,400 €	6,400 € à plusieurs centaines de millers d'€
Facebook					
Publication	0 - 80 €	80 - 800 €	800 - 2,400 €	2,400 - 12,000 €	12,000 € à plusieurs centaines de millers d'€
Snapchat					
Snap	0 - 100 €	100 - 800 €	800 - 2,000 €	2,000 - 10,000 €	10,000 € à plusieurs centaines de millers d'€
Youtube – Attention dépend surtout du nb de vues					
Video	0 - 2,500 €	2,500 - 10,000 €	10,000 - 18,000 €	18,000 - 50,000 €	50,000 € à plusieurs centaines de millers d'€
Tiktok					
Post	0 - 130 €	130 - 500 €	500 - 4,800 €	4,800 - 12,000 €	12,000 € à plusieurs centaines de millers d'€
Twitch – Attention dépend surtout du nb de vues					
Live	0 - 200 €	200 - 1,900 €	1,900 - 5,500 €	5,500 - 25,000 €	25,000 € à plusieurs centaines de millers d'€

FIGURE 5.8 – Tarifs des influenceurs
source : Kolsquare

7. une étude a constaté que le prix des billets est aussi plus élevé aux heures de pointes, à midi et en début de soirée.

La musique

La musique est le premier produit culturel immatériel qui a profité de l'arrivée d'Internet. Son histoire en ligne a été marquée par le piratage.

La musique ayant été numérisée dans les années 80 avec les CD, elle était parfaitement adaptée à sa diffusion sur Internet. Le hic est que les maisons de disque ont longtemps cru qu'elles pourraient en interdire la diffusion sur Internet pour préserver la vente physique qui les arrangeait [8]. Le résultat est qu'il a fallu attendre plus de 10 ans après la création du Web pour voir une offre légale de téléchargement de musique sur Internet. Pendant ce temps, les politiques, bras armée des *majors*, ont fait la guerre au piratage, mais sans succès. Finalement ce sont les offres légales, comme Spotify pour la musique et Netflix pour la vidéo, qui ont été les plus efficaces pour lutter contre le pirage, cf figure 5.9.

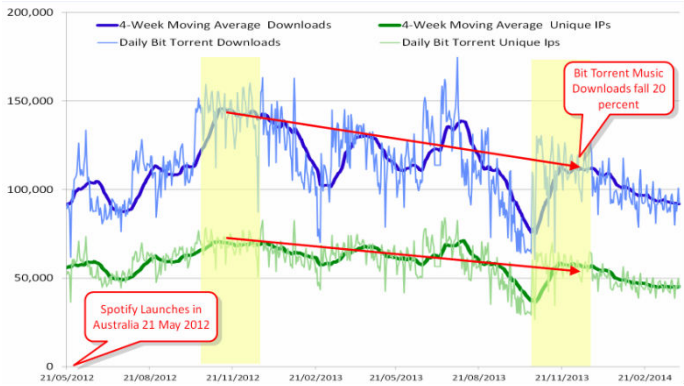


FIGURE 5.9 – Évolution de l'usage de Pirate Bay en Australie après l'arrivée de Spotify
source : Spotify 2014

Ainsi Internet a remis en cause un modèle économique qui n'avait plus de raison d'être. Puisque la musique peut être diffusée pour un coût quasiment nul, pourquoi imprimer des CD, les déposer dans des magasins pour que finalement le client les dématérialise afin de les mettre sur son baladeur et sur son ordinateur ? Ne serait-il pas préférable d'éliminer tous les intermédiaires inutiles, de réduire ainsi le prix de la musique tout en augmentant la rémunération des artistes ? Aujourd'hui la situation a évolué et l'offre légale sur Internet existe, mais les intermédiaires sont restés et parasitent allègrement les musiciens qui ont perdus l'opportunité de toucher directement leur public.

L'analyse faite en 2010 figure 5.10, montre qu'un artiste qui s'autoproduit a besoin de vendre directement 143 CD à 10 $ par mois pour avoir le SMIC [9], en passant par CD Baby il lui faut en vendre 155 (les 8 en plus étant pour CD Baby). S'il est un artiste connu qui peut négocier fermement avec sa maison de disque, alors il lui faut vendre chez les disquaires 1 161 disque (les 1 018 CD en plus étant pour les intermédiaires), s'il est moins connu cela sera 3 871 disques par mois qu'il devra vendre, toujours pour toucher le SMIC.

8. ou par flemme.
9. un SMIC à 1430 $ soit 1058 euros fin 2013

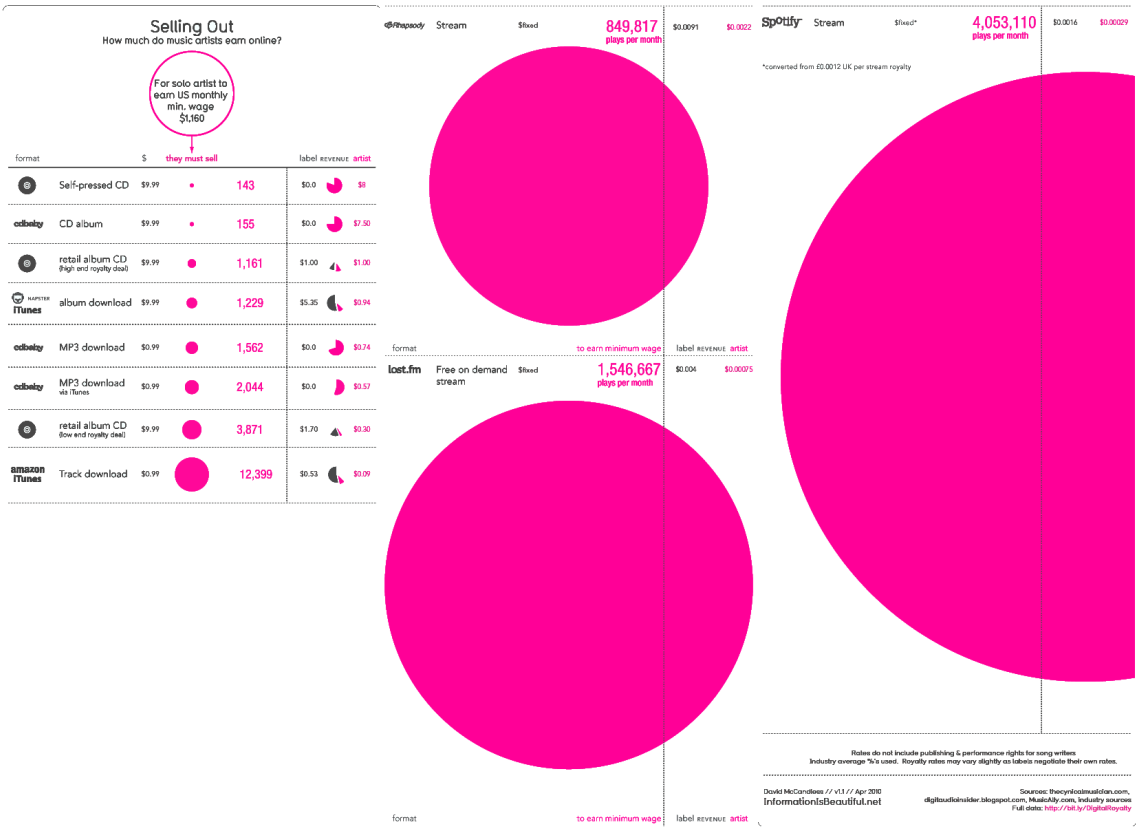


FIGURE 5.10 – Combien gagne un musicien sur Internet ?
La surface du disque indique le nombre de diffusions nécessaire pour gagner le SMIC
source : *http://www.informationisbeautiful.net/2010/how-much-do-music-artists-earn-online/*

En vendant à la chanson via iTune ou Amazon (1 $ la chanson), il doit vendre 12 399 chansons par mois (soit 1430 $ pour lui, 10 969 $ pour iTune ou Amazon). Et avec l'écoute en ligne, les revenus de l'artiste s'effondrent puisque ses chansons doivent être écoutées des millions de fois par mois toujours pour gagner le SMIC. Avec Spotify il faut plus de 4 millions d'écoutes soit plus de 13 000 auditeurs qui écoutent toutes les chansons [10] de l'album tous les jours.

La licence globale votée par l'assemblée nationale, avant que le gouvernement Fillon l'annule, proposait pour un abonnement mensuel de 5 euros d'avoir accès à l'ensemble de la musique. Si on considère qu'un abonné écoute 100 CD par mois, cela veut dire que l'écoute d'une chanson vaut 0,5 centimes. Pour toucher les 1430 $ mensuel qui nous servent de référence, il faut donc que le public écoute environ 250 000 chansons de l'artiste soit 16 fois moins que ce que demande Spotify (sachant que pour un service équivalent, Spotify demande à ses clients 10 euros par mois et non 5).

Si on raisonne dans l'autre sens, avec 24 millions d'abonnés haut débit en France, les revenus de la licence globale serait de 120 millions d'euros par mois. De quoi nourrir plus de 100 000 artistes au SMIC. À titre de comparaison il y avait 32 000 musiciens déclarés sous le statut d'intermittent du spectacle en France en 2004 (contre 7 000 en 1987). Mais l'énorme majorité

10. 10 chansons par album pour simplifier

sont au chômage et parmi eux 16 % sont au RMI [11]. Toujours à titre de comparaison, en 2012 Johnny Hallyday a gagné 630 000 euros par mois [12], plus de deux fois plus que le numéro 2. Mais ce revenu, 0,5% des revenus de la licence globale, est essentiellement lié aux concerts et non aux ventes de disques, considérées comme marginales.

Au niveau global, la musique en ligne a généré un chiffre d'affaire de 11,4 milliards de dollars en 2019, soit le double des 5,6 milliards de dollars générés en 2012. On retrouve cette évolution en France où les chiffres d'affaire de la musique en ligne et de la vente physique de musique se croisent en 2017, cf figure 5.11.

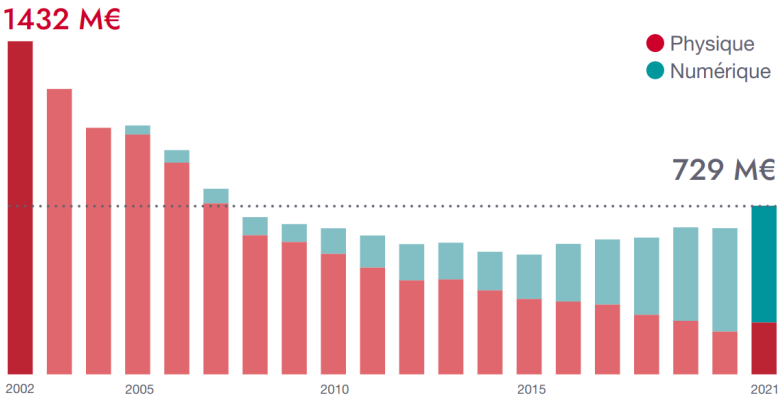


FIGURE 5.11 – Chiffre d'affaire de la musique en ligne ou sur support physique en France
source : SNEP 2022

L'audiovisuel

Il existe un autre domaine culturel de plus en plus présent sur Internet, en particulier avec l'arrivée de la fibre : l'audiovisuel. Les films avaient déjà plusieurs vies, au cinéma, à la télévision, en DVD, à la location, les voici maintenant en vidéo à la demande. Comme pour la musique, l'offre Internet de films, la vidéo à la demande, VAD ou *VOD in english*, a mis du temps pour apparaître laissant le champs libre au piratage pendant une bonne décennie. Aujourd'hui l'offre dominante est l'abonnement à Netflix et autres mais avec l'inconvénient de n'avoir accès qu'à une partie de la production audiovisuelle. Quoi qu'il en soit, ce nouveau mode de cinéma à la maison à tout chamboulé. Les ventes physiques se sont écroulées et la VAD a enfin décollé dans les années 2010, cf figure 5.12. Les majors qui ont bloqué tout changement pendant des années tout en pleurant contre le piratage, se voient finalement dépassées par des concurrents qui ont su proposer une offre adapté à Internet.

Le succès de la vidéo en ligne est largement dû aux séries dont la qualité rivalise avec les meilleurs films. Les budgets des séries grossissent régulièrement. La série mythique Game of Thrones a dépensé 15 millions de dollars pour chaque épisode de la dernière saison, soit 10 fois moins qu'un film à gros budget mais 10 fois plus qu'un épisode de série française actuelle ou 100 fois plus qu'un épisode d'une ancienne série.

11. Etude du ministère de la Culture, note "Activité, emploi et travail" 2007-2, cf http://www.culture.gouv.fr/deps
12. http://www.linternaute.com/musique/business/johnny-hallyday-son-salaire-a-presque-triple-0113.shtml

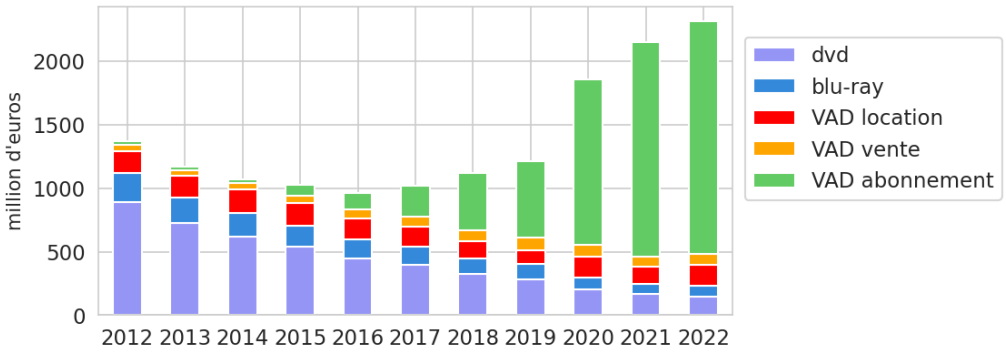


FIGURE 5.12 – Chiffre d'affaire de la vente physique de vidéos et de la VAD en France
source : CNC

Ainsi un nouveau monde télévisuel se développe avec des acteurs nouveaux comme Netflix ou Amazon qui ne produisent leurs propres séries que pour leurs clients. Ces séries associées à la liberté de regarder un film quand on veut ont séduit de très nombreux spectateurs (quasiment 200 millions d'abonnés à travers le monde en 2020 pour Netflix).

À coté, l'ancien monde de la télévision domine toujours largement, 70 % de fréquentation pour la télévision contre 6 % pour la VAD en 2019 en France [13]. Mais l'évolution lui est défavorable aussi elle s'adapte, en proposant la rediffusion à la carte et la plateforme Salto. Crée en 2019 par les principales chaînes de télévision françaises, Salto a pour but de concurrencer le Netflix. Quatre ans après, Salto est morte. On peut se demander si l'ancien monde pourra s'adapter au nouveau monde.

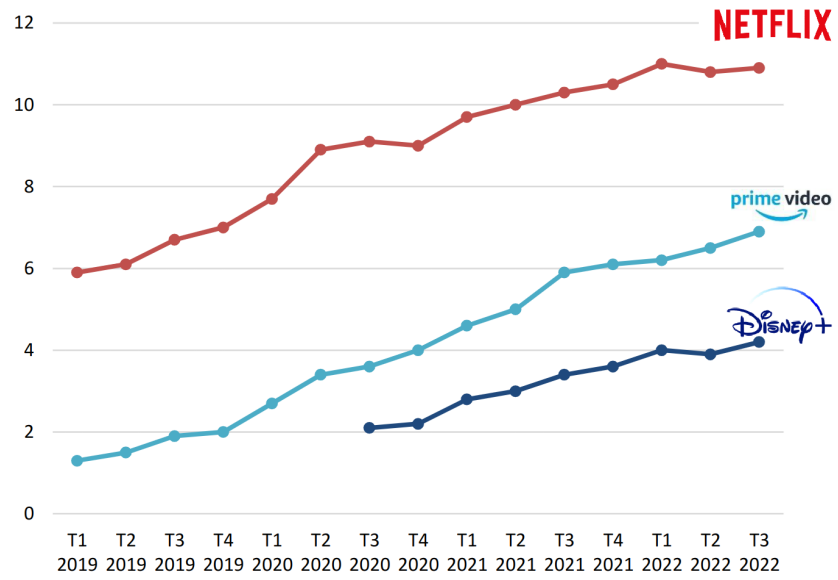


FIGURE 5.13 – Nombre de foyers en France pour les leaders de la VAD (en millions)
source : CNC 2023

13. sondage Baromètre NPA - Harris Interactive / T3 2019.

En terme de chiffre d'affaire, la VAD a atteint 1,7 milliards d'euros en France en 2022 et devrait dépasser les 20 milliards au niveau européen [14]. Ces chiffres sont à comparer aux 32 milliards de chiffre d'affaire mondial réalisé par Netflix en 2022.

Le jeu vidéo

Le marché du jeu vidéo pèse 330 milliards de dollars en 2022 (1/3 du marché du voyage). On estime à plus de 3 milliards le nombre de joueurs, la moitié étant en Asie (2 milliards en 2015).

83 % des ventes de jeux se font sur Internet. Steam propose plus de 50 000 jeux téléchargeables sur Mac, Windows et Linux.

Les jeux en ligne Un tiers des joueurs jouent en ligne (sur Internet contre d'autres joueurs). Deux tiers des revenus proviennent des jeux en ligne ce qui s'explique par le fait que les jeux en ligne demande parfois un abonnement mensuel et qu'il est possible de faire des achats au sein des jeux (objets spéciaux, avantages).

Historiquement les jeux en ligne ont commencé avec les MUD, *Multi-user dungeon*, dans les années 70 mais le véritable succès date de années 90 avec les MMORPG [15] dont le plus célèbre est World of Warcraft (2004) qui a dominé le secteur avec plus de 10 millions de joueurs de 2008 à 2014 et un gain global estimé à 14 milliards de dollars (basé principalement sur l'abonnement mensuel nécessaire pour jouer).

Minecraft, un autre grand succès dans le monde des jeux vidéo, peut se jouer seul ou en ligne. Le modèle économique repose sur la vente du jeu, la connexion au serveur pour jouer en groupe et l'achat d'extensions. Racheté par Microsoft pour 2,5 milliards de dollars en 2014, ce jeu génèré 380 millions de dollars en 2021, dont 110 millions pour la vente du jeu sur ordiphone, pour environ 130 millions de joueur (2020).

La rupture qu'offre Internet est la possibilité de créer une communauté de joueurs avec leurs codes. Des entreprises ont changé les règles (du jeu) en proposant leur jeu gratuitement, convaincues, à juste titre, de pouvoir vendre l'appartenance au club.

Free to play Les jeux gratuits se divisent en 3 groupes. Les logiciels libres qui ne rapportent pas de gains financiers à leur auteur. Les jeux gratuits qui permettent d'acheter des objets pour embellir leur personnages (des *skin* mais sans que cela change le rapport de force entre les joueurs et enfin les jeux qui offrent un avantage aux joueurs qui sont prêt à payer pour cela.

Puisqu'on s'intéresse à l'économie, examinons les jeux qui rapportent de l'argent. Dans ceux qui n'offre que des embellissements, League of Legends est un représentant intéressant du *Free to play* puisque l'entreprise Riot Games génère un chiffre d'affaire de 1,5 milliards de dollars en 2022 sans vendre le moindre jeu. Ses revenus viennent des ventes de *skin*, des publicités

14. Chiffre de l'IVF, https://www.ivf-video.org/market-information. Notons que l'IVF indique que la France représente 14 % du marché européen donc 2,8 milliards c.a.d. nettement plus que les chiffres du CNC.
15. Massive Multiplayer Online Role-Playing Game

et des sponsors dans leurs vidéos sur YouTube ainsi que dans les tournois qu'ils organisent. Riot peut générer un tel chiffre d'affaire ainsi car League of Legends compte des centaines de millions de joueurs.

Joueurs en ligne (1 heure)	1 331 475
Joueurs actifs (30 jours)	153 109 020
Heures vues sur Twitch (30 j)	95 391 662
Max vues simultanée (30 j)	433 090

TABLE 5.1 – Statistiques sur League of Legends
source : https://activeplayer.io/league-of-legends/, le 01/08/23

Fortnite est un autre jeu gratuit au succès encore plus important. Il a réuni 237 millions de joueurs sur le mois de juillet 2023 [16]. Son chiffre d'affaire est de plus de 6 milliards de dollars en 2022. Sa source principale de revenue est la vente de *skins*, de pas de danse et d'autres choses cosmétiques qui n'apportent pas d'avantage aux joueurs (peut-être un avantage psychologique si on se dit qu'un joueur prêt à payer pour cela doit beaucoup jouer. Dans certains cas c'est juste puisque certains objets demandent d'avoir un certain niveau pour pouvoir être achetés.).

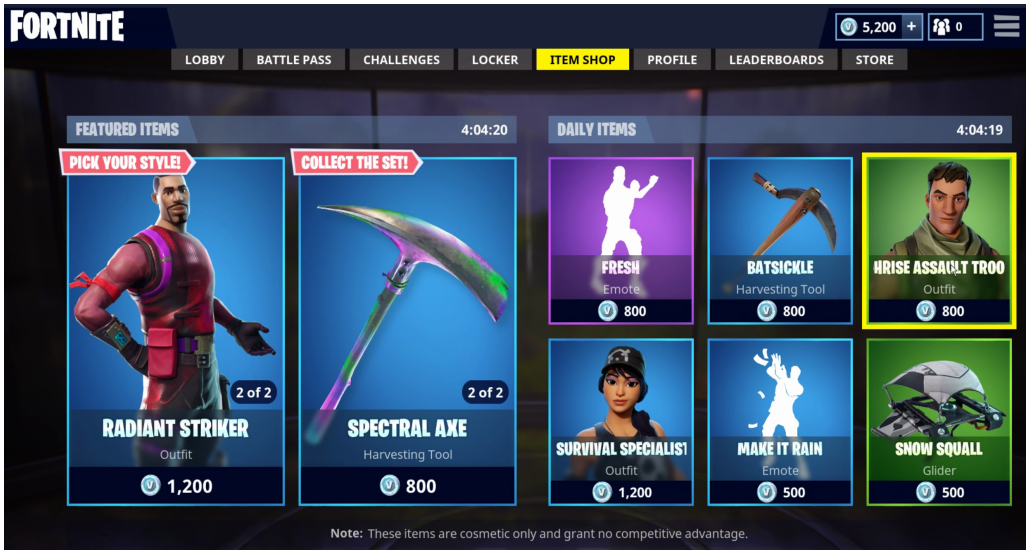


FIGURE 5.14 – Objets à acheter sur Fortnite

Dans le monde des jeux gratuits, il a aussi les *Pay-to-win* qui sont des *Free-to-play* mais dont les achats au sein du jeu offrent des avantages.

Candy Crash Saga est probablement le plus connu des jeux gratuits où payer permet d'acheter des vies et certains éléments qui aident. Avec environ 270 millions de joueurs par mois, Candy Crush a généré un chiffre d'affaire de 1,2 milliards de dollars en 2021. Il est à noter que contrairement aux jeux précédemment cités, Candy Crush ne se joue que sur ordiphone.

16. source : activeplayer.io

En Chine un autre jeu de la famille League of Legends [17] Honor of Kings est aussi un très grand succès de jeu gratuit sur ordiphone. Dans ce cas il est possible de payer pour avoir de meilleures armes ou des pouvoirs spéciaux. L'entreprise Tencent qui a développé le jeu déclare avoir 100 millions de joueurs par jour et a généré un chiffre d'affaire de 2,8 milliards de dollars en 2021.

FIGURE 5.15 – 3 MOBA à succès : League of Legends, Dota2, Honor of Kings

On peut constater que ces jeux gratuits dépassent en chiffre d'affaire les anciens jeux en ligne payants. Cela semble possible dès lors que la communauté de joueurs est suffisante, ce que permet Internet et ses 3 milliards de joueurs.

5.1.3 La vente de services en ligne

La différence entre un service et un produit immatériel n'est pas toujours simple. Est-ce que des vacances sont un service ou un produit immatériel ? D'un coté la prestation est proche du service, d'un autre le type de vente ressemble plus à celui d'un produit. Quoi qu'il en soit, cela ne change pas grand chose dans notre cas, les deux sont parfaitement adaptés à la vente en ligne.

Les sites de rencontre

Les sites de rencontre en ligne représentent un des services à diffusion du grand public les plus importants. En 2019, un tiers des européens ont utilisé au moins une fois un site de rencontre. En France on atteint 40 % pour les personnes entre 18 et 34 ans. On peut parler d'un phénomène de masse qui dépasse largement les agences matrimoniales d'antan. Aussi les sites pullulent, 2000 en France en 2019 (comme en 2012) avec des généralistes et des spécialistes dans tous les genres : politique, niveau social, religion, origine, sérieux ou pas. Dans ce dernier domaine certains sites affichent clairement leur coté sexuel, il ne s'agit plus de trouver l'âme sœur mais le bon coup [18].

Bien sûr cela ne concerne pas que la France, au niveau mondial le chiffre d'affaire était de 8,4 milliards de dollars en 2017.

Le *business model* de ces sites est relativement simple ce qui explique la multitude de l'offre. D'un point de vue informatique les coûts sont relativement bas, y compris le développement du site. L'affaire se complique pour obtenir l'audience nécessaire pour répondre au besoin

17. famille appelée MOBA : Multiplayer Online Battle Arena
18. Dans cette catégorie, Tinder arrive en tête. Il a généré 1,2 milliards de dollars de revenus en 2019.

des clients. On observe d'ailleurs régulièrement des campagnes de publicité pour lancer de nouvelles plateformes ou pour redynamiser des anciennes. Avec les sites spécialisés, le défis est moins important puisqu'on peut se permettre une communauté plus petite. Certains informaticiens gèrent seuls des sites au CA de quelques centaines de milliers d'euros annuel, largement de quoi vivre.

Pour d'autres la solution du gratuit (payé par la publicité) est tentante mais force est de constater que là aussi la voie est difficile. La concurrence est rude et surtout les sites payants sont actuellement assez gros pour pouvoir tuer ces trublions. Ainsi OkCupid, site gratuit ayant un réel succès outre Atlantique, a été acheté pour 50 M$ en 2011 par Match, un des plus gros sites payant.

Aujourd'hui le marché continue à bien se porter alors que le but de ces sites est justement de diminuer le nombre de célibataires. En fait il semble que ces sites génèrent un désir de nouvelles rencontres, qu'elles soient libertines ou sérieuses, en donnant un sentiment de facilité. Certains avancent que les sites de rencontre ont leur part de responsabilité dans la rupture des couples.

La bourse

Dans ce cas les entreprises vendent une infrastructure qui permet d'investir en bourse à un coût nettement inférieur à celui pratiqué par les banques, mais surtout l'infrastructure offre une qualité d'information et d'analyse sans aucune comparaition avec l'ancien monde.

La bourse est une vielle dame qui n'a pas bougé pendant des siècles. Un journal anglais indiquait il y a quelques décennies : « en un siècle, la seule réforme effective de la Bourse de Paris avait été le remplacement de l'éclairage au gaz par l'éclairage électrique ». Mais dans les années 70 l'informatique a fait son arrivée avec les réseaux informatiques qui ont relié les bourses du monde. La nuit du 4 août 1987, la Corbeille a disparu de la Bourse de Paris, l'informatique a remplacé les crieurs. Cette évolution a permis aux bourses de se développer et de dégager de fort gains de productivités durant les décennies qui ont suivi [19]. Bien sûr les réseaux informatiques des bourses ont été reliés à Internet ce qui a permis à tout le monde d'intervenir depuis chez soi dans les mêmes conditions que les professionnels. En 2020, durant la crise financière générée par la Covid, les particuliers ont passés 500 millions d'ordres par jour sur Euronext (qui gère la bourse de Paris, Bruxelles, Amsterdam, Dublin et Lisbonne) [20]. L'informatique puis Internet ont totalement démocratisé la bourse.

Regardons le plus gros marché financier, le marché des devises. Il a représenté en 2019 plus de 6 billions de dollars échangés à travers le monde par jour, plus que la production annuelle de produits industriels aux É-U. Bien sûr un échange d'un million de dollars US contre l'équivalent en euros cela ne représente pas la même chose qu'une production industrielle de la même somme, en particulier en terme de travail investi, mais lorsqu'autant d'argent circule un tout petit prélèvement génère des marges très importantes. Les statistiques produites par banque des réglements internationaux [21], figure 5.16, font apparaître deux points :

19. Informations extraites de l'article de M. Ruimy *De la corbeille à l'internet*, https://www.cairn.info/revue-les-cahiers-du-numerique-2003-1-page-153.htm.
20. https://www.moneyvox.fr/bourse/actualites/82781/epargne-3-chiffres-qui-montrent-que-la-bourse-a-la-cote
21. https://www.bis.org/statistics/index.htm

— le volume des transactions a explosé en 40 ans, est-ce dû à l'informatisation des systèmes boursier et leur connexion à Internet ?
— seule la part en jaune, non-financial customers, représente les échanges liés à l'économie réelle (environ 8 %).

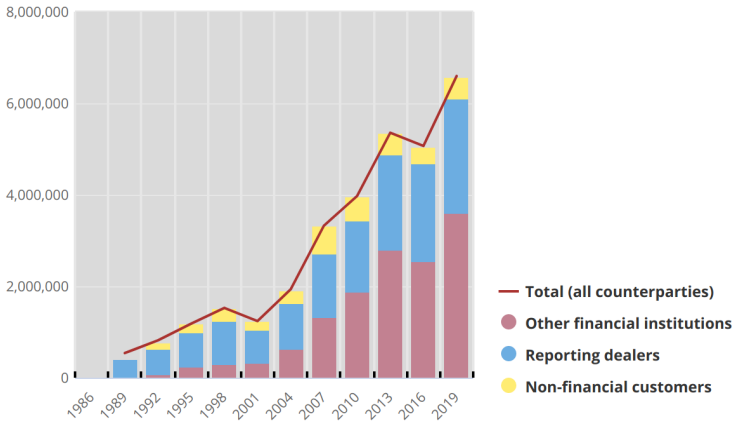


FIGURE 5.16 – Volumes du marché des devises (Forex) – chiffres en millions de dollars US
source : Banque des réglements internationaux 2020

Il serait intéressant d'avoir le volume en dollars ou en euros des plus gros marchés action depuis les années 80 pour mesurer l'impact de l'informatique puis d'Internet sur ces marchés. Malheureusement cette information n'est pas simple à trouver. Les données historiques accessibles sur Internet ne permettent d'avoir les volumes de transaction sur le New-York Stock Exchange (NYSE) seulement jusqu'en 2006 [22]. Euronext propose des données concernant ses marchés jusqu'en 2005 [23]. Dans les deux cas on ne note pas de variation significative des volumes durant ces 15 dernières années contrairement au Forex.

Une autre façon de regarder l'impact d'Internet sur la bourse est de regarder les compagnies créés avec l'arrivée d'Internet auprès du grand public. Ainsi E*Trade apparait en 1992 sur les plateformes America Online et Compuserve [24] et jusqu'à la fin des années 90 il a multiplié par 2,5 son chiffre d'affaire chaque année. C'est une belle croissance exponentielle, meilleure que celle du nombre d'Internaute qui n'a fait *que* x 2 par an à l'époque. Aussi non seulement E*Trade a profité d'un nombre potentiel de client qui augmentait en fléche mais aussi d'un plus grand appétit pour la bourse. Une étude indique qu'au milieu des années 90 20 % des américains investissaient en bourse contre 5 % dix ans plus tôt.

Autant le premier cas, Forex, ne permet pas de conclure sur l'impact d'Internet dans ce domaine, autant le second point montre qu'Internet a ouvert le marché de la bourse aux particuliers.

22. https://www.investing.com/indices/nasdaq-composite-historical-data
23. https://live.euronext.com/en/resources/statistics
24. Des réseaux informatiques des années 80 qui reliaient les passionnés d'informatique et de jeux vidéos. Bien sur ces réseaux se sont connectés à Internet dans les années 90 et sont devenus de fait des fournisseurs d'accès à Internet.

L'ubérisation

> *L'ubérisation (du nom de l'entreprise Uber) [...] consiste en l'utilisation de services permettant aux professionnels et aux clients de se mettre en contact direct, de manière quasi instantanée, grâce à l'utilisation d'une plateforme numérique.*
>
> Wikipedia

Si le nom de cette entreprise est devenu un nom commun c'est qu'il a radicalement changé le rapport au travail. Beaucoup d'entreprises ont découvert qu'un contrat à durée indéterminé, CDI, est nettement moins rentable que de faire travailler un auto-entrepreneur. Le principe c'est pas nouveau, on avait les consultants, mais la nouveauté est de ne plus avoir d'employés, mais seulement des indépendants contrôlés par une application numérique.

Ainsi Uber peut manipuler ses chauffeurs [a] à travers

- les courses proposées,
- les objectifs fixés,
- les *nudges*, manipulations psychologiques pour te faire faire ce que tu crois être le bon choix pour toi, mais qui est le bon choix pour Uber (exemple des badges),
- une vision partielle (information cachée, coté boite noire de l'application).

Et le problème est que les buts d'Uber et de ses chauffeurs sont opposés. Plus il y a de chauffeurs, moins les clients attendent et donc plus il y a course, plus Uber gagne de l'argent (25 % de commission). À l'inverse, moins il y a de chauffeurs, plus il y a de chance que la course soit pour moi et surtout plus le prix de la course est élevé, mais moins de chiffre d'affaire pour Uber.

L'ubérisation oblige dont à repenser le rapport au travail. Pour beaucoup c'est une régression des droits de l'employé puisque l'auto-entrepreneur doit gérer de son coté ses heures de travail, son salaire minimum, ses congés, arrêts maladie, natalité, sa formation et tout ce que le droit du travail garantit aux employés, sachant qu'il ne peut pas espérer financer ces droits avec 35 h de travail hebdomadaire. Par contre, pour les propriétaires de la plateforme numérique c'est le jack pot puisque le système passe très bien à l'échelle.

a. cf l'émission d'Arte à ce sujet : https://www.arte.tv/fr/videos/085801-007-A/dopamine/.

5.1.4 Les imprimantes 3D

On peut se demander ce que fait une section sur les imprimantes 3D dans ce chapitre sur le commerce électronique. On peut certes les acheter en ligne mais la raison fondamentale de leur présence ici est qu'elles vont changer nos façons de consommer et qu'elles ne sont vraiment utiles qu'avec Internet. Elles sont l'équivalent des enceintes branchées à l'ordinateur, un périphérique qui a permis la musique en ligne, la vidéo à la demande, YouTube... un périphérique nettement moins intéressant sans Internet. De la même façon les imprimantes 3D peuvent certes fonctionner sans Internet, mais leur utilitée réelle vient des plans et des logciels qui sont distribués sur Internet.

D'ailleurs les imprimantes 3D datent des années 80, il ne s'agit donc pas d'une nouveauté mais elles deviennent populaires seulement dans les années 2000. Les entreprises les utilisaient essentiellement pour faire des prototypes et de maquettes. Et pourtant on présente aujourd'hui

ces imprimantes comme une révolution.

Bien sûr en 40 ans les imprimantes se sont améliorées et permettent aujourd'hui l'impression en presque tous les matériaux possibles. Mais la révolution principale n'est pas à ce niveau, même s'il ne faut pas sous-estimer ce point (lorsqu'on ne construira plus les maisons mais qu'on les imprimera, le monde aura changé).

FIGURE 5.17 – Impression de maison par PERI

La principale révolution est la numérisation de notre monde et la capacité de partage des objets numériques qu'offre Internet. Avec un logiciel libre comme Blender il est relativement simple de créer les plans 3D d'objets. Il est encore plus simple de prendre sur Internet les plans d'un objet existant et de les adapter. Aussi l'envie d'avoir des imprimantes à un coût accessible est naturellement née dans les milieux dit *geek* pour boucler la boucle et appliquer au monde réel la recette des logiciels libres. Ainsi l'humanité pourra créer, partager les plans et imprimer les objets dont elle a besoin.

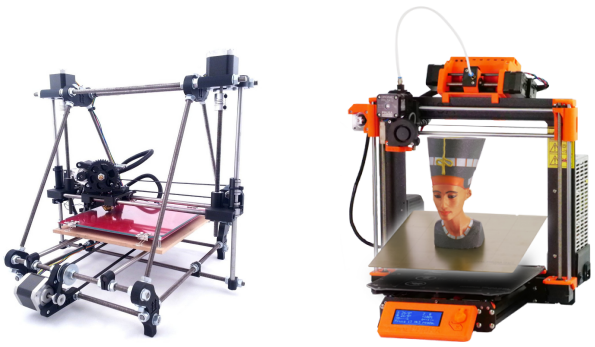


FIGURE 5.18 – RepRap Prusa Mendel (2010) et Prusa i3 MK3 avec 5 filaments (2019)

On peut deviner le mouvement idéologique derrière cette révolution apparemment technique. Pour les concepteurs de ces imprimantes populaires [25], il s'agit de se libérer de la mécanique lourde des entreprises et de lancer une nouvelle forme de production où le partage sera maître. La lutte contre le gâchis qui veut qu'on jette les objets plutôt que de les réparer, la lutte contre la délocalisation des centres de production et contre la surproduction sont aussi des idées asso-

25. début 2013, on trouve un bon nombre d'imprimantes 3D en kit pour moins de 500 $

ciées à ce mouvement. Bien sûr le premier objet qu'une imprimante doit pouvoir imprimer est une imprimante ou du moins les pièces qu'on ne trouve pas facilement dans le commerce [26].

Il est intéressant de constater que la sauce a pris. Même si les objets de ces premières imprimantes de *geek* étaient de qualité médiocre par rapport à des produits industriels, ces imprimantes abordables ont eu un véritable succès à la façon des premiers ordinateurs grand public (ZX81, Commodore 64...). Ce succès a ouvert la voie et rendu crédible l'idée que l'on aura tous accès à une imprimante 3D comme c'est le cas pour les imprimantes 2D. De là on se prend à imaginer les multiples applications possibles ce qui rend le marché encore plus crédible d'où des progrès en nette accélération avec de plus en plus de types de matériaux et le cercle vertueux est en marche.

En 2018 1,42 millions d'imprimantes 3D ont été vendues.

Légalité des reproductions

Ce que certains voient comme une avancée fait craindre à d'autres une perte économique sévère. Il serait naturel en effet qu'un changement de paradigme aussi important bouleverse les positions actuelles et donc que certains y perdent.

La crainte principale est celle du piratage. Les imprimantes 3D vont-elles faire faire au milieu industriel ce qu'Internet à fait à la musique ? L'analyse de la section 5.1.2 montre que les intermédiaires du monde de la musique ont bien fait de crier au loup puisque finalement ils continuent à se tailler la part du lion quand les artistes ont perdu l'occasion d'avoir un accès direct à leur public et sont restés aussi pauvres qu'avant.

Dans le cas des imprimantes 3D la situation est plus complexe. Un objet vendu est rarement le résultat d'une seule personne ou d'un petit groupe. De plus un objet produit en masse restera nettement moins cher qu'un objet imprimé. Aussi la crainte se situe à un autre niveau. Les designers, qui avaient la garantie que leur porte savon en plastique vendu 30 euros leur rapporterait légitiment un salaire, vont en effet avoir des soucis à se faire. Avec l'arrivée d'imprimantes plus performantes, un moulin à poivre en verre et métal sera aussi imprimable et plus généralement un grand nombre d'objets design vont subir de plein fouet l'arrivée des imprimantes 3D. Il existe déjà des sites web de plans numériques à imprimer où tout le monde peut déposer son plan de moulin à poivre. Il est sûr que des plans pirates y sont ou seront déposés. Coincé entre la concurrence et le piratage, le designer va devoir s'adapter (comme d'autres avant lui).

Certains designers vont s'adapter en vendant leurs plans à imprimer et en profitant du système pour personnaliser leur objets ou en vendant des multitudes de variantes. D'autre vont se battre pour restreindre l'usage des imprimantes 3D. La bataille a déjà commencé comme le montre cette intervention à l'assemblée nationale :

> *M. François Cornut-Gentille attire l'attention de M. le ministre du redressement productif sur les moyens d'action contre les risques de reproduction illégale liés à la*

26. donc pas les boulons, les tubes et les moteurs.

> *diffusion à venir d'imprimantes 3D sur le marché français. Ces imprimantes permettent en effet à son utilisateur de reproduire tout type de petit objet, du jouet à la pièce de rechange d'appareils d'électro-ménager, sans aucun droit de propriété et à moindre frais, pour peu qu'il trouve sur internet les plans de celui-ci. La prolifération de sites de téléchargement de ce genre de fichier est à craindre dans les années à venir ; elle risquerait, à terme, d'engendrer des effets aussi néfastes pour l'industrie que ceux que connaissent actuellement les secteurs de la musique et du cinéma. En conséquence, il lui demande les dispositifs envisagés par le Gouvernement relativement à ces dangers pour la propriété intellectuelle desquels il est nécessaire de se prémunir au plus vite.*
>
> *http://questions.assemblee-nationale.fr/q14/14-32786QE.htm*

Il sera en effet tentant d'imprimer l'interrupteur cassé de son réveil plutôt que de passer par le service après vente et payer une fortune pour 2 grammes de plastique. Il est probable que certaines entreprises offriront les plans pour imprimer de telles pièces de rechange, quitte à offrir les plans de toutes les pièces, quand d'autres iront au procès contre le piratage.

FIGURE 5.19 – La Saga des Neuf Mondes par Dutchmogul

Autre exemple, le monde des jeux de plateaux. Non seulement il va devenir simple de copier les jeux existant mais la concurrence va exploser. Actuellement les éditeurs limitent le nombre de jeux pour des raisons de rentabilité et donc de nombreux jeux restent dans des cartons. Malgré cela il y a déjà beaucoup de jeux publiés et rares sont les auteurs qui vivent de la vente de leurs jeux. Ajoutons à cela le fait que les jeux de société n'ont quasiment [27] pas de protection légale et on imagine le foisonnement de jeux qui vont sortir s'inspirant les uns des autres. Malgré tout, on peut légitimement espérer qu'en court-circuitant les intermédiaires les auteurs y gagneront financièrement. Actuellement un créateur de jeu touche entre 2 et 5% du prix de vente avant distribution d'un jeu, soit à peu prêt 1 euro par jeu [28]. Il est probable que celui qui prendra le temps d'imprimer un jeu sera d'accord pour verser 1 euro, voire plus, à l'auteur (surtout avec un système de paiement simple comme celui des bitcoins par exemple).

On voit que là où la valeur de la création est plus importante que celle de la matière, l'imprimante 3D risque de brouiller sérieusement les cartes, mais pas obligatoirement négativement.

27. Le nom du jeu peut être protégé, éventuellement les graphismes et c'est à peu prêt tout.
28. cf http://gusandco.net/2011/11/04/auteur-de-jeu/

La communauté

La force des imprimantes 3D réside dans la possibilité de partager ses œuvres. L'imprimante 3D perd de son intérêt sans son catalogue d'objet sur Internet et sans la possibilité de construire avec la communauté. Actuellement l'excitation autour de l'impression 3D est autant technique que communautaire.

FIGURE 5.20 – Impression de bonbons, plâtres médicaux et de chaussures
source : Dezeen magazine

Si le domaine des jeux de société n'est quasiment pas protégé, celui de l'alimentation et de la mode le sont encore moins [29]. Cela permet à chacun de copier allègrement les autres et d'apporter son petit plus. Ainsi des recettes de bonbons, n'appelons plus cela des plans, vont rapidement fleurir sur le réseau avec l'arrivée des premières imprimantes 3D pour cuisines en 2014. Les designers en herbe vont pouvoir se lancer dans la mode avec des bijoux de fantaisie voire des chaussures ou même des habits. Il ne vous restera plus qu'à indiquer au programme de redimensionner la chaussure à votre pied.

Le domaine des prothèses médicales ou du matériel médical comme le plâtre, profite aussi pleinement des imprimantes 3D. Dans le cas du plâtre on appréciera l'innovation qui permet d'avoir un *plâtre* résistant à la douche et qui ne démange plus (cf figure 5.20 au centre). Pour les prothèses l'intérêt est surtout économique, ce qu'apprécieront les pays en voie de développement. Avec les scanners et Internet il devient simple et économique de personnaliser les prothèses même si le laboratoire qui les conçoit est à l'autre bout du monde. Gageons que des associations caritatives sauront tirer avantage de ces possibilités.

Les interdits

Mais tout n'est pas rose. Aux États-Unis, si les armes à feu ne sont pas interdites, le gouvernement essaie de réguler leur vente voire de restreindre le libre droit d'avoir une arme. Mais que peut faire un gouvernement si chacun peut imprimer une arme chez lui ? Peut-il interdire la diffusion de plan qui peuvent être assimilé à la diffusion de documents [30] ? En France l'obtention d'une arme à feu est sérieusement contrôlée. Mais là encore, va-t-on interdire les imprimantes 3D dès lors qu'elles peuvent imprimer des armes ?

29. trop utilitaire, cf la conférence très intéressante de Johanna Blakley, http://www.ted.com/talks/johanna_blakley_lessons_from_fashion_s_free_culture.html

30. Aux États-Unis la réponse est non, la diffusion de plan de tels pistolets a été reconnue légale en 2018 au non de la liberté d'expression.

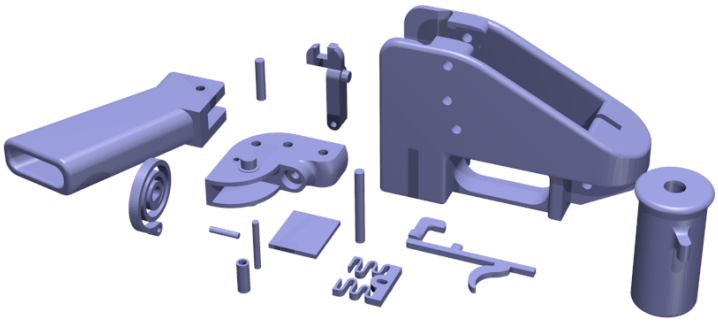


FIGURE 5.21 – Pistolet Liberator 1.1 de Defense Distributed
Rendu par Blender à partir des plans téléchargés

Le pistolet Liberator publié en 2013 est le résultat d'un projet visant à rendre impossible le contrôle des armes. Cette arme est en plastique, sauf les balles, ce qui la rend facile à fabriquer. Elle est peu chère et transparente au détecteur de métaux. Elle reste certes loin des performances usuelles d'un pistolet, elle n'a qu'une seule balle et n'est pas encore d'une efficacité parfaite, mais l'impression 3D en métal existe aussi. Ainsi Solid Concepts a imprimé un pistolet semblable à ceux du commerce. Dans ce cas le but était de montrer que les imprimantes 3D sont assez précises pour faire des objets fonctionnels de qualité en métal.

Il existe un autre domaine où l'arrivée des imprimantes 3D va poser des problèmes légaux, celui des médicaments. Un projet de recherche en cours vise à créer une imprimante permettant d'imprimer des molécules [31]. Là encore les changements vont être fondamentaux. L'accès au soin, en particulier aux médicaments génériques, va être grandement simplifié à travers la planète. Chaque patient pourra avoir exactement le dosage qu'il lui faut. Plus besoin d'une liste compliquée de médicaments, une seule capsule par repas ou moment de la journée. On peut même imaginer que les médicaments seront tellement personnalisés qu'il n'y aura plus deux médicaments identiques. Cet aspect sonne la mort des pharmacies actuelles qui deviendront peut-être un nouveau type d'imprimerie. Les plans des médicaments spécialisés viendront encore probablement des compagnies pharmaceutiques ainsi que les *encres* nécessaires à la création des médicaments. On devine que le contrôle de la diffusion de ces encres risque rapidement de devenir impossible.

Un autre domaine est aussi directement concerné par une telle imprimante, celui des drogues. Elle pourra les rendre plus accessibles ce qui devrait désorganiser les milieux mafieux, qui vendront peut-être les *encres* nécessaires.

Les plans des drogues et des médicaments vont circuler, c'est inévitable, d'ailleurs de nombreuses molécules sont déjà disponibles dans des livres et sur Internet.

31. cf l'interview de Lee Conin http://www.bbc.com/news/uk-scotland-17744314

5.2 Le commerce inter-entreprises – B2B

Le B2B est comme le B2C mais à destination des entreprises. Il suit a priori les mêmes évolutions que le B2C mais de façon nettement moins visible, car moins étudié, plus compliqué et peut-être plus secret [32].

Aux États-Unis, en 2018, la part en ligne du B2B industriel représente 4 T$ soit 67% du B2B industriel c.a.d que 67% de la production a été vendue via Internet. Il s'agit d'une progression remarquable en deux décennies, + 200 %, cf figure 5.22.

Pour les services les choses sont différentes puisque l'achat par Internet est encore inférieur en pourcentage aux ventes en ligne pour le grand public. Si les services sont simples à dématérialiser, l'interaction pour aboutir à un accord est plus complexe qu'un simple achat et on continue à préférer rencontrer physiquement un conseiller, expert, avocat plutôt que de faire la transaction en ligne.

En pourcentage, le B2B industriel en ligne est supérieur au B2B des grossistes qui est supérieur au B2C. La figure fig. 5.23 montre que les 2/3 des entreprises de production manufacturière commandent en ligne, lorsqu'on passe aux grossistes, ils ne sont plus qu'1/3 pour finalement arriver à la vente au détail en ligne qui ne représente que 10 % des ventes.

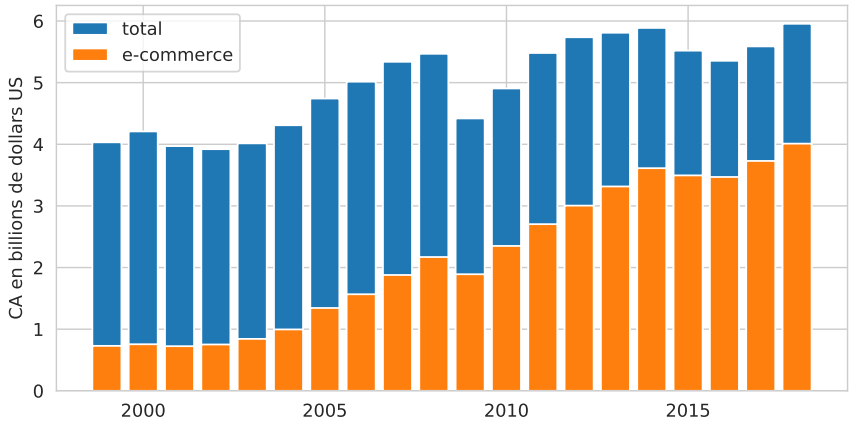


FIGURE 5.22 – Évolution du B2B aux États-Unis pour les produits manufacturés
source : US Census Bureau

32. Les chiffres des États-Unis sont les seuls que j'ai trouvés.

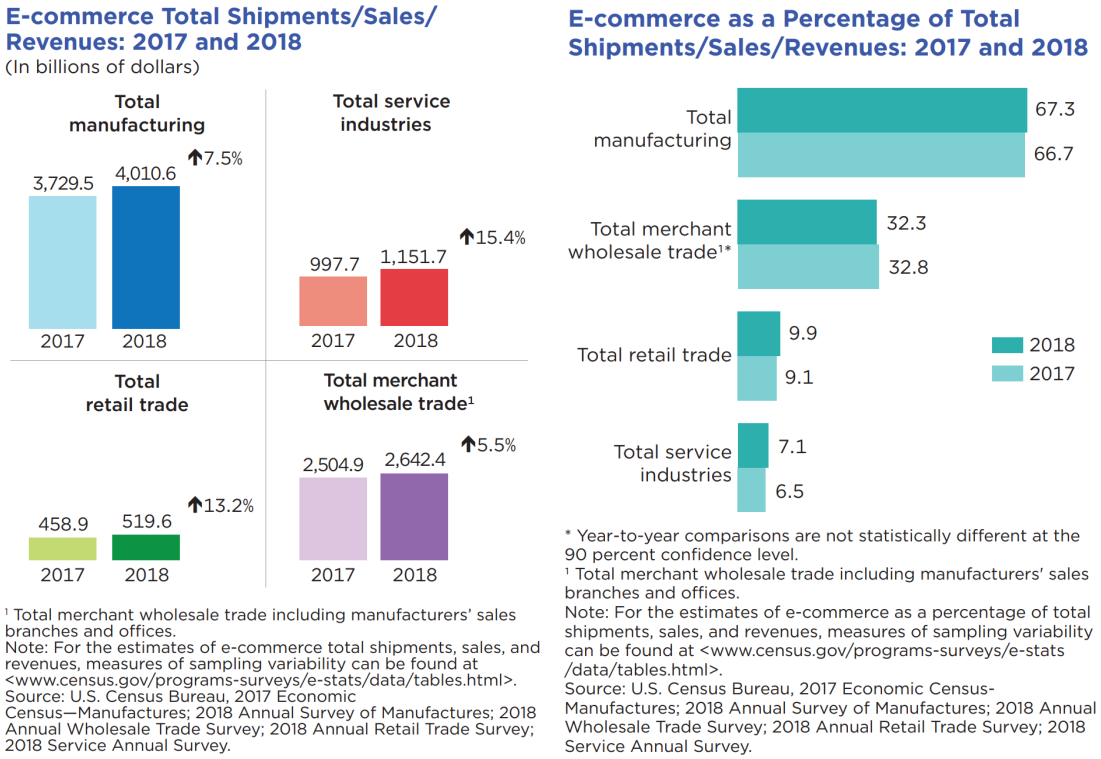


FIGURE 5.23 – Évaluation du B2B aux États-Unis en 2018
source : US Census Bureau 2020

Forrester indique de son coté que le B2B en ligne aux États-Unis était de 1,1 billions de dollars en 2018 soit 12 % du B2B [33] ce qui est nettement inférieur aux chiffres du Census Bureaux. On voit la difficulté à mesurer ce marché.

Si les services ne sont que très peu en ligne, il existe un autre domaine qui lui utilise pleinement Internet, c'est la bourse.

33. https://www.forrester.com/report/US+B2B+eCommerce+Will+Hit+18+Trillion+By+2023/-/E-RES136173

Chapitre 6

Payer en ligne

Qui dit commerce électronique dit paiement et de préférence un mode de paiement qui dépasse les frontières. Devenir le mode de paiement de référence peut être hautement lucratif aussi tous les acteurs financiers ont essayé à un moment de pousser leur solution sur Internet et de nombreuses startups sont nées [1]. Les vainqueurs sont pour l'instant PayPal et les crypto-monnaies.

On sait que l'argent, sous-jacent aux modes de paiements, est intrinsèquement source de pouvoir. Contrôler les transactions permet de prélever un pourcentage mais celui qui contrôle les moyens de transfert, les comptes bancaires, voire la monnaie peut en tirer d'autres avantages économiques et politiques nettement plus importants. Par exemple Paypal peut surveiller l'activité de ses usagers voire bloquer leur compte, vendre des données relative à ses clients, permettre de les contacter, faire des statistiques... Lors de la crise de 2008, les banques ont bien fait comprendre que si elles meurent, toute l'économie s'effondrerait. Avec tant de pouvoir, il semble naturel de confier cet outil de base de notre économie à l'État ou au moins que l'État puisse contrôler cette activité [2]. C'est le cas pour les monnaies nationales. Pour les institutions financières aussi mais partiellement, le contrôle étant limité par l'influence qu'ont les banques sur les politiques. Il existe aussi des monnaies et systèmes de paiement alternatifs et suivant les cas, l'attitude de l'État varie à leur égard. Ainsi les systèmes d'échange locaux (SEL) et les crypto-monnaies ont été interdits, tolérés ou encouragés suivant les lieux et époques.

Du point de vue purement financier, les revenus que peut générer un moyen de paiement ou une monnaie sont très importants. Les prélèvements sur les paiements avec les cartes de

1. qui se souvient de Mondex, eCash, e-gold ou S.E.T. ?
2. Depuis 2007 Paypal Europe est devenu une institution financière. Cela peut limiter les dérives spécifiques de PayPal mais les banques n'ont pas réellement cédé de pouvoir malgré la crise qu'elles ont générée.

paiement ont généré un revenu de 2,6 milliards pour les banques françaises en 2009 [3]. En 2012 Visa a dégagé un bénéfice de plus de 2 milliards de dollars et MasterCard un peu moins de 3 milliards. Alors bien sûr devenir le système de référence pour des milliards d'internautes fait rêver.

Mais le chemin est difficile. Il faut convaincre les internautes avec toute leur diversité, les sites marchants et surtout les institutions financières si on désire se relier au système monétaire physique. Il faut aussi satisfaire aux critères des États, stricts pour la création d'un mode de paiement, quasiment impossibles pour la création d'une monnaie [4], la monnaie étant un symbole fort considéré par de nombreux états comme relevant de la souveraineté nationale. Pourtant certains économistes sont pour une séparation de la monnaie et de l'État. L'Europe avec la Banque Centrale Européenne indépendante va dans ce sens. La porte n'est donc pas totalement fermée. On constate que les institutions observent toujours avant éventuellement d'interdire ou de valider. Dernièrement ce sont les bitcoins et plus largment les crypto-monnaies qui sont au cœur des préoccupations des banques centrales et de pays.

Dans cette partie nous allons donc regarder l'histoire et l'avenir des modes de paiement avec leur application à Internet ainsi que l'arrivée de nouvelles monnaies et leur impact dans notre monde physique.

6.1 La théorie

La première monnaie a été le grain d'orge, utilisé 3000 ans avant notre ère. Les cauris, des coquillages qui ont l'avantage d'être imputrescibles, ont été utilisés depuis -1300 av. JC jusqu'au 18e siècle. Les pièces de monnaie ont plus de 25 siècles. Puis est arrivé l'ère de la monnaie papier. Les lettres de changes date du 13e siècle, les billets de banque du 18e en Europe [5], les chèques du 19e. Enfin les cartes bancaires et les virements en ligne sont apparus au 20e siècle. Aujourd'hui les modes de paiement les plus usuels dans le monde physique sont :

1. le liquide ;
2. les chèques ;
3. les cartes bancaires ;
4. les versements.

Ils font tous intervenir un payeur, un bénéficiaire et leur banquiers respectifs mais de façons différentes. De plus chaque méthode a ses avantages et inconvénients. L'idéal serait d'avoir une monnaie électronique qui garde les avantages sans les inconvénients.

3. source : L'avenir de moyens de paiement en France par G. Pauget et E. Constans, mars 2012
4. Des simili-monnaies sont acceptées comme les Miles des compagnies aériennes, certes très limité à l'usage, mais dont la masse monétaire dépasse celle des dollars (The Economist 2005).
5. La Chine a utilisé des billets de banque autour de l'an 1000.

Le paiement en liquide permet de sauvegarder l'anonymat du payeur tout comme celui du bénéficiaire. Il permet les transactions entre particuliers. Enfin il est bien adapté à de petites sommes et permet aux parents d'envoyer leur enfant acheter le pain.

Son inconvénient principal est l'impossibilité d'annuler l'argent perdu ou volé pour pouvoir être remboursé. Cela le rend peu pratique pour le paiement de grosses sommes. On peut aussi lui reprocher sa divisibilité peu aisée, à savoir la difficulté pour faire la monnaie.

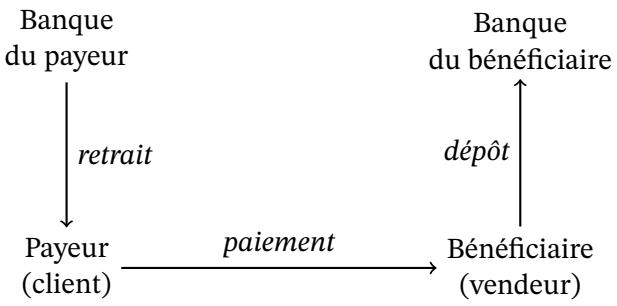


FIGURE 6.1 – Paiement en liquide

Les chèques suivent le même schéma que le liquide avec l'avantage de laisser une trace et de pouvoir toujours payer la somme exacte. Ils permettent les transactions entre particuliers et peuvent être annulés lorsqu'on les perd.

Le paiement par carte est très largement utilisé à travers le monde. Le nombre de carte de paiement Visa est de 3,4 milliards en 2019 (2,1 milliards en 2012). Celui de MasterCard est équivalent par contre UnionPay, le système chinois, avec ses 7,5 millards de cartes en circulation correspond à Visa + MasterCard [6].

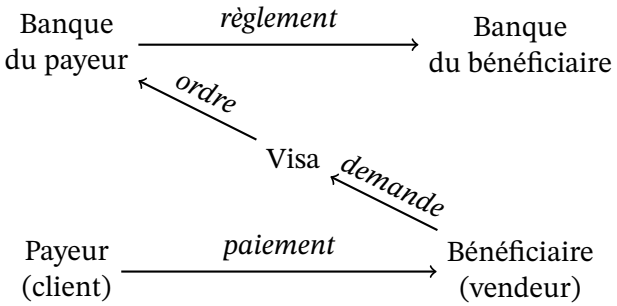


FIGURE 6.2 – Paiement par carte bancaire

Son fonctionnement permet d'avoir toujours l'appoint et garantit la sécurité grâce à la puce qui empêche un autre de l'utiliser.

Mais la carte peut être utilisée sans la puce. Cela permet la fraude sur Internet puisque le marchand dispose de toutes les informations pour faire des prélèvements. Il peut donc prélever de façon abusive, donner les informations à des personnes tierces ou se les faire voler. Notons enfin que la carte de paiement ne permet pas à des particuliers d'échanger de l'argent.

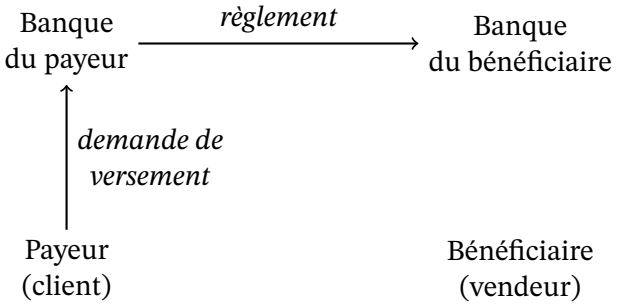


FIGURE 6.3 – Versement interbancaire

Les versements sont normalement le type de paiement le plus sûr. Ils sont dédiés aux sommes importantes et surtout adaptés au monde professionnel que ce soit pour payer les employés ou payer une autre société. Ils peuvent aussi être utilisés par les particuliers sur Internet pour payer un magasin ou un ami.

On peut les trouver trop lourds pour le paiement de petites sommes.

6. https://www.lesechos.fr/finance-marches/banque-assurances/le-chinois-unionpay-vient-defier-visa-et-mastercard-en-europe-1025

Ces exemples permettent d'établir une liste des avantages potentiels d'un moyen de paiement :

— la simplicité d'utilisation ;
— l'anonymat ou à l'inverse l'enregistrement de la transaction ;
— l'intégrité de ses économies si on perd le moyen de paiement ;
— la transaction entre particuliers ;
— la divisibilité ou la possibilité d'avoir toujours la somme exacte ;

À cette liste on peut ajouter les qualités nécessaires pour un moyen de paiement sur Internet :

— la garantie de l'intégrité de la transaction : soit le client est débité et le vendeur crédité, soit rien ne se passe,
— la sauvegarde des transactions afin de pouvoir retrouver l'état des comptes en cas de panne du système,
— la sécurité aux attaques de pirates, à la création de fausse monnaie, à la copie des billets électroniques...,
— la portabilité qui permet à tous les systèmes (ordinateurs, tablette, téléphone...) de communiquer,
— la convertibilité qui permet d'être changé en un autre type de monnaie (vers de la monnaie papier, vers une autre monnaie électronique...).

Notons que parmi ces caractéristiques, une seule est souhaitable ainsi que son contraire à savoir l'anonymat. Cela mène à deux catégories :

— les paiements anonymes, pour les petites sommes le plus souvent donc appelés les micro-paiements ;
— les paiements nominatifs ou vérifiables pour les sommes plus importantes.

À l'usage on retrouve bien ces deux catégories avec les autres caractéristiques qui se rattachent naturellement. Ainsi la simplicité d'utilisation est nécessaire pour les micro-paiements mais non nécessaire pour les paiements important où on accepte plus facilement de subir des étapes de vérifications. De même on peut accepter de perdre un porte-monnaie électronique qui a 10 euros, mais on n'acceptera pas que les traces du virement de son loyer aient disparues alors que l'argent a été débité.

En pratique on constate que les solutions développées ne suivent pas obligatoirement cette dichotomie. Ainsi les paiements avec téléphone sont souvent micro mais nominatifs alors que ceux avec des bitcoins peuvent être importants et anonymes.

6.2 Les micro-paiements

Le but est de développer un système pouvant remplacer le liquide. Des solutions s'appuient sur des porte-monnaies électroniques, d'autres réalisent des versements, enfin certaines sont purement logicielles et vont avec le développement de nouvelles monnaies. Ces dernières seront étudiées dans la section **??** sur la monnaie électronique.

Les solutions basées sur un porte-monnaie électronique se retrouvent dans de nombreux pays, mais ne traversent pas les frontières. Une solution française a été Monéo, héritière de la solution allemande Geldkarte. Elle permettait de payer un trajet de bus, un café rapidement, sans vérification comme pour du liquide. Elle a échoué et été remplacée par le paiement sans contact des carte bleues.

Sur Internet, une solution immatérielle a rencontré un véritable succès : Paypal. Ce système de versement est devenu de fait la référence du paiement en ligne même si les cartes bancaires restent plus utyilisée.

Enfin la véritable innovation en matière de paiement en ligne est la crypto-monnaie dont Bitcoin est l'initiateur et encore la référence.

Quelle que soit la mécanique développée, on sent que la difficulté liée aux micro-paiements électroniques réside dans la facilité avec laquelle on peut recopier une pièce de monnaie digitale puisqu'il ne s'agit que de 0 et de 1. Pour éviter les problèmes de fausse monnaie tout en gardant la facilité d'usage du liquide, différentes approches se dégagent :

— le porte monnaie électronique avec un support physique, une carte par exemple avec un lecteur,
— la solution logicielle avec sa sécurité intégrée au code (en utilisant la cryptographie),

Bien sûr, si on retire l'anonymat, qui est une des caractéristiques principales des micro-paiements, alors il existe une solution simple : le versement inter-comptes (ce que fait Paypal).

6.2.1 Le porte monnaie électronique

La carte à mémoire, brevetée en 1975 par Roland Moreno, a fait ses premiers pas en tant que carte téléphonique. Avec le temps elle a évolué pour devenir la carte à microprocesseur que l'on retrouve partout, de la carte bancaire à la carte Vitale en passant par les cartes SIM, Navigo, jusqu'aux cartes programmables comme les JavaCards. Chaque année, des milliards de cartes à puce sont fabriquées à travers le monde.

La sécurité de ces cartes est basée sur la difficulté à violer la puce avec un mécanisme de protection qui s'active en cas de tentative d'infraction. Ainsi la puce d'une carte bleue se bloque si l'on ne donne pas le bon code trois fois de suite.

Mais comme tout coffre fort, la sécurité n'est jamais totale comme cela a été démontré dernièrement lorsque la clé privée d'authentification de la véracité d'une carte bleue a été diffusé sur Internet, rendant possible la création de fausses vraies cartes (cf l'affaire Humpich et le dossier de Parodie.com).

D'un point de vue pratique, le point faible des cartes à puce à contact est le besoin de lec-

teurs pour communiquer. Cet aspect interdit les transferts d'argent entre particuliers [7] et rend caduque la sécurité de la puce lors des paiements sur Internet. Notons que cet aspect est nettement moins vrai pour les cartes à puce radio, il existe déjà des ordiphones qui peuvent communiquer avec de telles cartes.

Malgré ces inconvénients, la carte à puce est très largement utilisée ce qui en a fait un bon candidat pour un porte-monnaie électronique physique.

La Geldkarte (1996–2025) a été introduite en Allemagne en 1996. Ses principaux succès semblent être comme mode de paiement pour les transports en commun et pour les parcmètres. L'année la plus faste a été en 2007 avec une transaction moyenne qui a fortement chutée pour remonter doucement à 3 euros. Mais l'utilisation de la carte est en chute constante depuis 2007, cf figure 6.4, aussi en 2018 la Deutsche Bank annonce l'abandon de ce type de carte. En 2020 d'autres banque se retirent et la fin de la Geldkarte est prévue pour 2024/2025.

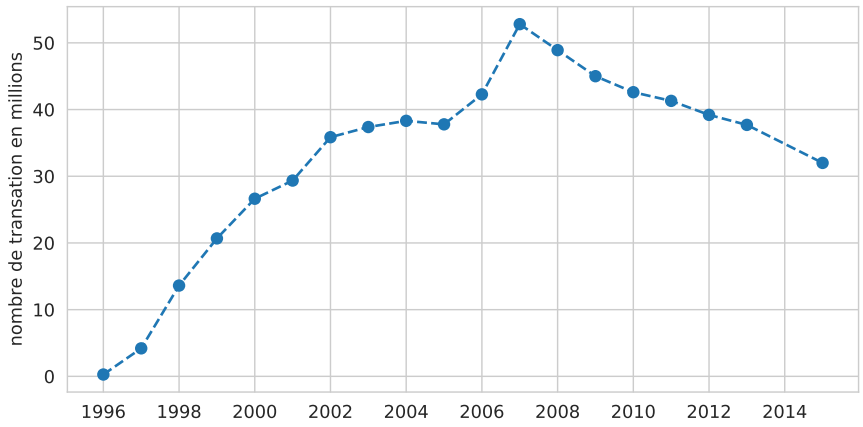


FIGURE 6.4 – Évolution de l'utilisation de la Geldkarte entre 1996 et 2015
source : bankenverband – Union des banques allemandes et Wikipedia

Le coût d'utilisation de la carte est de 0,3% de la transaction avec un minimum d'un centime. Le coût d'acquisition de la carte auprès de sa banque est en général nul mais peut être payant si la banque le décide.

Il est possible d'utiliser sa Geldkarte pour effectuer des paiements sur Internet avec un lecteur de carte à puce connecté à son ordinateur (prix : 60 euros).

Monéo (1999–2017) était l'application française de la Geldkarte. Elle a été créée par BMS, un consortium de banques françaises [8]. Son déploiement, lancé à Tours en 1999, est arrivé à Paris et sa région fin 2002 et a couvert l'ensemble du territoire en 2003.

7. ce qui de toute façon n'est pas au goût de la Banque de France qui craint des fraudes et son utilisation pour le blanchiment de l'argent sale

8. le Crédit Agricole, la BNP (28,5 % chacun), les Banques Populaires, le Crédit Lyonnais, le Crédit Mutuel (10 %), le CCF (7 %) et le CIC (6 %)

Elle permettait à l'utilisateur de payer des petites sommes, inférieures à 30 , € simplement et rapidement mais elle coûtait cher tant aux particuliers qu'aux commerçants.

En 2005 l'UFC [9] indiquait :

«*Moneo demeure un produit sans grand intérêt pour les consommateurs, et cela tant qu'il ne sera pas gratuit et totalement indépendant des banques.*»

En 2013 l'échec de Moneo est pattant. La BNP, la Poste et la Caisse d'Épargne se désengagent. Le groupe BMS-Moneo se reconvertit dans les cartes de restauration pour étudiants et vise le marché des tickets restaurants. En 2017 c'est la fin, Monéo-Resto est racheté par Edenred (tickets restaurants).

Techniquement, Monéo utilisait l'algorithme de chiffrage triple DES pour valider les cartes, probablement suivant le même principe de *défi* que les cartes bleues mais avec une clé plus longue. Le SCSSI [10] a certifié les composants de Monéo.

Pour des raisons de simplicité et de rapidité lors du paiement seule la vérification de l'authenticité de la carte était faite. Aucune vérification n'était faite pour vérifier que le porteur est bien le propriétaire de la carte. Il n'y avait pas de code à taper.

Il était possible de recharger sa carte sur Internet, après avoir acheté un lecteur de carte à puce, mais pas de l'utiliser pour faire des paiements a priori.

6.2.2 La carte radio

L'un des inconvénients de la carte à puce est le besoin d'avoir un lecteur et d'y insérer la carte pour effectuer une transaction. Ces lecteurs sont encombrant, coûtent chers et, à l'usage, la transaction est plus lente que s'il suffit de passer sa carte à proximité du lecteur. La carte radio [11], ou carte NFC du nom de la norme, répond à ces problématiques :

— un lecteur NFC tient dans une puce et son coût est négligeable. De nombreux ordiphones intègrent un tel lecteur.
— la communication radio se fait sans contact, rapidement et simplement.

Parmi les applications les plus connues de telles cartes, citons

— Navigo utilisées par la RATP dans le métro parisien,
— la carte à tout faire FeliCa développée et commercialisée par NTT DoCoMo et Sony au Japon,
— la carte de paiement PayPass de MasterCard et Motorola déjà utilisée dans plusieurs états des États-Unis.
— les cartes de paiement française qui, en plus de la puce électronique, disposent de plus en plus de la technologie NFC pour les paiements sans contacts.

9. L'Union fédérale des consommateurs (UFC-Que Choisir)
10. remplacé depuis par l'ANSSI (Agence nationale de la sécurité des systèmes d'information)
11. La carte communique par ondes radio. Pour pouvoir émettre, elle puise son énergie dans le champ électromagnétique généré le lecteur.

La norme NFC (Near Field Technology)

Comme pour la communication filaire, il existe une infinité de façon de communiquer via les ondes. Comme pour la communication filaire, il n'y a pas d'interconnexion sans norme, aussi trois acteurs majeurs, Nokia, Philips et Sony ont développé une norme pour les cartes radio, la *Near Field Technology* qui permet :

- une connexion seulement à courte distance sur 13.56 MHz (moins de 20 cm) qui garantie la connexion volontaire [a]
- le transfert de données à 106, 212 ou 424 kbit/s,
- une communication active ou passive suivant qu'on désire utiliser sa propre énergie ou celle de l'autre appareil (au moins un des deux doit être actif),
- un système d'amorçage permettant de s'authentifier puis rediriger la communication radio vers le Bluetooth ou le Wifi (d'autres protocoles radio au débit plus important)

Une extension de cette norme, la *Secure NFC*, ajoute par dessus la NFC un système d'authentification basé sur la cryptographie.

a. enfin normalement, des tests ont permis de lire une carte à plus de 10 mètres...

Ajoutons que de nombreux ordiphones intègrent la technologie NFC et disposent d'applications qui peuvent remplacer la carte Navigo par exemple ou stocker des tickets de métro. Il est également possible de payer sans contact avec son téléphone plutôt qu'avec la carte bleue.

Il ne reste plus qu'a pouvoir payer sur Internet avec sa carte NFC et donc à avoir des claviers avec lecteur NFC (la marque Cherry en propose) et des sites marchants qui permettent un tel paiement.

6.2.3 Le téléphone mobile – L'Afrique innove

Le téléphone portable étant un outil de plus en plus répandu, il n'est pas surprenant que des solutions de paiement l'utilisent. Ainsi les systèmes de paiement par carte ont couplé le paiement sur Internet avec une validation par SMS [12] pour améliorer la sécurité.

Durant les années 2000, Bouygues avait essayé de développer sa solution assez proche qui fonctionnait aussi dans le monde réel :

1. le client donne son numéro de portable au vendeur,
2. le vendeur l'entre dans son terminal relié à Bouygues ainsi que le montant de la transaction,
3. Bouygues envoie un SMS sur le portable du client et lui demande de confirmer l'achat en entrant son code secret,
4. le vendeur reçoit la confirmation de la vente et le terminal imprime le ticket.

Mais ce système n'a pas pris et n'existe plus.

12. au moment de payer votre achat, vous devez entrer sur le site web le code que vient de vous envoyer votre banque par SMS

À l'inverse, en Afrique des systèmes de paiement par téléphone sont largement utilisés. Ainsi M-Pesa au Kenya et en Tanzanie, et Zaad au Somaliland, remplacent l'argent liquide pour de nombreuses personnes avec les avantages de sécurité et de liquidité évidents.

Le paiement d'un achat avec Zaad suit la procédure suivante :

1. faire le `*888#`
2. entrer son code secret
3. indiquer que l'on désire payer un marchant : `4`
4. entrer l'identifiant du marchand
5. entrer le montant
6. confirmer
7. le marchant et le client reçoivent alors un SMS qui confirme le paiement.

Donner de l'argent à une personne suit la même procédure si ce n'est qu'on indique le téléphone de la personne et non l'identifiant du magasin. On peut aussi retirer de l'argent liquide avec son téléphone, voir son relevé "bancaire", payer des factures... Notons aussi que ce système permet de payer à distance, par exemple la glace de votre enfant alors que vous êtes au travail, puisqu'il suffit que vous sachiez le code du marchand et le montant. Dès lors le passage à l'e-économie est simple et il existe naturellement des sites web qui acceptent ce mode de paiement.

L'opérateur téléphonique Safaricom, propriétaire de M-Pesa, indique que 15 millions de kenyans utilisent M-Pesa et qu'un tiers du PNB du Kenya passe par son système de paiement (chiffres 2012). Statista indique 30 millions d'utilisateur en 2017 et 40 millions en 2020.

Notons enfin que ces systèmes alternatifs rencontrent du succès là où les offres bancaires sont réduites ou bien pour les populations qui n'ont pas accès au système bancaire. Cela place M-Pesa en situation de monopole dans ces cas, ce qui peut générer des abus comme des commissions excessives.

6.3 Les macro-paiements

Le système de macro-paiements les plus utilisés sur Internet reste la carte de débit. PayPal est second. En dehors de ces deux systèmes, on trouve les virements interbancaires et des systèmes plus marginaux. Parmi les systèmes marginaux, les bitcoins sont intéressants car anonymes, ce qui ressemble plus aux micro-paiements qu'aux macro-paiement, avec des frais d'usage importants qui en font plus une monnaie pour macro-paiements. Ils seront étudiés à la section suivante.

Alors que reste-t-il ? Pas grand chose. Regardons néanmoins le système de paiement SET qui montre que l'on peut proposer une solution techniquement bien, moralement tout aussi bien, supportée par les plus grands noms du monde du paiement, de l'informatique et même par l'Europe, sans pour autant trouver le succès.

6.3.1 SET (1996–2001)

La création en 1996 du protocole SET, Secure Electronic Transaction, est le résultat de la fusion de divers projets et de l'union des grandes sociétés du domaine que sont Visa, MasterCard, CyberCash, Netscape, IBM, Microsoft et DigiCash. Elle aurait du être un succès et ce d'autant plus qu'il s'agissait d'un protocole ouvert, donc pas de jaloux, une pérennité et intercompatibilité garantie.

Les spécifications de SET précisent chaque étape de la procédure (les spécifications "Business" sont assez précises pour comprendre en détail les différentes procédures) :

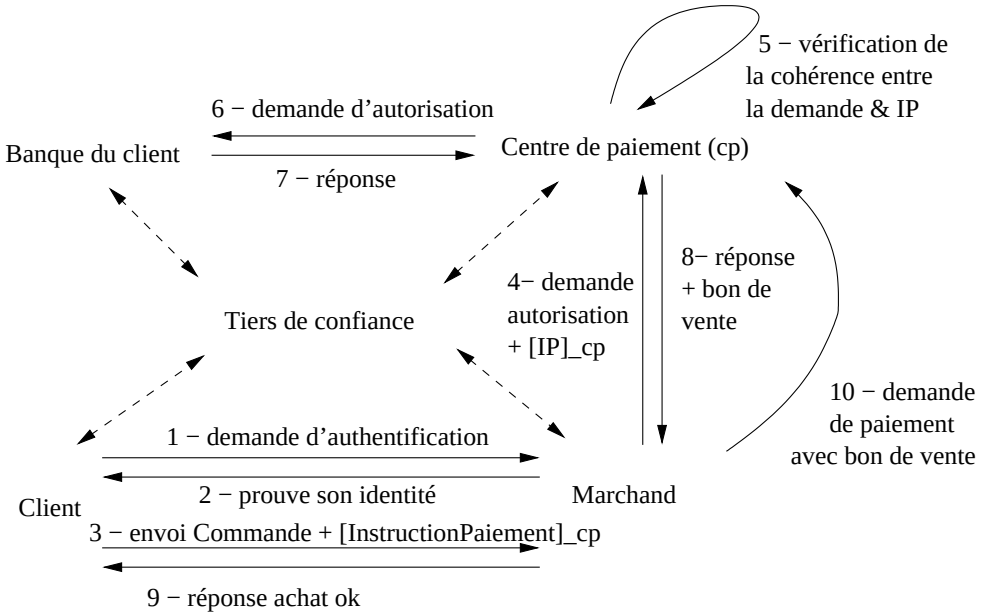


FIGURE 6.5 – Fonctionnement de SET
Les vérifications auprès du tiers de confiance sont faites
lors de la réception de chaque message pour en vérifier l'auteur

D'un point de vue technique, SET fait intervenir en plus du client, de sa banque et du vendeur, une autorité de certification (ou tiers de confiance) pour valider l'identité des partenaires et une passerelle de paiement qui centralise les demandes de paiement SET de la part des vendeurs pour décrypter l'identité bancaire du client et faire la demande à sa banque.

Du point de vue moral, la présence de la passerelle de paiement permet d'éviter que le vendeur puisse connaître les coordonnées bancaires du client. De même elle protège la vie privée du client vis-à-vis de sa banque en cachant le contenu de la commande et vis-à-vis du marchand en cachant l'identité de sa banque (cf le schéma figure 6.5).

En France l'application la plus importante de SET a été menée par le GIE Carte Bleue qui à travers sa société Cyber-COMM a promu ce système de paiement, d'autant plus intéressant pour le GIE que 60% des plaintes des porteurs de Cartes Bleues étaient alors liées à des achats

faits sur Internet.

Si SET est passé en mode de production et a été utilisé par des grands sites web comme celui de la Redoute, il n'a jamais atteint la masse critique nécessaire. Aussi courant 2001, VISA et MasterCard ont décidé d'abandonner le déploiement de SET. La nécessité pour l'acheteur de devoir disposer d'un lecteur de carte à puce relié à son ordinateur est probablement la cause principale de l'échec.

SET a finalement été remplacé par le système 3-D Secure [13] qui est utilisé tant par Visa que par MasterCard. On note que, là encore, la simplicité a gagné.

Notons aussi que l'arrivée des cartes NFC et des lecteurs dans les ordiphones n'ont pas relancé le projet.

6.4 PayPal

En tant que solution leader créée pour le paiement sur Internet, PayPal mérite sa section.

PayPal est un système lourd d'usage qui offre la traçabilité des transactions, donc plutôt pour les macro-paiements. Cependant PayPal vise aussi les micro-paiements, en particulier des micro-paiements pour biens numériques, comme un mp3 ou un article de presse [14].

L'innovation

Comment PayPal a réussi là où les autres ont échoué ? L'explication est dans la figure 6.6 extraite de leur site web. La réussite de PayPal n'est pas technique mais marketing : vous pouvez donner de l'argent à tout le monde avec PayPal, même à ceux qui n'ont pas de compte PayPal. Il suffit d'une adresse mail ou d'un numéro de téléphone. Si le destinataire n'a pas de compte PayPal, il se verra offrir le choix entre avoir un compte PayPal avec l'argent dessus ou donner un RIB pour que l'argent soit versé sur son compte bancaire. Bien sûr, comme il s'agit de petites sommes en général, le destinataire choisit d'avoir un compte PayPal. Ainsi en moins d'un an, PayPal a dépassé le million de comptes ouverts. Bien sûr ce point n'est probablement pas la seule raison du succès de PayPal. Le fait qu'un grand nombre de sites web l'accepte comme mode de paiement est certainement un élément important, ne serait-ce que pour conserver son argent sur PayPal.

Le succès initial ne s'est pas démenti comme le montrent les chiffres de la figure 6.7.

En octobre 2002 eBay a acquit PayPal pour 1,5 milliards de dollars. Une véritable synergie a pu se développer entre ces deux sites complémentaires. Lors de l'achat, les revenus de PayPal étaient d'environ 53 millions de dollars alors que ceux d'E-Bay étaient de 266 millions de dol-

13. vérification par un autre canal, SMS en général, que vous êtes bien à l'origine du paiement.

14. La commission appliquée alors est de 5 centimes + 0,6 % pour les paiements nationaux inférieur à 10 € et utilisant les codes QR, donc adaptée au commerce en ligne. Source : https://www.paypal.com/fr/webapps/mpp/merchant-fees

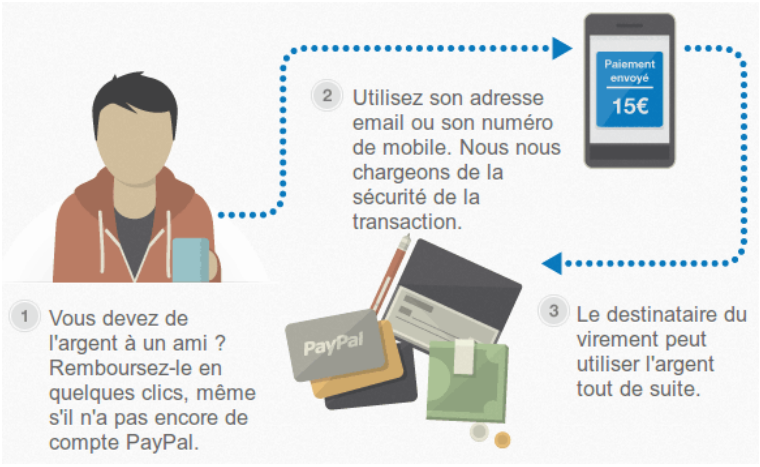


FIGURE 6.6 – Enrolement à la PayPal

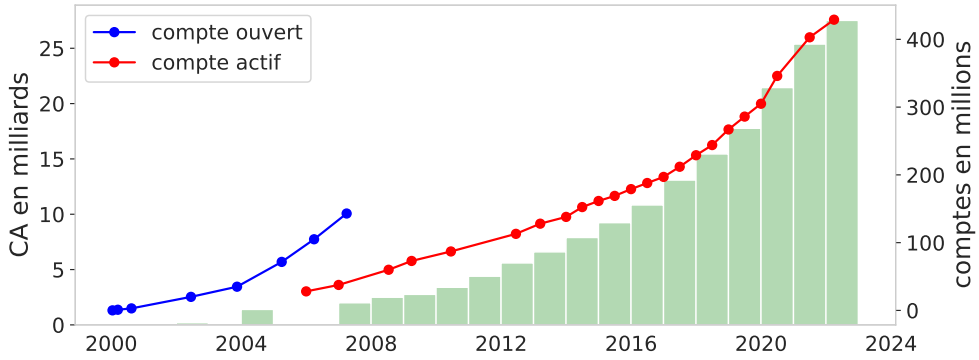


FIGURE 6.7 – Nombre de comptes et chiffre d'affaire de PayPal

Compte actif = au moins une transaction par trimestre

lars. Fin 2012 les revenus générés par PayPay ont représenté 39% des revenus de la nouvelle entreprise. En 2014 PayPal est devenue une spin-off de eBay à savoir qu'elle devient indépendante, chaque actionnaire d'eBay recevant autant d'actions de PayPal qu'il a d'actions d'eBay. En 2022 PayPal a fait un chiffre d'affaire de 27,5 G$ et un bénéfice de 2,4 G$.

Fonctionnement

D'un point de vue technique, PayPal n'est qu'un système de virements entre comptes. Aucune innovation mais un système simple qui passe par le site web de PayPal pour s'authentifier et initier ou valider le paiement. Pour des macro-achats sur Internet c'est tout à fait satisfaisant.

Le même manque d'innovation est en train d'être appliqué à une solution de paiement avec son compte PayPal dans le monde physique. Mais dans ce cas il n'est pas certain que le succès soit au rendez-vous, la procédure étant plus lourde qu'avec une carte de paiement (il faut entrer

dans le terminal du magasin son numéro de téléphone ainsi que son code secret [15]). Comme les tarifs de PayPal sont aussi plus élevés, la bataille n'est pas gagnée.

Tarifs

PayPal prend entre 3 et 4 % des montants qui transitent par son système de paiement. C'est un coût nettement supérieur à celui des cartes bleues. C'est aussi nettement plus cher que le coût des transferts interbancaires en France, en général gratuit, mais nettement moins que le coût de transfert vers l'étranger hors Europe, voir table 6.1.

Système	particulier en France	magasin en Europe (€)	magasin hors Europe
PayPal (2023)	0	0,35 € + 2,9 %	~ 0,35 € + 4,9 % + ? de change
TransferWise (2019)	0,8 €	0,8 €	1 € + 0,41 % + 0.35 % de change ($)
Carte Bleue Visa	impossible	~ 1 % (⋆)	1 € + 2,7 % (†)
Virement interbancaire (Société Générale 2019)	0	0	9 à 33 € (•) + ? de frais de change

TABLE 6.1 – Tarifs de PayPal comparé à d'autres

(⋆) varie fortement suivant les accords avec sa banque

(†) tarif 2015 Visa via la Société Générale

(•) 9 à 29 € si < 500 €, 13 à 33 € si < 4000 €, sinon ?

PayPal est surtout intéressant pour échanger entre particuliers, ensuite il faut faire attention. Si PayPal, comme les Cartes Bleues, fait porter les frais bancaires sur le vendeur, les frais de changes restent pour l'acheteur. Pour les paiements en devise étrangère, TransferWire [16] ou la carte Ultim de Boursoma sont préférables.

Pour un magasin, le choix des modes de paiement acceptés n'est pas seulement lié aux frais bancaires mais aussi à leur popularité. Aujourd'hui PayPal est assez populaire pour s'imposer de plus en plus auprès des magasins sur Internet mais pas dans le monde physique (même s'il y vient).

6.5 Les monnaies complémentaires

Si on appelle système de paiement tout système organisé permettant de rémunérer un service rendu ou l'achat d'un objet, alors il existe déjà de nombreux systèmes de paiement alternatifs mis en place de façon autonome.

Ces systèmes peuvent être limités géographiquement ou dans leur utilisation. Dans ce dernier cas on trouve Les Miles et les tickets restaurant.

15. cf http://venturebeat.com/2012/03/14/paypals-new-pos-service-is-a-piece-of-sht/
16. La néobanque N26 s'appuie sur TransferWire pour son offre en devises étrangères.

Mais les systèmes de paiement alternatifs ou complémentaires qui ont le plus marqué les esprits sont les monnaies locales, de par leur capacité à remplacer, localement, la monnaie officielle. Parmi les plus connues, citons les bons vieux Systèmes d'Echange Locaux, SEL dont la première expérience date de 1932. Cette année là, la ville de Wörgl en Autriche avait alors émis sa monnaie avec succès mais celle-ci a été interdite au bout de 9 mois par la Banque Nationale. En 1956 la même chose se produit en France à Lignières en Berry. Puis le rythme a accéléré durant les années 80 pour entrer dans les mœurs durant les années 90, voir figure 6.8.

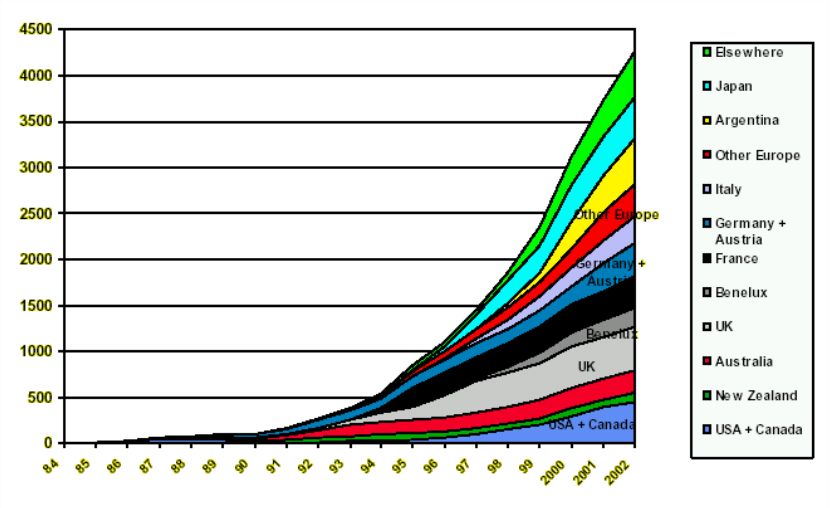


FIGURE 6.8 – Nombre de systèmes monétaires complémentaires dans 12 pays
source : Bernard Lietaer, The Future of Digital Money, 5e Digital Money Forum

Initialement le but de ce type de monnaie était d'aider les plus défavorisés, les exclus, en leur donnant une unité d'échange abordable afin de pouvoir continuer à exercer une activité. Mais elles offrent d'autres avantages. Elles garantissent que la richesse reste dans une zone géographique délimitée, ce qui favorise ses utilisateurs et donc les commerçants qui les acceptent. Elles peuvent être rattachées à la monnaie officielle ou pas. Elles peuvent augmenter la masse monétaire ou pas. Elles ont une souplesse qui les rend à même de répondre aux besoins qu'elles visent. Par exemple en Bavière, le Chiemgauer, une monnaie à parité avec l'Euro, permet de financer les associations locales en leur versant 3% des échanges Chiemgauer vers Euro [17]. Autre exemple, après la crise de 1929, des entrepreneurs suisses ont créé le WIR à parité avec le francs suisse. Il sert de relai lorsque l'argent officiel vient à manquer. Le WIR est toujours utilisé par un quart des entreprises suisses et permet de réduire fortement l'impact des crises financières. On a retrouvé cet effet d'amortisseur avec d'autres monnaies locales lors de la crise asiatique de 1997. Aussi on comprend que les États puissent voir d'un bon œil ces initiatives locales. Les États vont même parfois jusqu'à les encourager. De fait, le poids économique de ces monnaies a crû régulièrement durant les années 2000, cf figure 6.9.

En 2009, le Brésil a créé 5 banques communautaires afin de relancer l'économie dans des quartiers. Ces banques qui reposent sur des militants locaux, connaissent bien leurs *clients* et obtiennent des remboursements très satisfaisants tout en incitant les habitants à reprendre

17. cf http://www.recit.net/Le-Chiemgauer-une-monnaie

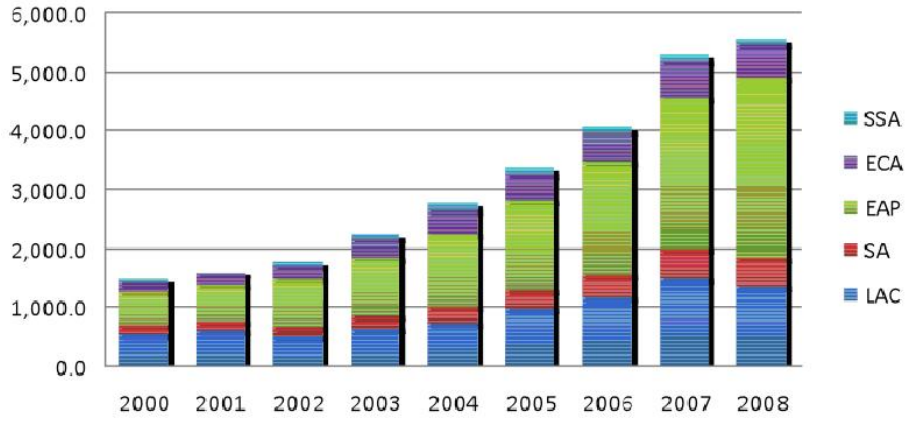


FIGURE 6.9 – Valorisation des monnaies locales par région (en millions de dollars)
Légende : EAP : East Asia, LAC : Latin America
ECA : Eastern Europe, SA : South Asia, SSA : Sub-Saharab Africa
source : Heiko Hesse, Ismail Dalla, voxeu.org, 2009

des activités et à dépenser localement.

Le Vénézuela a été plus loin en inscrivant le principe dans la loi et comptait plus de 5000 banques communautaires en 2011 (pour 100 au Brésil).

Mais ces monnaies parallèles aux monnaies fiats [18] sont le plus souvent en dehors des systèmes de taxations sur les biens, TVA, et sur le travail. Elles peuvent donc avoir un impact négatif si elles deviennent trop importantes et détruisent des activités économiques existantes.

On voit donc que la création de monnaies complémentaires n'est pas une nouveauté et qu'elles sont déjà largement intégrées dans nos sociétés. Aussi il n'est pas si surprenant de voir de telles monnaies apparaître sur Internet sans être directement contrées par les gouvernements [19].

6.6 Création de monnaies sur Internet

Pour créer du liquide sur Internet, une solution naturelle consiste à avoir des pièces numériques que les utilisateurs puissent s'échanger. Il est bien sûr nécessaire de respecter toutes les qualités demandées à une monnaie de micro-paiement (l'anonymat par exemple). Une autre solution consiste à utiliser la cryptographie pour effectuer des virements rendus publics pour vérification mais brouillés, là encore pour protéger l'anonymat.

Dans tous les cas la cryptographie est utilisée pour garantir au propriétaire de garder le contrôle de son argent et pour protéger son anonymat. Elle doit aussi prévenir

— la création de fausses pièces,

18. Une monnaie fiat est une monnaie contrôlée par un État.
19. Pour plus d'information sur les monnaies complémentaires, on pourra lire le rapport de Jean-Michel Cornu : http://www.club-jade.fr/images/jean-michel-cornu-l-innovation-monetaire.pdf

— la copie des pièces,
— l'espionnage des transactions d'un client par sa banque ou des tiers.

6.6.1 DigiCash (1993–2002)

La technologie de l'eCash a été mise au point dès 1993 par David Chaum au sein de sa société DigiCash. Cette monnaie a été mise en production par différentes banques mais elle n'a jamais pris. En Europe, la Deutsche Bank a fait une tentative en 2000.

Tout commence par la création des pièces. Il s'agit de créer de véritables pièces sans que la banque puisse savoir à qui elles appartiennent.

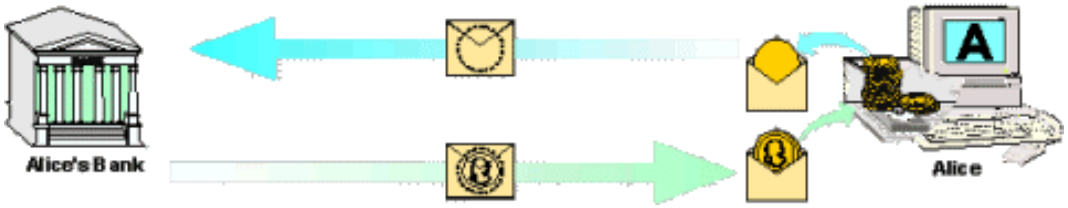


FIGURE 6.10 – Créations "anonyme" de pièces eCash

Pour cela Alice crée une pièce vierge avec un numéro de pièce unique qu'elle cache dans une enveloppe avant de l'envoyer à sa banque en lui demandant de donner à cette pièce une valeur déterminée. La banque débite la valeur désirée du compte d'Alice, marque la pièce de cette valeur sans ouvrir l'enveloppe. Elle renvoie le tout à Alice qui extrait la pièce marquée et la range dans son ordinateur.

Bien sûr la pièce, l'enveloppe et le marquage de la banque sont des images qui représentent l'identifiant numérique généré par Alice et l'opération de cryptographie qui brouille l'identifiant et celle de la banque qui valide l'identifiant brouillé.

Lorsqu'Alice veut payer Bob, elle lui envoie les pièces qui font le montant demandé.

FIGURE 6.11 – Alice donne des pièce à Bob qui les vérifie auprès de la banque d'Alice

Bob fait alors suivre les pièces à la banque d'Alice, laquelle vérifie qu'il s'agit de pièces qu'elle a validées (la banque ne peut pas savoir qu'il s'agit de pièces d'Alice). Elle vérifiera aussi que les pièces n'ont pas déjà été utilisées.

Finalement, Bob peut demander à la banque d'Alice des pièces neuves de la même somme ou demander un virement sur son compte.

Parmi les points faibles de cette méthode, notons la difficulté d'avoir l'appoint (sauf à avoir des millions de pièces d'un centime mais alors le coût de la transaction sera lourd) et l'obligation de devoir être connecté aux banques pour chaque transaction. Il est aussi probable que l'infrastructure du web 1.0 n'était pas adaptée à la diffusion d'une solution aussi lourde techniquement.

6.6.2 Le Bitcoin

Contrairement à l'eCash, les bitcoins sont simples à utiliser. Il n'y a pas de création de pièce pour l'utilisateur lambda donc pour en avoir, il faut en recevoir. Verser de l'argent revient à lire un code QR le plus souvent. Il est aussi possible indiquer le numéro de compte du vendeur (appelée adresse) et la somme à verser. Vous pouvez faire cela depuis votre ordiphone ou ordinateur. Le destinataire verra la somme arriver sur son logiciel.

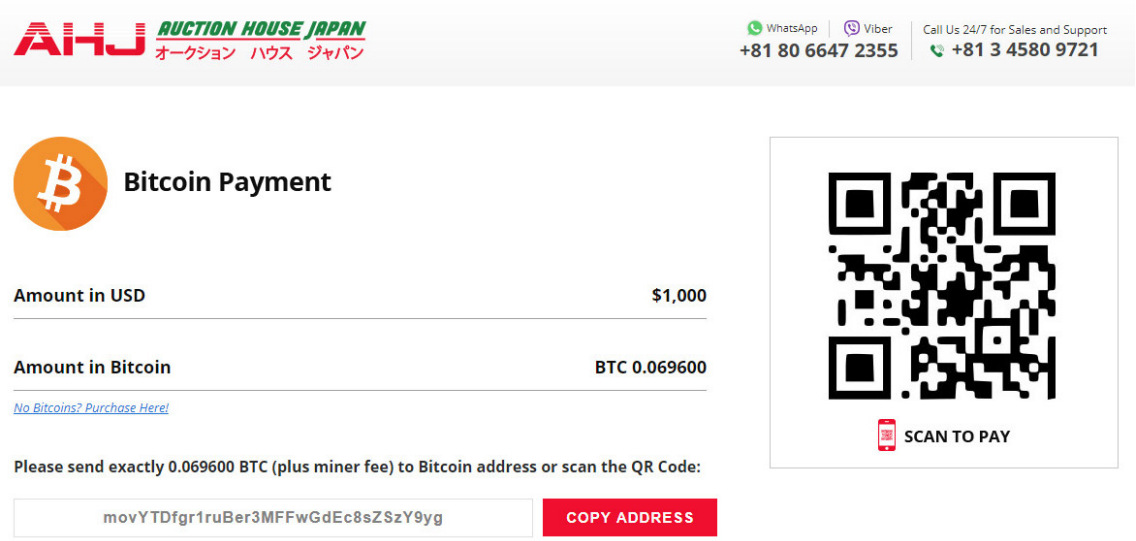


FIGURE 6.12 – Magasin qui présente la note en Bitcoin

Pour recevoir de l'argent, vous générez une adresse que vous transmettez. Vous pouvez générer autant d'adresse que vous le souhaitez, un par client, un par achat ou un seul pour tout. Cette adresse est écrite sur le grand livre de compte du Bitcoin [20] ainsi que la somme qui lui a été versée. Celui qui contrôle cette adresse peut y prendre l'argent pour le verser à une autre adresse.

Comme on a vu, il est également possible de générer un code QR qui comprend toutes ces informations.

20. Ce grand livre de compte que chacun peut recopier localement (attention, ce livre fait 300 gigaoctets en 2020) s'appelle la *blockchain* pour des raisons qu'on verra dans la partie technique ci-dessous.

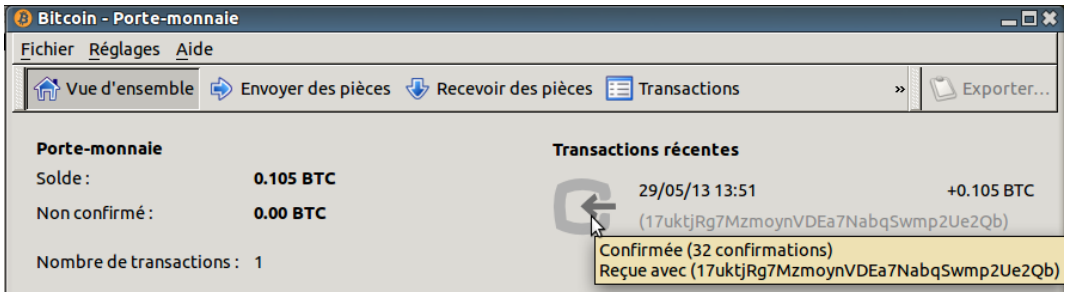


FIGURE 6.13 – Réception de premiers bitcoins dans ce (vieux) porte-monnaie
L'adresse 17uktjR... a été généré par ce porte-monnaie et transmis au payeur

Mise en œuvre

Installer une application qui permet de manipuler ses bitcoins sur son ordinateur peut être stressant pour certains, surtout lorsque les sommes sont importantes. Il faut savoir que si on perd le mot de passe associé à son compte, on perd ses bitcoins sans possibilité de les récupérer (c'est déjà arrivé plusieurs fois). Aussi pour certain il peut être préférable d'utiliser une plateforme d'échange qui ressemble à une banque [21]. C'est la solution la plus simple Lorsqu'on désire acheter des crypto-monnaies avec des euros.

— Binance est la plus grande plateforme de crypto-monnaie en terme de volume, elle propose des centaines de cypto-monnaies. Attention, elle a eu régulièrement des problèmes avec les autorités de différents pays et devrait quitter certains pays européen en 2023 [22].
— Coinbase est une entreprise américaine créée en 2012 pour les crypto-monnaies. Elle est en seconde position en terme de volumes échangé.
— eToro est une ancienne plateforme israélienne de finance qui a pris le virage des crypto-monnaies dans les années 2010. Elle est plus chère et moins populaire que Binance mais mieux intégrée dans le système financier des États,
— de très nombreuses autres plateformes existent, ainsi que des comparateurs.

Binance France et eToro sont enregistrées auprès de l'autorité des marchés financiers en tant que prestataires de services en actifs numériques, PSAN [23].

Il est possible d'avoir un compte sur une telle plateforme d'échange pour acheter et vendre des bitcoins puis de les rapatrier sur sa machine une fois la transaction faite. Cela a un coût mais vous êtes protégé contre une mésaventure qui pourrait arriver à la plateforme.

Pour suivre les transactions, pour visualiser le marché des crypto-monnaies, il existe des sites dédiés :

— CoinMarketCap permet de comparer les monnaies et d'avoir une description précise de

21. Comme une banque, une plateforme d'échange peut se faire voler ou disparaitre avec la caisse, c'est déjà arrivé.
22. https://www.cointribune.com/crypto-bientot-la-fin-de-binance-en-europe/
23. L'explication de ce status et la liste des plateformes enrgistrées sont ici : https://www.amf-france.org/fr/espace-professionnels/fintech/mes-relations-avec-lamf/obtenir-un-enregistrement-un-agrement-psan

chacune.
— Blockchain ou BlockChair permettent d'explorer la *blockchain* et de tracer les échanges.

Pour gérer ses bitcoins en local, il existe de nombreuses applications qui sont présentées dans la section choisir son porte-monnaie du site bitcoin.org. Pour une sécurité renforcée, il est possible d'utiliser un coffre fort physique à savoir une clef usb qui intègre de la cryptographie et garde votre clef privée au sûr. Parmi les plus connues citons les clefs de Ledger ou de Trezor.

Techniquement

La complexité du Bitcoins est cachée dans la mécanique. Là encore on utilise la cryptographie massivement mais celle à base de courbes elliptiques et non celle présentée dans le premier chapitre qui s'appuie sur les nombres premiers. Sans entrer dans le domaine des courbes elliptiques, regardons comment le Bitcoin fonctionne.

Le principe fondamental est un livre de compte dans lequel on écrit tous les transferts. La notion de pièce n'est pas présente. Si j'ai reçu un transfert de 1 bitcoin (transaction A, ancienne) et que je dépense 0,2 bitcoins, alors tout le monde doit pouvoir voir que ces 0,2 bitcoins proviennent du bitcoin que j'avais reçu. On s'appuie sur les transactions passées pour permettre les nouvelles.

L'émetteur signe ses paiements avec sa clef privée afin de pouvoir utiliser ses bitcoins. Il utilise la clef publique de son destinataire pour déposer la somme afin que ce dernier soit le seul à pouvoir la revendiquer (avec sa clef privée). En pratique la clef publique du destinataire est intégrée dans l'adresse de transaction.

Ainsi cela donne pour une transaction C (Courante) :

— `entrée` : l'adresse de la transaction A de 1 btc (bitcoin) que l'émetteur avait reçu
— `sortie 1` : l'adresse donnée par le destinataire et la somme de 0,2 btc
— `sortie 2` : l'adresse de l'entrée et la somme de 0,8 btc (il se donne ce qui reste)

L'émetteur signe le tout avec sa clef privée et voilà. Sa signature est obligatoire car la transaction A de 1 btc était signée avec sa clef publique.

Après la transaction C, la transaction A n'est plus utilisable car elle a un fils.

Dans le cas où on ne dispose pas d'une transaction précédente avec assez d'argent, il est possible de combiner plusieurs transactions reçues afin d'atteindre le montant voulu. La transaction décrite ci-dessus aurait alors eu plusieurs entrées.

Double dépense Afin que je ne puisse pas utiliser une seconde fois la transaction A pour payer quelqu'un d'autre, la transaction C est incorporée dans un bloc de transactions (lequel regroupe toutes les transactions des 10 dernières minutes en moyenne, cf Blockchain.info).

Lorsque ce bloc est publié, tout le monde est au courant de la transaction C, y compris le destinataire qui, alors, se considère payé. Bien sûr aucune autre transaction avec la transaction

A en entrée sera acceptée. Si durant la création du bloc j'avais utilisé 2 fois la transaction A, alors une seule des 2 transactions aurait été acceptée et seul un destinataire aurait pu voir qu'il a été payé.

La force du Bitcoin est que les blocs sont créés par tout le monde en résolvant un problème mathématique difficile, mais simple à vérifier lorsqu'on a la solution. Ainsi lorsqu'une personne indique qu'elle a la solution dans son bloc, les autres peuvent valider cette solution et tout le monde passe à la création du bloc suivant. Chaque bloc est lié à sont précédant ce qui crée une chaine de blocs, cf encart page 216.

Annuler la transaction Une autre façon de tricher est de créer un bloc menteur qui ne comprend plus la transaction C pour remplacer le bloc qui la comprenait. Ainsi le destinataire a cru être payé, et donc a livré l'achat, mais finalement son argent disparaît et comme la transaction A n'a plus de fils, le payeur récupère l'argent. Pour éviter cela, on considère que seule la plus longue chaine de blocs est la bonne. Aussi si je crée un bloc menteur pour remplacer le bon bloc, il va aussi falloir que je recrée tous les blocs suivant créés depuis. Or la construction d'un bloc est difficile à cause des problème mathématiques à résoudre et pour faire la chaîne de bloc la plus longue je dois aller plus vite que tous les autres mineurs réunis.

Faiblesses du système

Les créateurs de blocs, les mineurs, sont récompensés par 6,25 bitcoins par bloc créé [24] plus un pourcentage sur les transactions enregistrées [25]. Avec le temps, la récompense fixe baisse afin de ne pas créer trop de monnaie et le pourcentage augmente. Ce système motive les mineurs et fournit la puissance de calcul nécessaire au bon fonctionnement général.

Ce système génère des problèmes :

— plus la valeur du bitcoin est élevée, plus il est intéressant de miner, ce qui garantit la sécurité mais ce qui génère une consommation électrique démesurée comme on le verra.
— plus il y a de transactions, et plus les frais de transactions augmentent puisque les mineurs choisiront d'intégrer dans leur bloc les transactions les plus rémunératrices. Ainsi le prix moyen à payer pour que sa transaction soit intégrée devient bien trop important pour des micro-paiments (le prix varie de quelques dollars à quelques dizaines de dollars, cf figure 6.14).
— plus il y a de transaction et plus on doit attendre pour que sa transaction passe (problème de passage à l'échelle).

Lightning Network Pour répondre à ces problèmes, le *Lightning Network* et été crée. Il s'agit d'un réseau de niveau 2 qui se rattache de temps en temps à la chaîne du Bitcoin. Il permet

24. après la division par 2 de la récompense en mai 2020. Des divisions par 2 sont prévues tous les 4 ans par le protocole.
25. le pourcentage est choisi par le payeur mais plus il est important, plus les mineurs ont envie d'inclure la transaction dans leur bloc

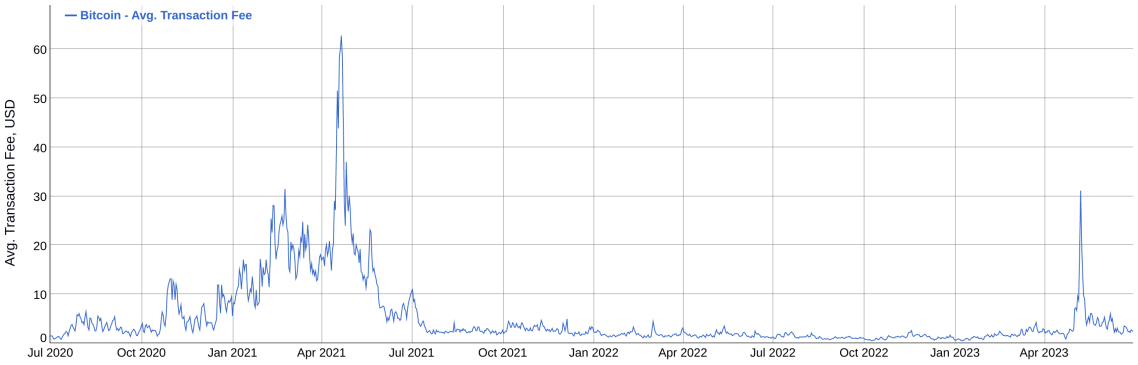


FIGURE 6.14 – Frais moyens pour une transaction en bitcoins

des paiements très rapides (en dessous de la minute voire de la seconde) et des frais de transaction très faibles (0,003 % soit 1000 fois moins cher que Visa). De plus il résout le problème de passage à l'échelle en permettant des billions de transaction par seconde. On a donc une solution miracle qui a néanmoins un coût : une perte de sécurité par rapport au Bitcoin.

Ce réseau est intéressant seulement pour effectuer un nombre significatif de paiements afin d'amortir les frais de transaction liés au dépôt et au retrait de bitcoins sur ce réseau (transactions écrites sur la chaîne du Bitcoin).

Voici comment fonctionne le *Lightning Network* :

- on ouvre un canal avec une autre personne
- pour chaque canal (entre 2 personnes) :
  - chacun dépose une somme de bitcoin prise sur la chaîne du Bitcoin
  - on choisit la durée et nombre d'échanges possible, éventuellement infinis.
  - lorsqu'on ferme le canal, on écrit la balance sur la chaîne du Bitcoin.
- payer revient à modifier la valeur de chacun dans le canal (cela ne génère pas de trace sur la chaîne du Bitcoin d'où la perte de sécurité mais aussi la possibilité de frais très faibles).

L'astuce est qu'on peut rebondir de personne en personnes pour payer son destinataire. Ainsi il est possible d'échanger avec tous les membres du réseau. Chaque personne intermédiaire (nœud du réseau) prend au passage une petite commission. Aussi il est intéressant d'être un nœud central. C'est ce que font certains services qui offrent une application pour payer sur le *Lightning Network* en créant initialement une connexion, entre l'utilisateur et leur nœud [26].

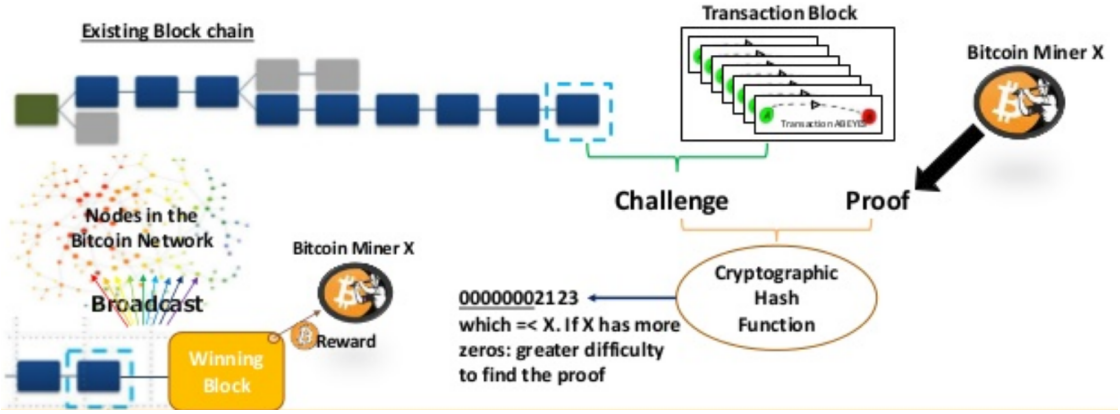
Notons qu'il est possible d'ouvrir soit même plusieurs canaux, en particulier si on a plusieurs partenaires avec lesquels on a des échanges commerciaux. L'application BitBanana offre un contrôle total sur ses connexions et donc permet cela.

26. C'est le cas de Breez ou de Phoenix.

La *blockchain*

La blockchain est souvent considérée comme la merveille de l'article de Satoshi Nakamoto qui présente le bitcoin [a].

L'idée de base est d'avoir un livre ouvert où on (les mineurs) écrit les pages (blocs) à la suite, chaque page étant liée de façon incassable à la précédente. La seule façon de casser le système est de repartir d'une ancienne page et de créer plus de nouvelles pages que le livre en a actuellement car le livre de compte de référence est celui qui a le plus de pages. Sachant qu'il y a vraiment beaucoup de personnes (ordinateurs) qui écrivent le livre, il faut être plus rapide que tous les autres réunis. A priori c'est impossible [b]. On a donc un système sans contrôleur qui garantit que personne ne triche en imposant au tricheur potentiel d'avoir une puissance de calcul supérieure à celle de toute la communauté (on appelle cela la preuve de travail ou *proof of work*).



En pratique, un mineur va prendre un groupe de transactions dans la file d'attente publique des transactions (il peut choisir celles qui paient le plus pour être validées). Il les range dans un bloc, le *Transaction Block*, avec le condensat du dernier bloc validé. Maintenant il faut qu'il trouve un nombre, *Proof*, qui combiné à ce bloc sera passé à une fonction dont le résultat doit commencer par X zéros. Pour trouver ce nombre *Proof* le mineur en essaie plein jusqu'à ce que ça marche. Il n'y a pas d'autres façons de faire. C'est cela qui est gourmand en puissance de calcul.

Une fois le nombre *Proof* trouvé, le mineur annonce publiquement son résultat qui est validé par les autres mineurs [c] et ainsi le nouveau bloc est ajouté à la *blockchain*. Si le temps nécessaire pour valider le bloc avec son nombre *Proof* a été inférieur a 10 minutes, on augmente X afin que le calcul soit plus long la prochaine fois, sinon on diminue X.

Ce mécanisme de la *blockchain* peut être appliqué à d'autres cas à tel point qu'une économie se construit sur les applications possibles de la *blockchain* (pour les notaires par exemple).

Pour plus de détails, voir Blockchain 101 - A Visual Demo.

a. https://bitcoin.org/bitcoin.pdf

b. Avec le système de regroupement de mineurs pour se distribuer les récompenses, on pourrait imaginer que cela arrive, mais cela devrait se voir.

c. Exécuter une fois la fonction est rapide, c'est le faire des milliards de fois pour trouver le bon nombre qui prend du temps.

Moralement

La grande force du Bitcoin est qu'il n'appartient à personne, donc à tout le monde. Le Bitcoin est une monnaie décentralisée. Il n'y a pas d'entreprise ou de banque derrière le Bitcoin ni même d'État. Le réseau Bitcoin est géré par tous les serveurs qui collaborent, ces derniers étant rémunérés pour cela à un prix prédéterminé par de la création de monnaie.

Une autre force du Bitcoin est qu'il s'agit d'un logiciel libre. Cela implique que la sécurité du système peut être analysée par n'importe qui et surtout que tout le monde peut développer des applications liées au Bitcoin. Ainsi on trouve de nombreuses applications pour ordinateurs et ordiphones mais aussi des applications au monde physique (il existe des pièces physiques Bitcoin).

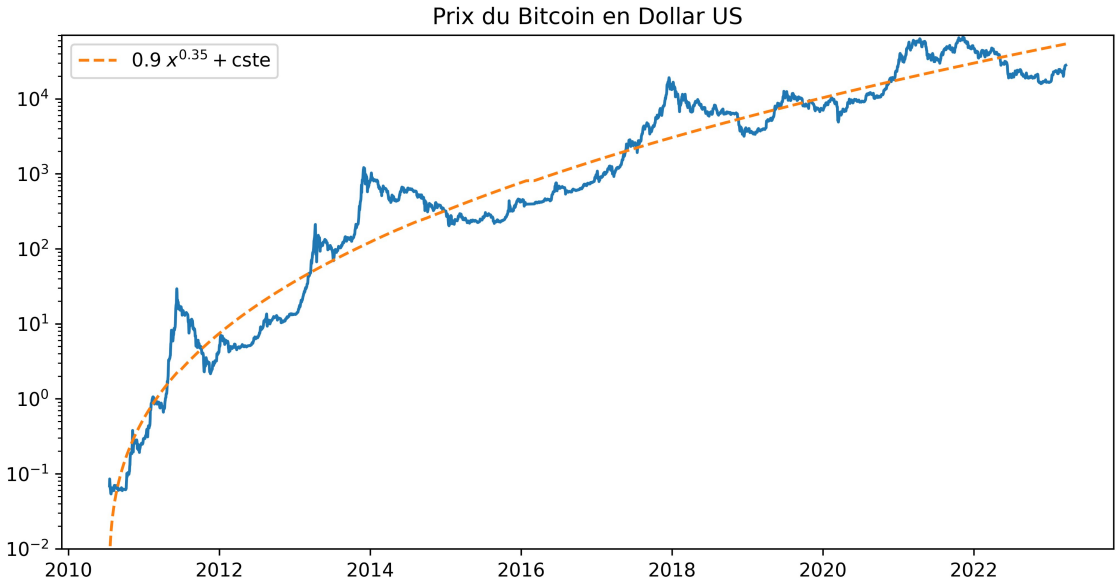


FIGURE 6.15 – Bitcoin par rapport au dollars depuis 2010

Notons enfin que la valeur du Bitcoin est celle du marché de l'offre et de la demande. Actuellement cette valeur est hautement volatile aussi il est déconseillé d'y investir plus que ce que l'on peut se permettre de perdre. On peut néanmoins constater qu'elle progresse régulièrement à long terme, cf figure 6.15, et penser qu'elle se stabilisera avec le temps.

D'ici là, sa popularité grandissante et certains événements géopolitiques ou simplement techniques en font régulièrement exploser le cours. La valorisation du Bitcoin a ainsi dépassé les 600 milliards de dollars en 2021 ce qui est 100 fois plus que l'ensemble monnaies complémentaire non étatiques en 2008, cf figure 6.9. À titre de comparaison, le dollars US, qui a la plus grosse masse monétaire du monde, pèse 1 800 milliards en 2019 [27].

Une des raisons de l'augmentation des cours est la limitation du nombre de bitcoins, nombre limité à 21 millions de par son protocole. Aussi la seule façon de répondre à la demande est d'augmenter la valeur du Bitcoin puisqu'il n'est pas possible d'émettre plus de bitcoins. Cet

27. https://www.federalreserve.gov/paymentsystems/coin_data.htm

aspect peut pousser certains à conserver leurs bitcoins en attendant que sa valeur monte, ce qui raréfie l'offre et donc pousse à la hausse. On peut donc y voir un placement spéculatif plutôt qu'une monnaie, surtout que le nombre de magasins acceptant les bitcoins reste limité.

Tous ces points rendent possible une intervention des États, ce qui aurait évidemment un impact sur le cours du Bitcoin. En août 2013 l'Allemagne a reconnu le Bitcoin comme une monnaie de transaction légale alors qu'en juillet la Thaïlande l'interdisait. En mars 2014 le fisc des États-Unis a déclaré que les bitcoins sont un bien et non une monnaie, et, en tant que tel, sont imposables sur les plus values. L'approche de la BCE est équivalente, le Bitcoin est un placement et non pas une monnaie [28].

Autre aspect moral concerne l'impact écologique du Bitcoin. La validation des transactions demande la résolution de problèmes mathématiques dont la difficulté croît avec la puissance de calcul mise en œuvre pour les résoudre. Cela implique un coût énergétique croissant avec le succès du Bitcoin et/ou le renouvellement des serveurs. Le fait que la difficulté soit liée à la puissance de calcul devrait mener à un équilibre puisqu'à partir d'un moment la part de gâteau pour chacun sera trop petite pour être rentable. Cela étant cet équilibre ne semble pas encore atteint comme le montre la courbe 6.16.

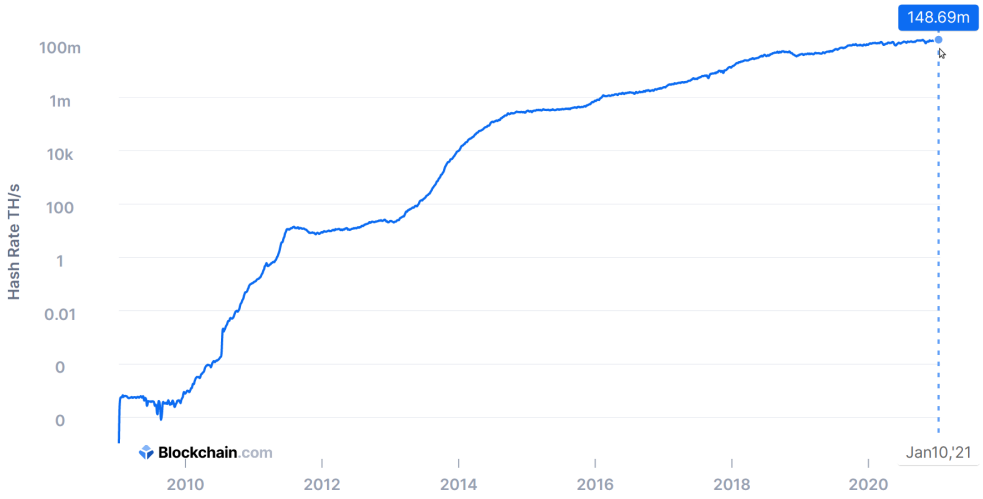


FIGURE 6.16 – Évolution de la puissance de calcul des serveurs Bitcoin

Cette puissance nécessaire pour faire fonctionner le système a donné lieu à de nombreux articles sur le gaspillage énergétique du Bitcoin. Le calcul de la consommation électrique liée au Bitcoin est délicat. S'il est possible de mesurer le nombre de cycles d'horloges il est difficile de connaître la consommation électrique, tous les ordinateurs n'ayant pas la même efficacité pouvant aller de 0,001 W-s par giga hash/s (GH/s) pour du hardware spécialisé à 19 W par GH pour un classique Raspberry Pi (chiffres de 2013). Une machine spécialisée la plus classique est l'ASIC que de nombreux mineurs utilisent. La version 2015 consomme 0,2 w/GH. Aussi une autre façon de calculer est d'évaluer le modèle financier des mineurs.

Fin novembre 2017, le gain journalier pour les mineurs est d'environ 20 millions de dollars.

28. Pour plus d'information sur la légalité du Bitcoin suivant les pays : https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory

Cela permet de consommer beaucoup d'électricité tout en dégageant des bénéfices. Pour avoir un ordre de grandeur, 1 MW.an coûte environ 1 million de dollars en consommation de base. Certains annoncent que les mineurs dépensent 60% de leurs revenus en électricité ce qui permet au rythme d'aujourd'hui de dépenser 12 millions par jours soit 4,4 G$ par an donc 4,4 GW.an ou 38,5 TWh, soit presque la consommation annuelle de la Hongrie (40 TWh d'après le rapport 2017 de l'IEA).

Le site dédié de Cambridge qui affiche arrive à des chiffres similaires [29] et annonce une consommation annuelle de 130 TWh à la mi-2023 (les Pays-Bas consomment 110 TWh / an).

Il y a donc un véritable problème écologique qui n'existe que pour garantir que personne ne puisse fausser les transactions et non pas pour réaliser les transactions. D'autres crypto-monnaies basées sur d'autres systèmes de validation des transactions qui n'ont pas ce problème.

6.6.3 L'Éthereum

Dans le monde des crypto-monnaies, la plus importante après le Bitcoin est l'Éther, la monnaie du réseau Éthereum.

La technologie Éthereum se base sur un ordinateur virtuel, l'EVM [30], qui permet d'exécuter des contrats dit intelligents, *smart contract*, écrits en langage informatique. Ces contrats sont la grande idée de l'Éthereum. Il s'agit de contrats financiers, ou ayant un aspect financier, qui s'appuient sur la monnaie de l'Éthereum. On peut citer comme exemple de contrat une enchère qui remettra automatiquement la plus haute enchère au vendeur, une caution qui rend l'argent si les termes du contrat sont respectés, un ticket d'entrée qui donne le code dès qu'il reçoit l'argent etc. Les possibilités sont infinies. Pour garantir le bon fonctionnement des contrats, ils sont écrits dans la *blockchain* d'Éthereum sans possibilité de les modifier. L'ordinateur virtuel d'Étherum exécute les contrats tout comme les mineurs du Bitcoin enregistrent les transactions. Ainsi il n'est plus nécessaire d'avoir des tiers de confiances (avocat, banque, intermédiaire...) puisqu'on a un système automatique inviolable.

Mais s'il est possible d'exécuter du code sur l'infrastructure d'Éthereum, pourquoi se limiter à des contrats financiers et pourquoi ne pas exécuter de véritables programmes informatiques, des jeux par exemple ? C'est possible mais avec deux limites :

— Le code d'un contrat est exécuté sur l'EVM qui est une machine très lente car fortement redondante (pour des raisons de sécurité). Éthereum annonce que l'EVM est 1 million de fois plus lente que sur une machine classique. Le stockage aussi coûte cher.
— Une erreur de programmation dans un contrat peut coûter une fortune, le code est visible et les pirates adorent exploiter les erreurs dans les contrats [31].

Aussi il existe les *dapps* ou *decentralized applications* qui mettent le début de leur programme (ou l'API) dans la chaîne d'Éthereum avec un lien vers le cœur du programme qui tourne sur

29. Cambridge Bitcoin Electricity Consumption Index : https://ccaf.io/cbeci/
30. L'*Ethereum Virtual Machine*
31. cf cette liste de failles : https://ventral.digital/posts/2022/12/15/ethereum-smart-contract-auditors-2022-rewind

un serveur quelque part sur Internet. Ainsi les frais d'exécution sont limité au lancement du programme et une erreur dans le programme n'a d'impact que sur le serveur, ce qui peut être corrigé facilement. Il en est de même pour les données, une *dapps* peut choisir de stocker ses données sur son serveurs et certaines données importantes dans la chaîne, ce qui mène aux fameux NFT dont on parlera.

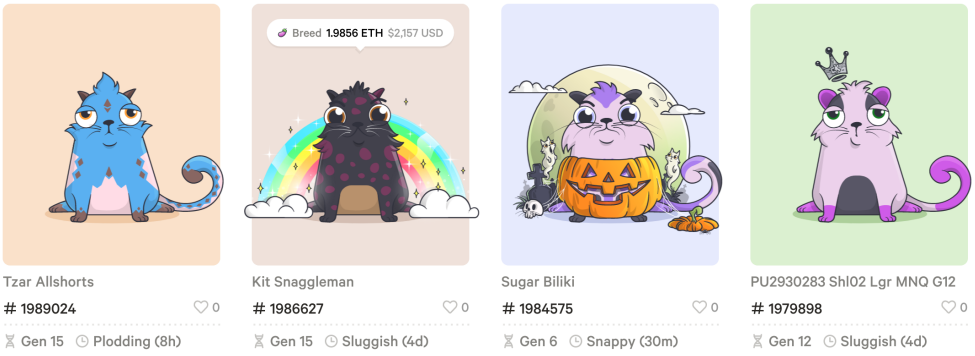


FIGURE 6.17 – CryptoKitties
Une *dapps* pour acheter et faire un élevage de chats.
L'ADN de chaque chat et son propriétaire sont stockés dans la chaîne.

En pratique les contrats sont exécutés lorsqu'ils sont intégrés au sein d'un bloc de la chaîne. Il est également possible d'indiquer qu'on désire exécuter un contrat déjà enregistré dans la chaîne. Par exemple on peut enchérir sur une enchère en donnant l'adresse du contrat et la somme qu'on propose. Cette action est elle-même un contrat, un contrat qui appelle un autre contrat (l'enchère).

Il est également possible de programmer des actions dans le futur en s'appuyant sur un contrat comme l'Ethereum Alarm Clock [32] qui déclanchera notre contrat à la date voulue [33].

Enfin, le contrat le plus simple est un versement d'Éther. L'Éther étant à la base des contrats financiers, il est devenu une monnaie d'échange voire de spéculation comme le Bitcoin. Il est aussi très volatile, comme le Bitcoin.

Comme tous les contrats n'ont pas la même taille ni la même complexité, est il logique que leur exécution sur l'EVM génère des calculs plus ou moins importants. Aussi chaque opération d'un contrat a un coût exprimé en gaz (cf l'encart sur le gaz page 222 pour plus de détails). On a donc deux coûts : celui pour que sa transaction soit prise, c.a.d. que son contrat soit lancé, et celui de l'exécution du contrat. Ces deux coûts sont fusionnés en un : le prix du gaz. Ainsi une personne qui veut lancer un contrat à 21 000 gaz (un versement en éther) indique qu'il est prêt à payer 30 nano-éther pour 1 gaz. Si ce prix est plus cher que le prix du marché, alors son contrat sera exécuté en priorité.

32. https://github.com/ethereum-alarm-clock/ethereum-alarm-clock
33. En octobre 2023 une faille a été découverte dans l'Ethereum Alarm Clock et elle n'a pas été corrigée depuis. Il est possible que Chrono Logic, l'entreprise qui avait développé ce système, soit morte.

Les contrats intelligents ou *smart contracts*

Ces petits programmes informatiques sont la réussite d'Éthereum. Inscrits dans la chaîne et exécuté sur l'EVM (*Éthereum Virtual Machine*), ils sont :

— transparents, tout le monde peut lire leur code
— immuables, il sont gravés dans la chaîne et ne peuvent être effacés ou modifiés → ils peuvent être réutilisés (appelés)
— déterministes
— de taille maximale de 24 kB (contournable)

Les contrats sont écrits dans des langages dédiés comme Solidity ou Vyper[a]. Voici un exemple de système d'enchère avec une limite temporelle :

Solidity

```
pragma solidity ^0.4.25;

contract OpenAuction {

    address public beneficiary;
    uint public auctionStart;
    uint public auctionStop;
    bool public ended;
    uint public highestBid;
    address public highestBidder;

    constructor (address _beneficiary, uint _biddingTime) public {
        beneficiary = _beneficiary;
        auctionStart = now;
        auctionStop = auctionStart + _biddingTime;
    }

    function bid() public payable {
        assert(now < auctionStop);
        assert(msg.value > highestBid);
        if (highestBid != 0) {
            highestBidder.transfer(highestBid);
        }
        highestBid = msg.value;
        highestBidder = msg.sender;
    }

    function endAuction() public {
        assert(now >= auctionStop);
        assert(!ended);
        ended = true;
        beneficiary.transfer(highestBid);
    }

}
```

Vyper

```
# Open Auction contract

beneficiary: public(address)
auctionStart: public(timestamp)
auctionStop: public(timestamp)
highestBid: public(wei_value)
highestBidder: public(address)
ended: public(bool)

# constructor
@public
def __init__(_beneficiary: address, _bidding_time: timedelta):
    self.beneficiary = _beneficiary
    self.auctionStart = block.timestamp
    self.auctionStop = self.auctionStart + _bidding_time

# create function for bidding
@public
@payable
def bid():
    assert block.timestamp < self.auctionStop
    assert msg.value > self.highestBid
    if not self.highestBid == 0:
        send(self.highestBidder, self.highestBid)
    self.highestBid = msg.value
    self.highestBidder = msg.sender

# end auction and send the highest bid to the beneficiary
@public
def endAuction():
    assert block.timestamp >= self.auctionStop
    assert not self.ended
    self.ended = True
    send(self.beneficiary, self.highestBid)
```

La partie violette déclare les variables que l'on pourra consulter et qui donne l'état de l'enchère, en jaune le constructeur puis les fonctions en vert. Ce code est ensuite compilé pour donner deux parties :

— une description lisible pour utiliser le service, l'ABI ou *Application Binary Interface*
— le code, bytecode, qui sera exécuté sur l'EVM.

Il ne reste plus qu'à les déployer, payer le coût en gaz et c'est parti, chacun peut faire des enchères.

a. Solidity est le langage initial des contrats, il est proche de JavaScript. Vyper, proche de Python, est arrivé par la suite avec une volonté de réduire le risque de produire du code avec une faille de sécurité.

Du Gaz dans l'Éther

Pour faire exécuter un contrat dans l'Éthereum, il faut payer les mineurs dont les ordinateurs vont effectuer les calculs. Le prix est défini en Gaz avec un prix fixe pour différentes opérations. Le prix du Gaz s'exprime en GWei c.a.d. 10^9 Wei, un Wei étant la plus petite unité de l'Éther à savoir 10^{-18} ETH.

Opération	Prix en Gaz
une addition	3
une multiplication	5
une comparaison	3
état d'un compte	700
charger un *mot* de la mémoire	800
sauver un *mot* en mémoire	20 000
transférer des ETH	21 000

TABLE 6.2 – Exemples de prix des opérations sur l'Éthereum

Le cours du Gaz est variable et suit l'offre et la demande. Si vous désirez que votre contrat s'effectue rapidement, vous indiquez que vous êtes prêt a payer cher le Gaz, à l'inverse s'il n'y a pas urgence, vous pouvez payer moins cher (cf https://etherscan.io/gastracker pour le prix courant à payer suivant l'urgence). Début 2021 le prix du Gaz est cher, il a décuplé en 2020 pour atteindre 100 GWei ce qui fait le Gaz à 0,01 centime d'euro avec un éther à 1000 €. Un transfert d'éther coûte donc 2,1 € en janvier 2021. Été 2023, le prix du gaz est à 33 GWei et le cours à 1700 €, donc le transfert d'éther est à 1,2 €. Dans les deux cas, c'est bien trop cher pour les micro-paiements.

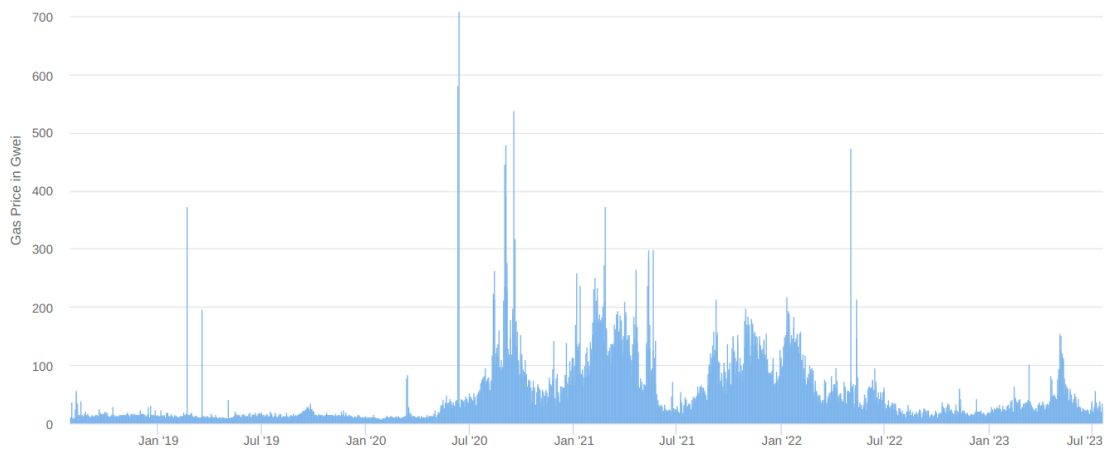


FIGURE 6.18 – Prix moyen du Gaz
source : Etherscan

La finance dématérialisée – DeFi

Comme on l'a vu la force de l'Éthéreum est ses contrats intelligents qui permettent de programmer des opérations financières (entre autres). Aussi un nouveau type de finance s'est développé en dehors des banques, salles de marché et autre entités financières. Il a néanmoins ses propres acteurs et une infrastructure complexe que ce schéma résume :

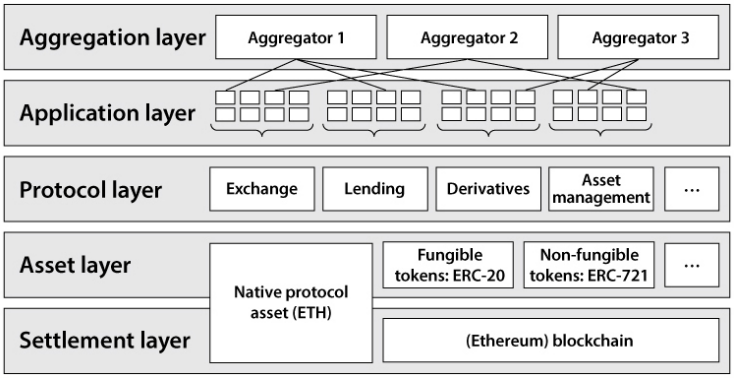


FIGURE 6.19 – Schéma en couches de la DeFi
auteur : Fabian Schär

La base est la chaîne Éthereum. Ce n'est pas une obligation mais de fait c'est la chaîne la plus utilisée. Vient ensuite la couche des biens avec le jetons fongible ou pas. Puis les protocoles présentent en filigrame les contrats. Au dessus on trouve les applications web ou sur ordiphones qui utilisent ces contrats. Enfin les aggrégateurs fusionnent plusieurs services de base en services financiers complets.

Au niveau des biens on trouve deux normes fondamentales. L'ERC-20 est à la base de milliers de jetons de toutes sortes. Il y a des jetons qui sont d'autres crypto-monnaies, d'autres sont des jetons de votes, des jetons de jeux, de lotteries... En juillet 2023, on recense [34]

— 12 jetons ERC20 dont la masse monétaire > 1 G$
— 96 jetons ERC20 dont la masse monétaire > 1 M$

Le jeton ERC-721 plus connu sous le nom de NTF, *Non Fungible Token*, est la références pour enregistrer les œuvres numériques. Parmi les plus célèbres, citons les cryptopunks et les *Bored Apes* qui représentent de petites images qu'on peut utiliser comme avatar. Chacune vaut des dizaines voire des centaines de milliers d'euros en 2023. On peut en acheter sur OpenSea, une des plateformes d'enchère pour les NFT.

Au niveau supérieur, voici quelques exemples de contrats financiers :

— La monnaie stable (*stable coins*) peut utiliser des contrats pour garantir la parité avec une autre monnaie (souvent le $).
— Le contrat permettant d'emprunter des euros en mettant en caution une crypto-monnaie.
— Le contrat gardien qui redistribue l'argent entre les parties que si elles sont d'accord sur la répartition.

34. https://www.coinlore.com/token-types/erc20

Les monnaies stables Les *stable coins* joue de rôle de stabilisateur afin de pouvoir faire de la finance dématérialisée sans les risques liés à la variabilité des crypto-monnaies. Leur rôle est donc très important.

La mécanique qui permet de lié un jeton à une monnaie fiat comme le dollar, peut être basée sur une crypto-monnaie de référence ou une monnaie fiat. Dans le premier cas la technique consiste à demander une caution de la crypto-monnaie de référence nettement supérieure à la somme considérée afin de pouvoir vendre la crypto-monnaie si elle baisse trop et récupérer la somme considérée. Le second cas est plus simple, puisqu'en cas de vente du jeton stable, on prend l'équivalent dans les stocks de monnaie fiat (sauf si l'émetteur du jeton a émis plus qu'il n'a de réserves...). Ainsi on a parmi ces monnaies stables :

- jeton avec caution dans la chaîne (la crypto-monnaie de réféence) :
  - le DAI est cautionné en ETH (1 DAI = 1 $ avec une caution = 150 % de la somme désirée en DAI)
  - le WBTC est cautionné en bitcoin (1 WBTC = 1 btc)
- jeton avec caution hors chaîne :
  - les USDT et USDC sont cautionné en $ dans une banque (1 USDx = 1 $)
  - le PAXG est cautionnés en or (1 PAXG = 1 once d'or)

La somme des cautions, pour les monnaies stables mais aussi pour d'autres opérations, est une façon de mesurer l'activité de la DeFi :

FIGURE 6.20 – Total des sommes en caution de la DeFi et valorisation des monnaies stables
source : DEfiLlama

Le crash de mars 2022 est lié à la chute de la chaîne Terra et de ses monnaies Luna et UST. UST était une monnaie stable arrimée au dollar et Luna était sa crypto-monnaie de référence (caution). La mécanique était qu'on pouvait toujours échanger x Luna pour leur valeur en UST et inversement. Aussi si l'UST baisse à 0,99 $, on peut acheter 100 UST pour 99 $, puis avec on achète x Luna que l'on revend pour 100 $ et on gagne 1 $. Le fait d'avoir acheter des UST fait remonter son cours.

En mai 2022, la monnaie stable UST a décroché suite à des ventes importantes et plutôt que d'en profiter comme on vient de voir, les investisseurs ont eu peur ce qui a entrainé une panique qui a fait chuter Luna de 80 $ à 0,01 cents, ce qui achevé l'UST qui s'est totalement effondré. Sachant que l'UST était une monnaie stable majeure, le total de sommes en caution dans la DeFi a été divisé par deux.

En 2023, la DeFi ne s'est pas remise de ce crash et la question de la confiance qu'on peut avoir en des monnaies stables basées sur des crypto-monnaies est toujours d'actualité (notons que le DAI qui a un fonctionnement différent n'a pas bougé, y compris durant cette crise).

Reconstruire Wall Street

La DeFi a besoin de certaines infrastructures financières de la TradFi [35].

Les plateformes d'échange Étant donné le nombre de crypto-monnaies et d'autres actifs, il est important de pouvoir les échanger sans devoir repasser par des dollars ou des euros à chaque fois. Aussi il existe des plateformes d'échanges centralisées, un site web usuel où on achète ses crypto-monnaies et où on peut passer d'une crypto à un autre, et des plateformes d'échange décentralisées qui utilisent des contrats pour échanger des cryptos. La force des premières est leur simplicité d'accès, leur faiblesse est que si elles meurent, leurs clients perdent leurs avoirs.

Les DEX [36] à l'inverse ne possèdent pas les avoir des échanges, par contre elles disposent de réserves qui permettent justement d'effectuer ces échanges. Un des fonctionnements des DEX est d'avoir une cagnotte avec 2 monnaies qui s'équilibre automatiquement en liant les cours aux réserves :

Soit x et y les reserves des 2 monnaies. On veut avoir toujours $x\,y = k$ avec k une constante. Donc si je donne Δx alors je reçois en échange Δy ainsi calculé :

$$(x + \Delta x)\,(y - \Delta y) = k \quad \Longrightarrow \quad \Delta y = y - \frac{k}{x + \Delta x}$$

Si je mets autant que la réserve de la première monnaie, $\Delta x = x$ alors je ne récupère que la moitié de la réserve de la seconde monnaie $\Delta y = y/2$. Pour tout prendre, $\Delta y = y$, il faut mettre une infinité, $\Delta x = \infty$. Le système est fait pour des échanges Δx petits par rapport à la taille de la réserve, sinon les prix s'envolent. Ce comportement permet une triche connue pour générer des prix anormaux dans l'espoir de récupérer ses gains ailleurs (cf ci-dessous). Bien sûr un tel prix anormal sera rapidement corrigé par d'autres investisseurs qui feront une bonne affaire en équilibrant cette DEX avec une autre, cf figure 6.22.

Les oracles Une des grandes faiblesses de la chaîne Éthereum est qu'elle ne sait rien du monde. Pourtant ce qui se passe dans le monde physique est très important pour la finance. Comment faire de la finance sans son flux Bloomberg? Si je veux construire un contrat qui enregistre les paris d'un tournois sportif, il faut que mon contrat sache de façon certaine qui a gagné tel match pour distribuer les gains.

Aussi on a construit les oracles dont le travail est d'enregistrer dans la chaîne des informations de l'extérieur [37], ce qui permet ensuite aux contrats de prendre en compte la donnée pour agir. Bien sûr, il faut avoir confiance en l'oracle pour être certain que le contrat fonctionne bien. Si l'oracle triche, ou si des personnes assez riches génèrent un micro-crash sur un DEX qu'utilise un oracle comme référence, alors le contrat se trompera (probablement en faveur des

35. Finance Traditionnelle
36. Decentralized EXchange
37. un oracle peut aussi sortir des informations de la chaîne comme des statistiques sur certains usages.

tricheurs). Aussi il est préférable d'utiliser plusieurs oracles pour travailler en toute confiance. Ainsi pour connaître le cours de l'ether dans un contrat, on regarde les valeurs entrées par un ensemble d'oracle et on prend la moyenne, cf figure 6.21.

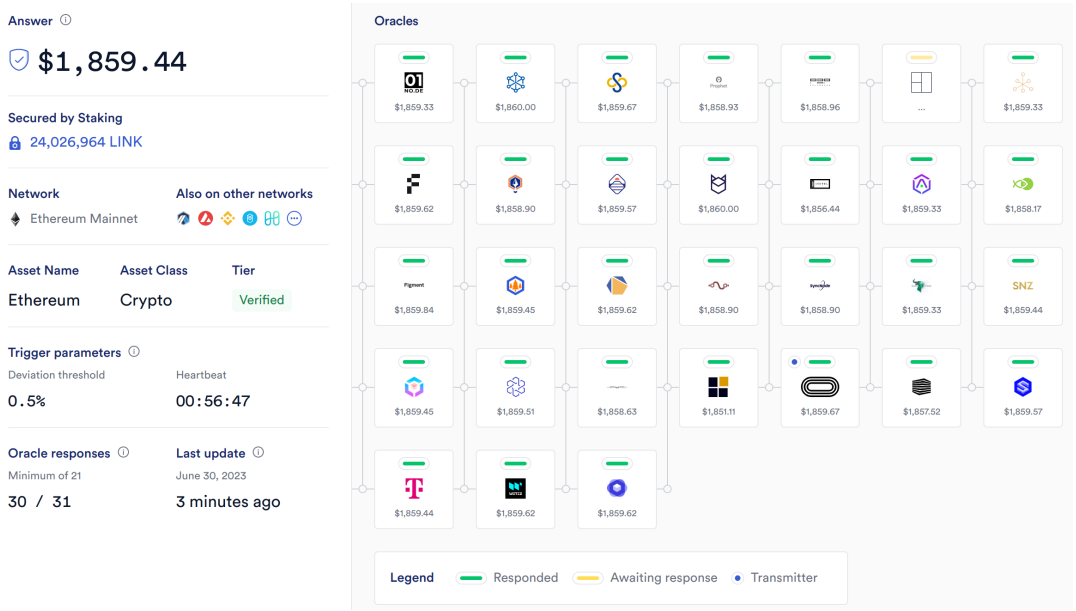


FIGURE 6.21 – Prix de l'Ether en dollars auprès d'un ensemble d'oracles
https://data.chain.link/ethereum/mainnet/crypto-usd/eth-usd

Equilibrer les DEX Parmi les contrats existants, les contrats d'emprunts sont bien utiles pour emprunter de la monnaie fiat en mettant en caution de la crypto-monnaie [38].

Dernièrement l'emprunt flash a été crée pour emprunter sans caution et rembourser en même temps, ou disons au sein du même bloc. Cela permet d'avoir l'argent pour faire une opération financière très rapide, prendre le bénéfice et rembourser. Ainsi on peut dans un seul bloc, emprunter, acheter sur une DEX, vendre sur une autre et rembourser, cf figure 6.22. Le bon coté pour le système est que cela permet que tous les DEX affichent les mêmes valeurs de change.

Il est également possible de refinancer une crypto dette avec un emprunt flash. Il suffit de faire un emprunt flash, rembourser sa dette, récupérer la caution et ainsi pouvoir faire un nouvel emprunt à un meilleur taux puis rembourser l'emprunt flash avec la somme empruntée. Tout cela au sein d'un bloc.

38. Pour ce type d'emprunt, la caution est supérieure à la somme empruntée et le contrat vend automatiquement la caution pour rembourser le prêteur si le cours de la crypto-monnaie baisse assez pour que la caution ne vaille que la somme empruntée.

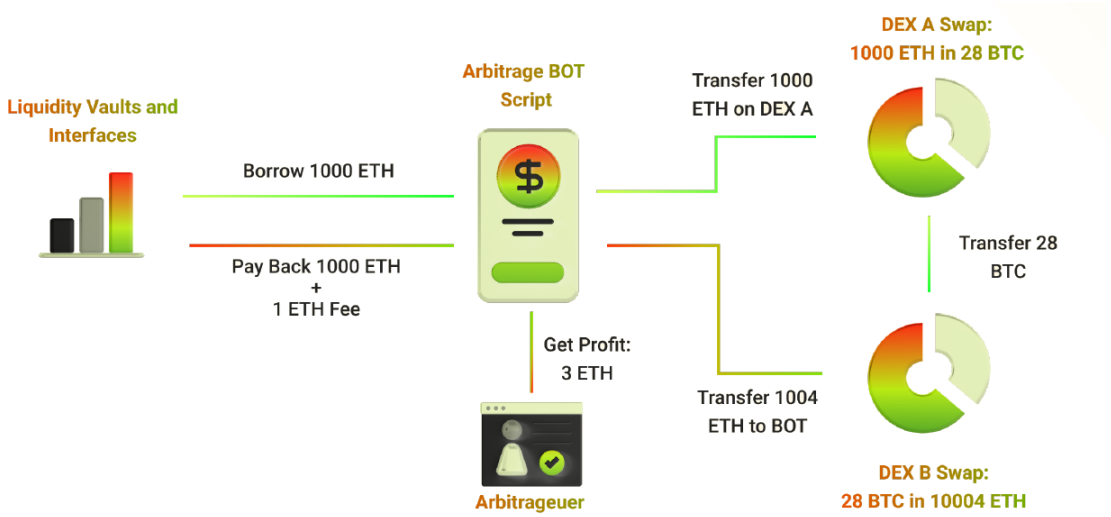


FIGURE 6.22 – Emprunt flash pour équilibrer deux DEX

Éthereum 2.0

Le fonctionnement du choix des transactions à valider ainsi que le mécanisme de preuve était les mêmes que pour le Bitcoin, à savoir qu'on utilisait la preuve par travail. Depuis fin 2022, Éthereum a choisi de passer à la preuve par enjeux (*proof os stakes* ou PoS).

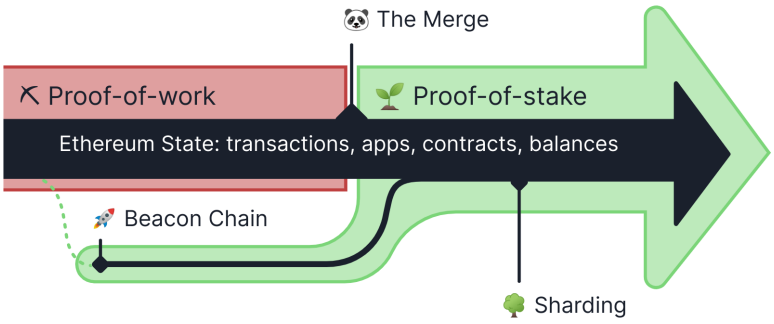


FIGURE 6.23 – Changement de méthode de preuve pour l'Éthereum

L'équivalent des mineurs s'appelle les validateurs dans la preuve par enjeux. On devient validateur en bloquant 32 éthers et en ayant un ordinateur qui participe au travail de validation.

Le principe de base de la preuve d'enjeu consiste à tirer au sort qui, parmi les validateurs, va valider le prochain bloc. L'idée est que les validateurs n'ont pas envie de détruire le système qui leur appartient, donc que le validateur écrira de façon honnête le prochain bloc. Il sera rémunéré pour ce petit travail ce qui revient à rémunérer l'argent mis en dépôt pour avoir le droit de valider les blocs (bien plus faible que la rémunération des mineurs du Bitcoin car il n'est plus besoin de rémunérer une consommation électrique folle).

Cela étant il y a des failles dans ce système si on l'applique tel quel. Le mineur peut vouloir optimiser ses gains et pour cela valider des blocs de différentes branches de la *blockchain*, les fausses comme la vraie, avec l'idée que si une fausse devient la plus longue, sa participation sera rémunérée. Aussi pour lutter contre cette stratégie, valider un bloc d'une mauvaise branche sera puni et entraînera une amende. Ainsi valider toutes les branches n'est plus rentable et il vaut mieux se focaliser sur le bonne.

D'autres types d'attaques ont été imaginé, comme l'achat d'assez de possesseurs pour les convaincre de tricher ensemble et donc avoir le poids pour écrire une fausse *blockchain*. Normalement Éthereum a pensé à tout mais seul l'avenir pourra le dire.

Du point de vue écologique, ce nouveau système est un véritable succès comme le montre le comparatif figure 6.24. En passant de la preuve par le travail à la preuve par enjeux, le système de validation de l'Éthereum a fait passer sa consommation de 78 TWh / an à 2,6 GWh / an. On est passé de la consommation de la Belgique (2022) à celle de 500 foyers français.

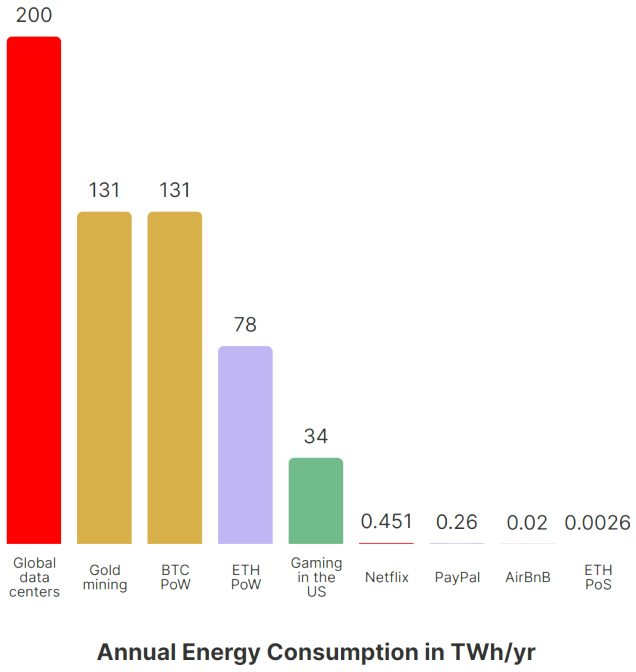


FIGURE 6.24 – Comparaison de la consommation électrique de l'Éthereum (PoW et PoS).

Des réseaux de niveau 2 (L2)

Comme pour le Bitcoin, l'Éther n'est pas adapté aux micro-transactions à cause du coût trop élevé des transactions. Aussi on applique la même solution avec des réseaux de niveau 2 qui travaillent dans leur coin et viennent inscrire des données dans la chaîne de l'Éthereum de temps en temps pour profiter de la sécurité qu'elle offre. Cela permet de résoudre le trilème des chaîne de bloc à savoir :

Une chaîne de bloc ne peut résoudre simplement 2 de ces 3 points mais le troisième sera

toujours très difficile :

— la sécurité
— la décentralisation (pas de nœud central, pas de chef qui choisit)
— le passage à l'échelle (accepter toujours plus de transactions)

Éthereum remplit les 2 premiers mais plafonne à 1 M transactions / jour.

D'autres réseaux, de niveau 2, s'appuient sur la *blockchain* d'Ethereum pour sa sécurité et peuvent ainsi remplir les 2 autres critères.

Optimism, Arbitrum ou Polygon en sont des exemples. Les 3 sont aussi des EVM mais avec des coûts (gaz) nettement inférieurs.

Rollup Une façon de baisser les coûts s'appelle le *rollup*. Cela consiste à

1. faire 100 transactions sur un réseau de niveau 2,
2. enregistrer la trace sur Ethereum (presque 100 fois moins cher).

Il existe 2 manières de faire cela.

Optimiste	Zéro connaissance
— L2 publie les transactions (supposées correctes) — une compression est enregistrée sur L1 — un délais permet à quiconque de montrer une faude — si fraude, alors on annule et on punit le tricheur — sinon, c'est validé	— L2 enregistre les transactions — une preuve de leur validité est envoyée dans L1 Fabriquer la preuve est un calcul difficile et donc faire une EVM compatible (zkEVM) est compliqué.

La méthode optimiste est simple à mettre en œuvre mais elle oblige à surveiller ce qu'on n'a pas tous envie de faire. De plus le délais pour dénoncer une tricherie, délais d'une semaine par exemple, ralentit nettement les transactions.

Aussi la méthode zéro connaissance est préférable si elle marche. Des évolutions prometteuses de zkEVM laissent à penser que le *rollup* zéro connaissance pourrait prendre son envol en 2023.

L2 + jetons + NFT = jeux On sent qu'on a un combo gagnant. Un niveau L2 offre la vitesse nécessaire et des frais assez faibles pour permettre des transactions fluides dans un jeux en ligne. Les jetons peuvent être une monnaie qui permet d'acheter dans le jeu et en dehors du jeu, quand aux NFT ils sont le support naturel pour les objets voire les personnage du jeu. On peut ainsi imaginer un joueur monter un personnage à un niveau 10 et le revendre, avec les jetons, à un autre joueur. Tout ce qui peut se construire, s'acheter et se vendre dans un jeu produit une économie dont les concepteurs du jeu contrôlent les rouages et peuvent prendre

une commission sur les transactions. Ainsi vous avez un jeu à l'entrée libre mais lucratif tant pour les concepteurs que pour les meilleurs joueurs.

On retrouve cette mécanique dans le jeu Axis Infinity qui a été un énorme succès jusqu'en mars 2022 lorsque le jeu s'est fait voler l'équivalent de 620 M$ en ether et USDC. Cela a fait chuter la valeur du jeton du jeu de 99% et le nombre de joueur est passé de 2,7 millions à environ 250 000.

Pour certains, le fait que les nouveaux joueurs achètent des personnages à des joueurs plus avancés et donc que le système a besoin de nouveau entrants pour que l'économie fonctionne, est proche d'une pyramide de Ponzi.

6.6.4 Les bébés Bitcoin

Le succès du Bitcoins, ses faiblesses et le désir de créer la crypto-monnaie qui offre les bonnes spécifications, ont poussé à la création de monnaies alternatives basées sur les principes du Bitcoin. Il existe aussi beaucoup de crypto-monnaies créées simplement pour enrichir ceux qui les lancent (c' est simple à faire puisque le code du bitcoin est ouvert).

Le site CoinChoose liste les monnaies vivantes (134 début 2020). On peut choisir une monnaie en fonction de sa popularité et donc de la possibilité de l'utiliser réellement comme monnaie, en fonction de ses caractéristiques avec le désir de promouvoir la « bonne » monnaie ou en fonction du rendement espéré pour spéculer. Le site Coin Market Cap présente chaque monnaie de façon complète ce qui permet aussi de se faire un avis.

Voici une présentation rapide de quelques monnaies alternatives au Bitcoin et à l'Éther et leurs spécifications :

— Le Ripple (XRP) est une des premières crypto-monnaies rattachée à une entreprise qui veut interagir avec les banques. Un procès pour création abusive de pièces est probablement une des raisons de sa baisse depuis 2018.
— Le Bitcoin Cash (BCH) est le fruit d'une scission majeure du Bitcoin en août 2017 pour amméliorer les transactions. En tant que scission il reprend le livre de compte des Bitcoins au 1er aout 2017 et donc tous les possesseurs de Bitcoins à cette date sont automatiquement possesseurs de Bitcoin Cash. Le succès initial est passé et la baisse régulière.
— Les Litecoin (LTC) est une copie du Bitcoin avec des transactions plus rapides et une masse monétaire finale plus grande.
— les Monero (XMR) est une monnaie qui désire offrir le plus grand anonymat possible.
— Le Dogecoin est initialement présenté comme une blague avec l'image du mème Doge. L'intérêt déclarée par Elon Musk pour cette monnaie lui a fait prendre un envol inattendu avant de retomber sèchement.
— Le Tether (USDT) est une crypto-monnaie stable ancrée au dollar US : 1 USDT = 1 $.

L'entreprise Tether Limited permet cette stabilité en garantissant qu'elle peut racheter tout tether avec des dollars. Cependant avec le temps on s'est rendu compte que cette affirmation est fausse, que non seulement Tether Limited n'a pas les fonds le permettant mais en plus rien ne l'oblige de rembourser contractuellement. Quoi qu'il en soit, le Tether a tenu et est stable.

— Le Dai est une autre crypto-monnaie stable dont la valeur est toujours 1 $. Plus précisément il s'agit d'un contrat Éthéreum dans lequel l'utilisateur qui fabrique des Dais met en gage des crypto-monnaies pour assurer la stabilité (laquelle est garantie tant que le système ne craque pas).

Notons que certaines monnaies très populaires ont vu leur cours s'effondrer voire tomber à zéro. En 2022, le cours de Luna est ainsi a chuté de 80 $ à rien en une semaine, générant 60 milliards de dollars de perte.

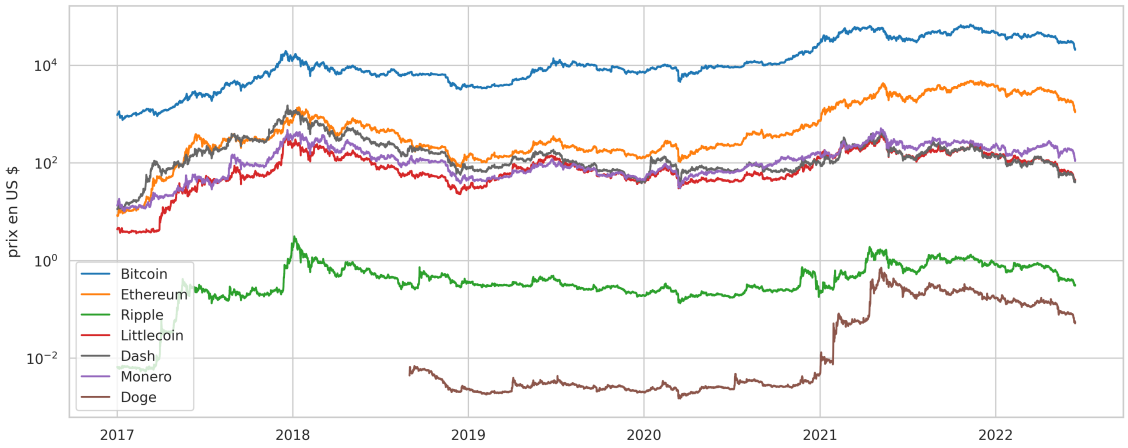


FIGURE 6.25 – Cours en dollars de quelques crypto-monnaies

De nouvelles monnaies sont régulièrement crées. Il est toujours tentant d'y participer au début en comparant aux débuts du Bitcoin et des autres monnaies qui ont "réussi" mais attention aux risques que la monnaie soit abandonnée et que votre investissement disparaisse dans la poche de ceux qui l'ont créée.

Plus

Pour en savoir plus sur les crypto-monnaies :

— le blog de Jacques Favier la voie du Bitcoin regarde avec son œil d'historien cette nouvelle monnaie et les réactions qu'elle suscite.
— le site web d'Éthereum est riche et bien écrit,
— les sites web d'information sur les crypto-monnaies : CoinDesk et le CoinTelegraph pour suivre l'actualité.

Troisième partie

L’animal politique

Chapitre 7

Une nouvelle démocratie

Si Internet modifie à tel point notre façon de vivre, il est naturel que ces modifications changent aussi notre rapport à la démocratie. De fait les changements sont nombreux même si nous votons toujours pour des élus qui nous représentent et si l'abstention est toujours aussi forte.

Le principal changement est la possibilité d'exister sans la presse et les médias classiques. Tout candidats peut écrire ses idées sur son site web comme le font de millions de citoyens. La difficulté n'est alors plus de s'exprimer mais d'être lu. Le filtre n'est plus l'accès au média mais de sortir du bruit.

Autre changement, Internet offre un meilleur accès à l'information. Les compte-rendus de certains conseils municipaux, des séances de l'assemblée nationale sont accessibles, les organismes d'état comme la cours des comptes publient leur rapports sur le web, idem pour les appels d'offre de l'État, pour la loi que nul n'est censé ignorer, etc. Toute ces informations font des citoyens avertis, toutes ces traces rendent le politique redevable.

Un dernier point fort largement utilisé est celui de pouvoir contredire nos élus. De nombreux blogueur se font un plaisir de souligner leurs erreurs, les microblogs comme Twitter sont inondés de commentaires en direct lors de débats, les propositions sont analysées et archivées.

Ces aspects ont déjà eu comme impact de changer les campagnes électorales. Non seulement tout candidat communique directement avec ses électeurs et ce pour un coût dérisoire mais surtout tout candidat se doit d'être présent sur Internet, d'avoir son site web voire son blog et son microblog pour le citoyen qui veut en savoir plus ou suivre en direct.

Maintenant la question est de savoir comment aller plus loin ? Comment peut-on améliorer notre démocratie avec cet outil ? On sent bien que la démocratie directe devient possible avec Internet alors qu'elle était techniquement impossible avant. Il y a certainement d'autres formes de démocratie à inventer pour que les citoyens se réconcilient avec la politique.

Mais ces points positifs en cachent des nettement plus noirs. Si Internet ouvre de nouvelles possibilités démocratiques, c'est aussi un merveilleux outils pour les régimes totalitaires et force est de constater que nos démocraties cèdent largement au biais de la surveillance massive au prétexte de lutte contre le terrorisme. C'est aussi le paradis pour les complotistes et

les manipulateurs qui trouvent un accès direct aux citoyens pour diffuser des fausses informations comme on l'a vu dans le chapitre sur la communication. Internet n'est peut-être pas l'avenir rose de la démocratie mais le cauchemar d'un état policier en création, d'un retour vers l'obscurantisme.

Ce chapitre commence par l'aspect Big Brother de l'Internet pour continuer avec des points plus optimistes, la transparence, la citoyenneté sur Internet et enfin quels types de démocratie deviennent possibles.

7.1 Surveillance

La notion de vie privée sur Internet est un point fort d'actualité. La mémoire de ce système, la possibilité de suivre à la trace les internautes, d'intercepter leurs communications sont des points largement débattus mais très largement négligé devant les avantages qu'offrent Internet et les services des grandes entreprises comme Google ou Facebook. Les révélations d'un Edward Swnoden sur la surveillance massive de la NSA [1] font couler beaucoup d'encre mais il est peu probable que cela pousse la majorité des internautes à changer leur habitude et décident de mieux protéger leur vie privée.

La NSA, National Security Agency

La NSA est en charge de l'interception et du déchiffrage des messages transmis de façon électronique pour le compte des États-Unis, que cela soit l'armée ou l'administration (de nombreuses entreprises américaines ont aussi profité d'informations de la NSA).

Son histoire remonte à la seconde guerre mondiale durant laquelle les américains et les britaniques ont su intercepter avec succès les messages des allemands et de japonais. À partir de cette période, il était évident que l'interception des communications électroniques était de première importance.

En 2013 la NSA comptait entre 30 et 40 000 employés et disposait d'un budget de 10 milliards de dollars. Elle est probablement une agence plus grande que la CIA.

7.1.1 D'Échelon à Prism

Plus grand monde utilise le courrier papier. Le téléphone, le fax et maintenant Internet ont largement remplacés ce mode de correspondance. Si on y a gagné en rapidité et fiabilité, force est de constater qu'on y a perdu en confidentialité. Il est en effet plus simple d'intercepter massivement des communications sur un réseau téléphonique ou sur Internet que du courrier postal. Aussi on peut dire qu'Internet est le meilleur ami des espions. Il leur offre sur un plateau la possibilité de (presque) tout savoir sur chacun de nous. Et sachant que l'on connecte de plus en plus de chose sur le réseau, les objets demain, il va bientôt être difficile d'aller aux toilettes sans que nos espions attitrés soient au courant.

1. National Security Agency, cf encart

Tous les services secrets utilisent ce mouchard, mais il en est un qui dispose de ressources que personne n'a, la NSA. Cette agence américaine dédiée aux écoutes et à l'espionnage électronique dispose

— des nœuds d'interconnexion les plus importants d'Internet sur son sol ce qui lui permet d'intercepter l'énorme majorité des communications internationales, voire inter-opérateurs au sein d'un pays, cf figure 7.1,
— des entreprises qui offrent les services les plus utilisés ce qui lui permet d'accéder légalement à leurs données, cf l'en-tête de la même figure 7.1,
— des entreprises de matériel informatique les plus populaires (même si la Chine peut légitimement revendiquer la première place en tant que fabricant) ce qui permet de déposer des mouchards physiques au sein des appareils,
— d'un budget que peu de pays peuvent s'offrir, 10 milliards de dollars en 2012,
— d'un environnement académique de mathématiciens, cryptographes et informaticiens le meilleur du monde.

Aussi il n'est pas étonnant qu'elle ait eu des envies d'hégémonie à savoir intercepter toutes les communications. Cette envie à commencé avant même qu'Internet ne s'ouvre au grand public, lorsque les communications utilisaient surtout le réseau téléphonique. Fort de ses capacités technologiques les États-Unis ont développé le programme Echelon avec leur partenaires anglophones, le Royaume Uni, l'Australie, la Nouvelle-Zélande et le Canada.

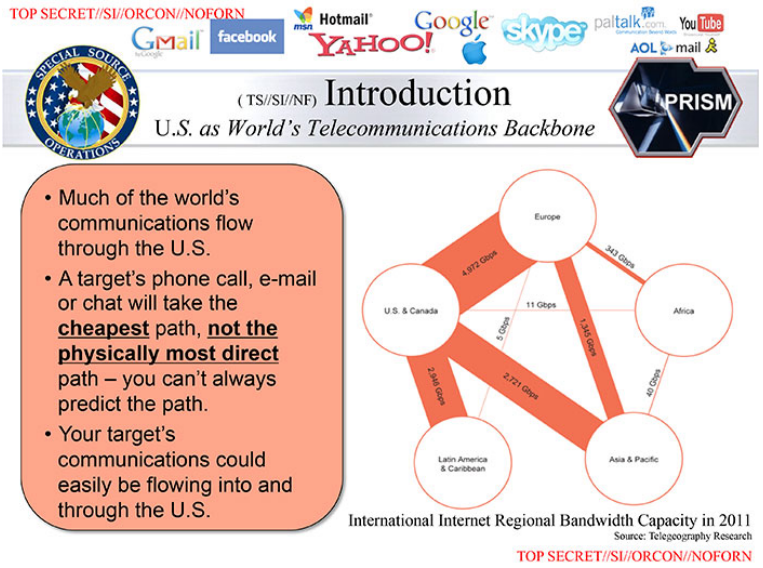


FIGURE 7.1 – Présentation interne de la NSA sur l'avantage américain en terme de réseau
source : NSA, diffusé par Edward Snowden en 2013

Echelon

Ce programme initialement destiné à surveiller l'URSS et ses alliés durant la guerre froide s'est étendu pour couvrir de plus en plus de communications. Durant les années 70, la première base d'écoute des communications téléphoniques par satellite a été construite pour couvrir le

monde entier dans les années 80. Mais Echelon ne s'est pas limité aux satellites et en 2013 il semble clair qu'il couvre toutes les communications téléphoniques et par Internet.

Le point de controverse porte plus sur l'usage que sur l'existence d'Echelon. En tant que programme militaire qui espionne les autres armées, c'est de bonne guerre. Mais dès lors que cet outil sert à intercepter les communication des entreprises voire celles des individus, il y a un véritable risque de quitter le cadre de la démocratie pour glisser vers un régime nettement moins sympathique. C'est le principal reproche qui lui est fait car Echelon a effectivement servi à des fins économiques mais aussi pour intercepter en masse des communications personnelles.

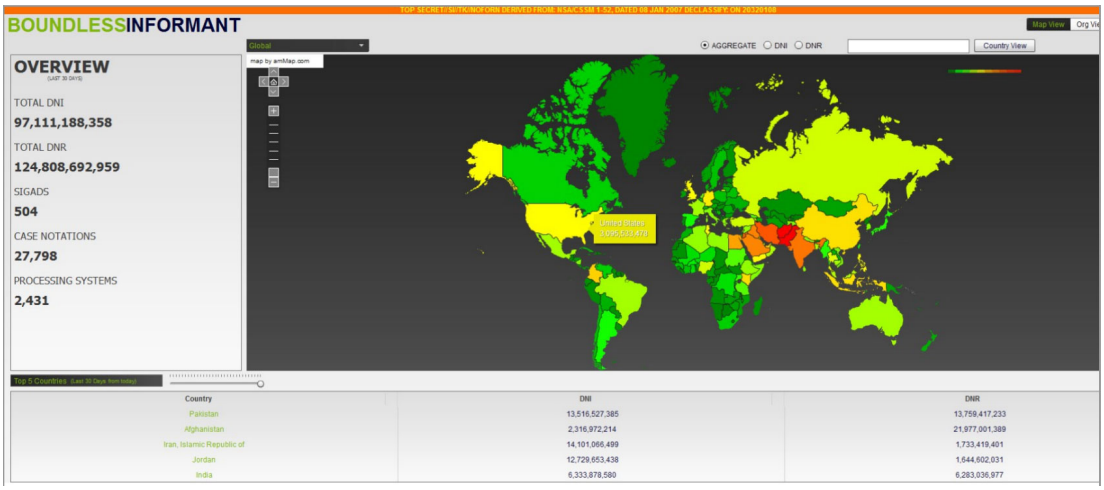


FIGURE 7.2 – Boundless Informant, un logiciel de la NSA de synthèse des écoutes
source : NSA, diffusé par Edward Snowden en 2013

Aux États-Unis le choc a surtout été d'apprendre que les citoyens américains sont aussi massivement espionnés, y compris les élus, alors que la loi américaine l'interdit. La NSA se défend en indiquant que seules les méta-données sont gardées, à savoir quel numéro communique avec quel numéro, quand, combien de temps..., et non la conversation en elles-mêmes. Cette excuse déjà en cours en 2006, sous la présidence de Bush fils, avait été fortement critiquée alors par Joe Biden, celui qui allait devenir le vice président des États-Unis en 2009 :

> *I don't have to listen to your phone calls to know what you're doing. If I know every single phone call you made, I'm able to determine every single person you talked to. I can get a pattern about your life that is very, very intrusive. . . . If it's true that 200 million Americans' phone calls were monitored - in terms of not listening to what they said, but to whom they spoke and who spoke to them - I don't know, the Congress should investigative this.*
>
> *Je n'ai pas à écouter votre conversation téléphonique pour savoir ce que vous faites. Si je sais chaque coup de fil de que vous donnez, je peux connaitre chaque personne avec laquelle vous avez parlé. Je peux avoir une vision de votre vie et cela est très, très intrusif... S'il est vrai que 200 millions d'appels téléphonique d'américains ont été tracés - non pas en écoutant ce qui est dit, mais en sachant à qui ils parlent et qui leur parlent - je ne sais pas, le Congrès devrait enquêter là dessus.*

La capture d'écran figure 7.2, montre qu'en 2013 on est à plus de 2 milliards d'interceptions mensuelles de tout type aux États-Unis et près de 100 milliards d'interceptions sur Internet et 125 milliard d'interceptions téléphoniques au niveau mondial. Il est triste de constater que le vice-président n'a pas su lutter contre cette dérive. Un sondage [2] montre qu'à l'inverse, les Démocrates ont fondamentalement changés d'avis en arrivant au pouvoir, pour passer de 37 % qui approuvaient le programme de surveillance de la NSA en 2006 à 64 % en 2013.

Prism

Sur Internet on peut faire plus simple que d'intercepter les communications lorsqu'on est les États-Unis et que l'on dispose des principales entreprises du net sur son sol. On peut simplement les forcer, à l'aide de la loi, à transmettre les données dont elles disposent. C'est le programme Prism. Ainsi les principales entreprises américaines de l'Internet ont été forcées à donner les clefs de leurs serveurs à la NSA et cela dans le plus grand secret. La figure 7.3 montre les dates d'enrôlement pour ces entreprises.

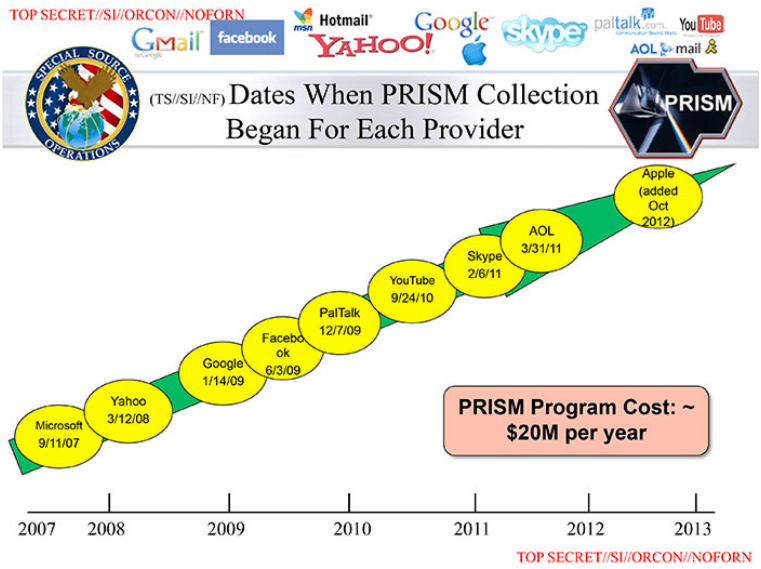


FIGURE 7.3 – Dates de l'enrollement des entreprises du net au programme Prism
source : NSA, diffusé par Edward Snowden en 2013

Avec de telles entreprises dans la poche, on comprend la puissance de la NSA qui peut lire les courriers Gmail, savoir tout ce que vous avez mis de privé sur votre page Facebook, écouter vos conversations sur Skype... Le coût affiché de 20 millions de dollars par an est ridiculement faible et offre un rapport qualité/prix imbattable.

2. cf http://www.theguardian.com/commentisfree/2013/jun/14/nsa-partisanship-propaganda-prism

Muscular

Prism étant légal, on peut espérer qu'il y ait des limites, en particulier que les entreprises sachent ce que fait la NSA. Mais pour les espions, la fin justifie souvent les moyens. Cela expliquerait le programme Muscular dont le but est d'infiltrer Google et Yahoo afin d'accéder à toutes les données sans limites légales. Là encore le document figure 7.4 est des plus explicite.

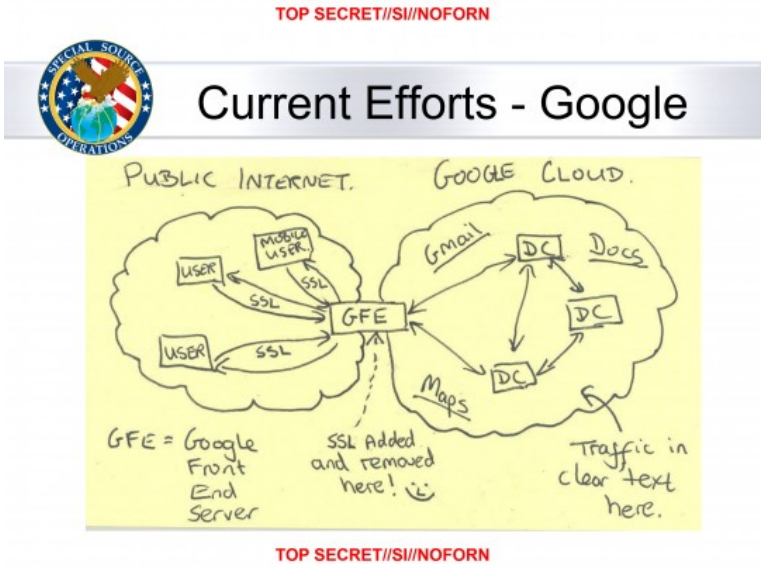


FIGURE 7.4 – Schéma sur l'infiltration au sein du Google Cloud
source : NSA, diffusé par Edward Snowden en 2013

Ce programme Muscular n'est pas isolé. Les débordements révélés par Edward Snowden, le fait que de nombreux employés de la NSA puissent accéder aux données de n'importe qui et établir une surveillance librement quelque soit la personne visée, soulignent la nécessité d'introduire des mécanismes efficaces de surveillance des surveillants. Une première étape pourrait être de protéger les lanceurs d'alerte afin d'être plus facilement informé des abus.

France : la loi sur le renseignement

Cette loi légalise certains comportements illégaux déjà en œuvre des barbouzes et autres policiers afin de créer l'équivalent de la NSA. Les points majeurs sont :

- une surveillance de masse,
- la pose de boites noires chez les FAI pour intercepter toutes les communication et détecter les comportements suspects,
- l'autorisation de mise en œuvre des techniques de recueil du renseignement vient du premier ministre. Les juges sont court-circuités,
- 4 ans de conservation des métadonnées

Notons que le Premier ministre peut ordonner à tout moment que la mise en œuvre de la technique concernée soit interrompue et que les renseignements collectés soient détruits sans délai. On ne veut pas voir dans cette mesure une protection contre la divulgation d'affaires politiques.

7.1.2 Les lanceurs d'alerte

Les lanceurs d'alerte [3] sont les personnes qui dévoilent une atteinte grave à l'intérêt général dont elles sont témoins.

Si ces lanceurs d'alerte ne peuvent être la seule réponse au dysfonctionnements graves, leur existence est une sécurité importante pour la démocratie. Il semble donc nécessaire de les protéger légalement, en faisant bien attention de séparer le bon grain de l'ivraie à savoir les lanceurs d'alerte des délateurs intéressés. L'alerte pouvant être de toute nature, industriel, politique, écologique, médical, etc, il est important de ne pas limiter le champs des dénoncements possibles.

En France, la loi n° 2013-316 du 16 avril 2013 relative à l'indépendance de l'expertise en matière de santé et d'environnement et à la protection des lanceurs d'alerte garantit la protection du lanceur d'alerte mais en limitant son champs à ce qui faisait l'actualité à l'époque (le médicament Médiator et la disparition des abeilles en particulier).

Une loi de 2007 protège les employés du secteur privé qui signalent les faits de corruption et une autre de 2013 qui porte sur les conflits d'intérêts en politique.

En 2016 la loi Sapin 2 chapitre II [4] généralise la portée tant en retirant les notions de secteurs qu'en élargissant la liste des infractions qui méritent une alerte. L'article 6 dit

> *Un lanceur d'alerte est une personne physique qui révèle ou signale, de manière désintéressée et de bonne foi, un crime ou un délit, une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou une menace ou un préjudice graves pour l'intérêt général, dont elle a eu personnellement connaissance.*
>
> *Les faits, informations ou documents, quel que soit leur forme ou leur support, couverts par le secret de la défense nationale, le secret médical ou le secret des relations entre un avocat et son client sont exclus du régime de l'alerte défini par le présent chapitre.*

La procédure pour faire remonter une alerte est indiquée dans l'article 8, elle se résume à :

1. Faire remonter les faits en interne par le canal *ad hoc* que doit avoir toute entreprise de plus de 50 personnes ou administration,
2. À défaut de réaction informer la justice ou une autorité administrative
3. À défaut de réaction dans les 3 mois, possibilité de diffuser l'information publiquement.

La protection accordée protège contre le licenciement et accorde l'anonymité lors de la diffusion de l'information à la justice. Il est aussi prévu des sanctions contre ceux qui feraient obstacle au signalement du lanceur d'alerte et contre ceux qui intenteraient une procédure abusive en diffamation.

3. *whistleblowers* en anglais à savoir celui qui siffle la faute en référence au sport.
4. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033558528/

Pour une information plus détaillée il est recommandé de lire la page didiée [5] de la Maison des lanceurs d'alertes.

Fin 2019, l'Europe a voté une directive "sur la protection des personnes qui signalent des violations du droit de l'Union" [6]. Un an après la transposition de cette directive dans le droit français n'avait pas commencé [7]. Parmi les évolutions notons que la procédure de signalement passe à 2 étapes, interne ou autorités compétentes puis divulgation au grand public.

Edward Snowden

Le 6 juin 2013 Edward Snowden rend public à travers la presse des informations sur le système d'écoute mis en place par la NSA. Ces révélations ont mis au grand jour l'ampleur des activités de la NSA.

Photo de Laura Poitras (Praxis Films) - juin 2013

Ayant commencé à travailler à la CIA en 2006, il a changé régulièrement d'employeur mais est toujours resté lié au milieu des services secret. Il se déclare comme un expert consulté par les dirigeants des agences sur des points techniques complexes. Un ancien collègue de la NSA l'a défini comme un génie hors norme. De son coté la NSA a indiqué qu'il a triché sur ses diplômes et qu'il n'était un informaticien quelconque qui a volé des mots de passe pour obtenir les documents qu'il a transmis.

Quoi qu'il en soit, il en a assez vu pour considérer que la surveillance globale de la NSA devait être révélée publiquement puisque ses questions officielles n'avaient pas eu de réponses autres que *Tout va bien*.

> *The more you're told its not a problem until eventually you realize that these things need to be determined by the public and not by somebody who was simply hired by the government.*

Il indique aussi avoir choisi les documents qu'il a transmis afin d'étayer ses propos sans mettre en danger le fonctionnement et les membres de la NSA.

Il est actuellement réfugié politique à Moscou après être passé par Hong Kong où il a donné l'interview expliquant son geste. On pourra aussi regarder Citizenfour le documentaire [a] qui couvre cette histoire ou le biopic "Snowden" d'Oliver Stone.

a. Oscar 2015 du meilleur documentaire.

Ailleurs dans le monde, le statut des lanceurs d'alerte varie. Pour un État il y a toujours le risque que ses affaires illégales soient mises au grand jour et lorsque l'on parle de services secrets ou de l'armée, c'est vu comme un trop grand risque. Aussi les lois sont le plus souvent schizophréniques, moralement elles vont dans le sens de la protection des lanceurs d'alerte mais elles y mettent des conditions, comme ne pouvoir dénoncer les abus qu'auprès des autorités.

Ainsi aux États-Unis où la protection des lanceurs d'alerte est liée à la liberté d'expression, la Court Supreme a restreint cette liberté pour les affaires liés à la défense et pour les fonctionnaires dans le cadre de leur travail. En dehors de ces points, les révélations d'actes illégaux, de gaspillage massif d'argent et certains autres points, doivent être fait auprès de l'Office of Special Counsel, l'autorité administrative dédiée.

5. https://mlalerte.org/procedure-aide-pour-lancer-l-alerte/
6. La directive : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32019L1937 et le site qui suit ce sujet https://whistleblowerprotection.eu/
7. En moyenne le délais pour transcrire une loi est de 18 mois, les règles européenne demande d'éviter absolument les retards supérieurs à 2 années.

Les scandales sont encore largement présents dans nos sociétés et n'ont pas de raison de disparaitre tant que la société ne s'en donnera pas les moyens. La culture du secret, la crainte de nuire à sa propre entreprise, le corporatisme, les labyrinthes administratifs sont autant de raisons qui vont à l'encontre de la dénonciation d'actions illégales. Un changement fondamental du système passe par une plus grande transparence, à laquelle participent pleinement les lanceurs d'alerte, mais qui n'est pas forcément du goût de tous.

WikiLeaks

Créé en 2006 par Julian Assange, WikiLeaks [a] est une association qui lutte pour la transparence et dévoile des documents secrets.

Elle est devenu célèbre avec la divulgation d'informations sur les guerres menées en Afghanistan et Irak par l'armée américains [b]. Mais le coup d'éclat qui a fait la une de tous les journaux, a été la diffusion en 2010 de 250 000 messages diplomatiques des ambassades états-uniennes [c]. Ces messages ont été publiés et analysés par les plus grands journaux du monde au grand dam du gouvernement américain. Julian Assange est devenu depuis une cible retranchée dans l'ambassade de l'Équateur à Londres, celui qui a fourni les messages à WikiLeaks, Chelsea (Bradley à l'époque) Manning a été condamné à 35 ans de prison et WikiLeaks a été attaqué financièrement, Paypal, Visa et MasterCard faisant de sorte à ce qu'il ne soit plus possible de faire de dons à l'association.

Depuis Wikileakds continue à diffuser des documents secrets. Durant l'été 2015, un demi-million de documents du ministère des affaires étrangère d'Arabie Saoudite ont commencé à être publiés, montrant les énormes moyens financiers mis en place pour la diffusion de l'Islam sunnite à travers le monde et pour contrer l'Iran chiite.

a. http://195.35.109.53/
b. dont cette vidéo qui a marqué les esprits https://collateralmurder.wikileaks.org/
c. https://wikileaks.org/cablegate.html

Évasion fiscale et blanchiment d'argent

Parmi les fuites retentissantes il y a celles qui touchent l'évasion fiscale, le blanchiment d'argent et l'optimisation fiscale agressive. Voici des fuites importantes diffusées par le Consortium international des journalistes d'investigation.

- 2014 : **Lux leaks**
  - Antoine Deltour dénonce PricewaterhouseCoopers
  - Evasion fiscale de 343 entreprises
- 2015 : **Swiss leaks**
  - Hervé Falciani dénonce HSBC
  - 180 G€ évadés pour 100 000 clients et 20 000 companies *offshore*
- 2016 : **Panama papers**
  - 11,5 M documents fuités
  - 214 k entreprises *offshore* qui touchent entre autre
    - 12 chefs d'état
    - 128 dirigeants politiques et hauts fonctionnaires
    - 29 des 500 personnes les plus riches du monde
- 2016 : **Football papers**
  - 18,6 M documents fuités
  - Système d'évasion fiscale pour joueurs et entraineurs
- 2017 : **Paradise papers**
  - 13,5 M documents fuités
  - 120 G€ pour l'Europe (20 G€ pour la France)
  - Optimisation fiscale souvent (mais est-ce éthique ?)

7.2 Transparence

La transparence offre la possibilité d'observer ce qui est fait. Dans son acceptation générale est concerne les entreprises et les administrations afin de permettre aux citoyens de noter les actions illégales ou même simplement très peu éthiques (l'autre sens s'appelant la surveillance).

Elle peut entrer en conflit avec la protection de la vie privée ou d'autres protections comme le secret médical, la protection des sources des journaliste ou le secret défense. Aussi il est nécessaire de définir une ligne de partage entre ce qui est du ressort d'une protection et ce qui est du ressort de la transparence. Une telle ligne ne peut être gravée dans le marbre et doit pouvoir s'adapter aux différents cas.

> *La protection de la vie privée d'un individu est une raison importante pour faire exception au droit à l'information. Cependant, cela ne signifie pas que l'accès à un document doit être systématiquement refusé s'il contient des données personnelles. Transparence et vie privée sont deux droits fondamentaux d'importance égale, aucun des deux ne prévaut sur l'autre. Un examen attentif de ces deux principes est la clé d'une solution appropriée.*
>
> Peter Hustinx, Contrôleur européen de la protection des données, 2005

Il est d'autant plus nécessaire de lui laisser la possibilité d'évoluer que les nouvelles générations n'ont pas les mêmes inquiétudes que leurs ainés pour ce qui touche la vie privée. Pour Mark Zuckerberg, fondateur de Facebook, la frontière se déplace vers la transparence :

> *People have gotten really comfortable not only sharing more information and different kinds, but more openly and with more people.*
> *Les gens sont vraiment devenus à l'aise non seulement pour partager de l'information et différents trucs, mais aussi de façon plus ouverte et avec plus de personnes.*

Si depuis cette déclaration de 2010 il a mis de l'eau dans son vin, d'autres n'hésitent pas à dire que la vie privée est morte.

Il existe aussi la frontière entre l'intérêt de la collectivité versus la protection de l'individu. C'est au nom de cet intérêt que des dirigeants peuvent, maladroitement, dire que celui qui n'a rien à se reprocher n'a rien à craindre de la surveillance étatique. Maladroitement car on retombe sur le cas de la NSA et on peut se demander si les surveillants ne sont pas eux même la source de danger. Maladroitement car chacun a besoin d'une zone privée.

> *Il y a une idée reçue : les métadonnées c'est anonyme, ça ne risque rien. Mais si je partais avec toutes vos données de connexion, j'en saurais plus sur votre vie privée qu'en cinq ans de mandat.*
>
> Le député Sergio Coronado lors du débat sur la loi Renseignement – avril 2015

Aussi, dès lors qu'il y a surveillance massive, on peut se demander si l'équilibre alors ne serait pas dans la réciprocité à savoir que les entreprises et les administrations soient transparentes.

Une mairie ne devrait rien avoir à cacher à ses administrés ou à qui que ce soit. On peut penser de même pour une région, un État [8], Pour une entreprise qui a une interaction forte avec le public voire une mission de service public, la transparence là encore devrait être la norme. Pour les autres entreprises il semble raisonnable d'imposer un minimum de transparence (les entreprises cotées en bourse acceptent déjà un niveau de transparence financière).

Facteur économique

Si l'aspect moral est évident, il y a aussi un aspect économique à la transparence. Le premier concerne la libre concurrence et la lutte contre la corruption. Par exemple les marchés publics se doivent d'être transparents d'après les directives européennes comme le rappelle la Commission Européenne lors d'un remontage de bretelles :

> *... Les procédures d'adjudication ouvertes et transparentes qu'imposent les règles de l'UE sur les marchés publics renforcent la concurrence, offrent une meilleure protection contre la corruption et permettent aux contribuables de bénéficier de services plus efficaces et d'un meilleur rapport qualité-prix.*
>
> *Le fait de modifier les termes et conditions essentiels d'un marché public sans donner aux soumissionnaires la possibilité de concourir pour son attribution risque sérieusement de fausser la concurrence, de dissuader les nouveaux soumissionnaires potentiels et d'aboutir au gaspillage de l'argent des contribuables.*
>
> http://europa.eu/rapid/press-release_IP-12-73_fr.htm

Notons qu'il n'est pour toujours facile d'être cohérent en la matière. Si le président Sarkozy déclare «*Il y a des gens qui profitent de l'augmentation du pétrole, n'y allez pas, allez acheter votre essence là où c'est moins cher.*» cela ne veut pas dire que l'administration va aller dans le même sens.

Ainsi un particulier a découvert sur le site du ministère des finances le prix des carburants dans toutes les stations services (les stations ont obligation de faire remonter cette information). Il a donc utilisé cette information pour faire une application Android, Carburant Futé, qui permettait de savoir le prix de l'essence autour de soi. Ainsi un conducteur pouvait choisir en connaissance de cause et faire jouer la concurrence.

Sauf que le ministère ne l'a pas entendu de cette oreille et a considéré que l'utilisation de ses données devait être rémunérée. Le fait que l'application était gratuite, ne générait pas de revenus et rendait un service public n'y a rien changé, l'auteur devait payer une redevance. Aussi l'auteur a fermé son application. Trois plus tard, en 2014, les données ont été libérées.

Les sites qui permettent aux consommateurs de noter les hôtels, les restaurants ou autres services, participent aussi à la transparence et ont un véritable impact économique. Une étude indique qu'une étoile de plus sur le site Yelp augmente les revenus d'un restaurant entre 5 et

8. Il ne serait pas absurde d'imaginer une part de transparence au sein des services secrets et de l'armée.

9 % [9]. Si on ajoute à ces avis participatifs des informations administratives, on améliore d'autant le conseil, surtout lorsqu'il s'agit de l'avis des services sanitaires sur les restaurants comme c'est le cas à San Francisco, cf figure 7.5.

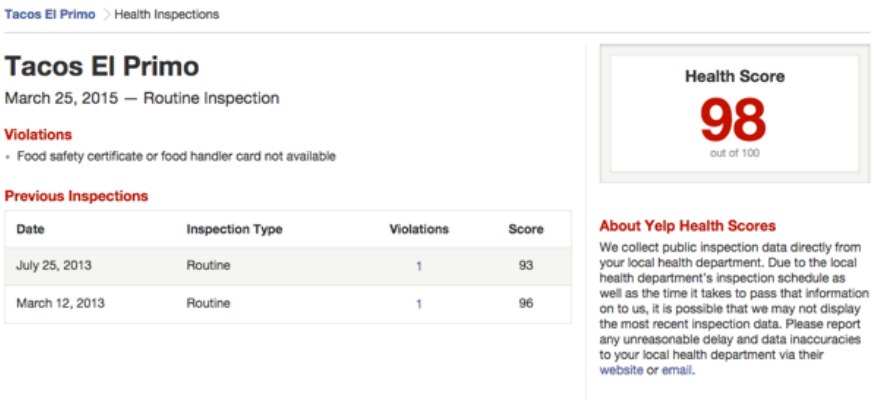


FIGURE 7.5 – Conseils Yelp avec avis sanitaire

Justice sociale

La transparence est aussi un facteur de justice sociale. Lorsque des catégories entières sont traitées différemment sans réelles raisons on peut parler d'injustice sociale. Cela peut être aussi bien dans un sens que dans l'autre, discrimination ou privilèges.

En matière d'impôt par exemple il est connu que certains savent naviguer pour éviter de payer. Barrack Obama a voulu lutter contre ce phénomène en appliquant la règle suggérée par Warren Buffet [10] pour contrer le fait qu'un grand nombre de millionnaires ont un taux de taxation inférieur aux classes moyennes. L'opposition a pu bloquer cette loi. Cette histoire peut être transposée à beaucoup de pays.

Une façon d'éviter ces abus peut être de les rendre public. Ainsi les pays scandinaves, précurseurs en matière de transparence, publient depuis fort longtemps les revenus et impôts de chaque citoyens. Depuis 2013 l'accès à cette information est limité aux personnes qui s'identifient ce qui permet aux personnes dont les fiches ont été visitées de savoir par qui [11] (une sorte de double transparence).

Toujours dans le domaine des impôts, les impôts locaux varient de façon très importantes d'une ville à l'autre et même au sein d'une ville puisque la valeur locative sur laquelle se base l'imposition n'est que rarement mise à jour [12]. Si les taux d'imposition des départements sont bien indiqués sur le site de données publiques du gouvernement, celui des villes n'est pas visible et la valeur locative de chaque maison encore moins. Là encore la publication des valeurs locatives retenues participerait à la justice sociale [13].

9. étude de 2011 : http://www.hbs.edu/faculty/Pages/item.aspx?num=41233
10. cf http://en.wikipedia.org/wiki/Buffett_Rule
11. cf http://www.skatteetaten.no/nn/Person/Skatteoppgjer/Sok-i-skattelistene/
12. une expérimentation est en cours en 2015 pour y remédier, espérons que les résultats seront publics.
13. cf l'article de Claire Gallon et Johan Vincent sur http://www.metropolitiques.eu/L-open-data-de-la-fiscalite-en.html
m.à.j. sur http://www.ricou.eu.org/e-politique.html

À l'inverse la publication des personnes qui touchent le RSA n'est pas publique non plus. Pourtant là aussi on pourrait y trouver des avantages comme détecter les fraudeurs patents, conseiller ceux qui n'en profitent pas mais qui pourraient ou découvrir qu'un proche a besoin d'aide.

7.2.1 Open Data

Avec Internet l'information est largement partagée sur le Web et chacun a au bout du clavier accès à plus d'information que n'en ont eu les générations précédentes. Mais cette information est souvent perdues dans le flux, partielle, mal présentée, protégées par des formats fermés... ou tout simplement elle est faite pour être lue par un humain et non pour être analysée par un programme informatique. Or l'information brute, les données, peut permettre de savoir beaucoup de choses y compris des choses que l'on ne désirait pas diffuser.

L'Open Data consiste à rendre les données librement accessible dans un format lisible par tous. C'est un acte de transparence qui peut avoir un impact économique fort. C'est aussi pour beaucoup c'est un acte de communication car l'Open Data est à la mode. Ainsi la SNCF a son site d'Open Data, https://data.sncf.com/, mais tant la cartographie des gares faites par des membres du projet OpenStreetMap que les faibles données accessibles font plus penser à une opération marketing qu'une réelle volonté de transparence [14]. Par exemple les données sur les retards des trains sont une synthèse générée par la SCNF et non les données brutes sur l'heure d'arrivée de chaque train. Les données brutes permettraient d'extraire un grand nombre d'informations qui peuvent aller jusqu'à l'état des voies, le taux de grévistes et plein d'autres informations auxquelles ni moi ni la SNCF ne pensons.

On comprend le danger politique mais c'est aussi une chance d'avoir des retours qui permettent d'améliorer le système.

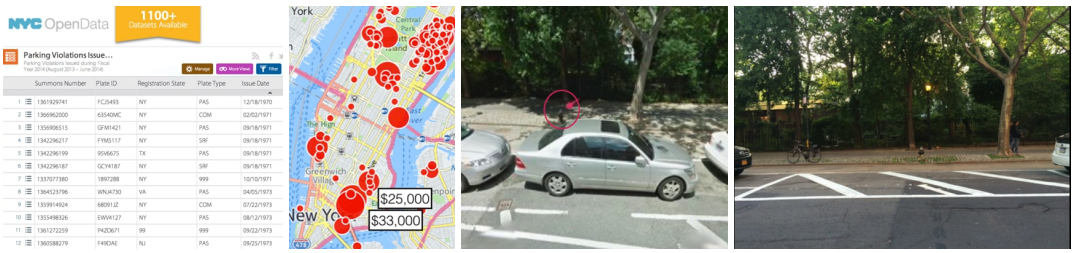


FIGURE 7.6 – Les données ouvertes améliorent la signalétique
source : Ben Wellington : How we found the worst place to park in New York City – TED 2014

Par exemple la ville de New-York n'avait probablement pas pensé, en rendant publique la liste des amendes pour stationnement, qu'elle pourrait améliorer sa signalétique. Un particulier a calculé avec ces données le "prix" annuel des places illégales et a découvert que certaines places sont très lucratives pour la ville. Il s'agissait des places devant les bornes d'incendie qui ne étaient pas indiquée comme telles et qu'un automobiliste pouvait très facilement confondre avec une place autorisée, la borne n'étant pas toujours très visible. Suite à cette constatation le

14. il aussi est possible que la volonté de transparence soit réellement là mais que des actions internes bloquent la diffusion de données.

particulier a prévenu la mairie qui a ajouté une signalétique au sol dans les semaines qui ont suivies, cf figure 7.6.

Basic data for everyone (DK)

Dans le cadre de son plan 2011-2105 d'eGovernement, le Danemark a décidé en 2012 l'ouverture des données fondamentales comme le cadastre, les cartes topographiques, les adresses, certaines données sur les individus. Cet accès à l'information simplifié, mais aussi l'impact structurant de cette ouverture [a], devrait permettre au Danemark de générer des économies d'environ 100 M€ par an pour les secteurs privés et public (66 et 34 M€ respectivement). Le coût de l'ouverture des ces données est de plus 40 M€ sur 4 ans mais les gains rendent l'opération rentable pour le secteur public dès la 3e année.

source : http://uk.fm.dk/publications/2012/good-basic-data-for-everyone/

a. actuellement les adresses sont générées au niveau municipale sans aucune cohérence entre les villes

Une tendance générale

La libre diffusion des données de l'État est une notion relativement ancienne mais ce n'est qu'avec Internet qu'elle prend pleinement son sens, les données devenant directement accessibles. Comme souvent sur Internet le mouvement de l'Open Data des données publiques a été initié par les pays anglo-saxons. Les État-Unis avec leur longue tradition de diffuser librement les données de l'État avaient déjà ouvert la voie avant que l'on parle d'Open Data avec la diffusion de nombreuses données [15].

Dans les années 2000 la fondation Open Knowlegde a su promouvoir la libération des données administratives en particulier en Angleterre, champion de l'Open Data.

> *We believe open knowledge can empower everyone, enabling people to work together to tackle local and global challenges, understand our world, expose inefficiency and challenge inequality and hold governments and companies to account.*
>
> *Nous pensons que le savoir ouvert démultiplie nos possibilités, permet le travail partagé pour répondre aux défis locaux et globaux, améliore notre compréhension du monde, souligne les inefficacités et inégalités et rend redevables les gouvernements et entreprises.*
>
> Open Knowledge se définissant – cf section About, avril 2015

15. Les marins connaissent depuis longtemps les bulletins météo météo mondiaux diffusé au format Grib par les services météo américains et les cartes marines numérique des États-Unis en libre accès. La France vend ces informations.

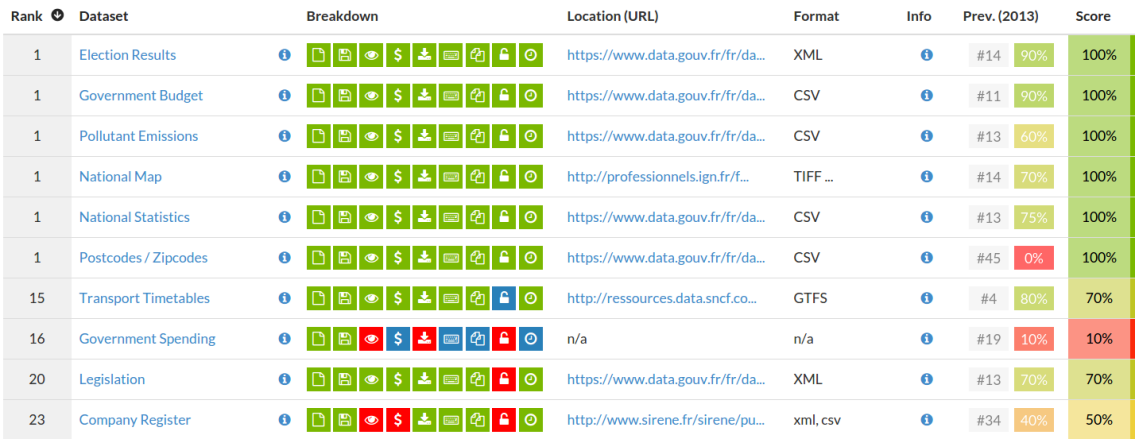
FIGURE 7.7 – Pays ayant le plus ouvert leurs données – *source : Open Knowledge 2018*
6 critères : licence ouverte, format machine, téléchargeable en bloc, à jour, public, gratuit

Ajoutons que des données ouvertes implique des données partagées ce qui permet d'éviter d'avoir les mêmes bases développées dans plusieurs ministères et garanti une meilleure qualité de la base tant d'un point de vue structurel qu'au niveau de la validité des données qui y sont.

Aujourd'hui la majorité des pays ont un programme d'ouverture des données publiques mesurés par l'Open Knowledge ainsi que par l'OpenData Barometer. Chaque organisme ayant sa métrique, les résultats varient. Fin 2018, le top 10 d'OpenData Barometer est Canada, UK, Australie, France, Corée, Mexique, Japon, Nouvelle Zélande, USA, Allemagne.

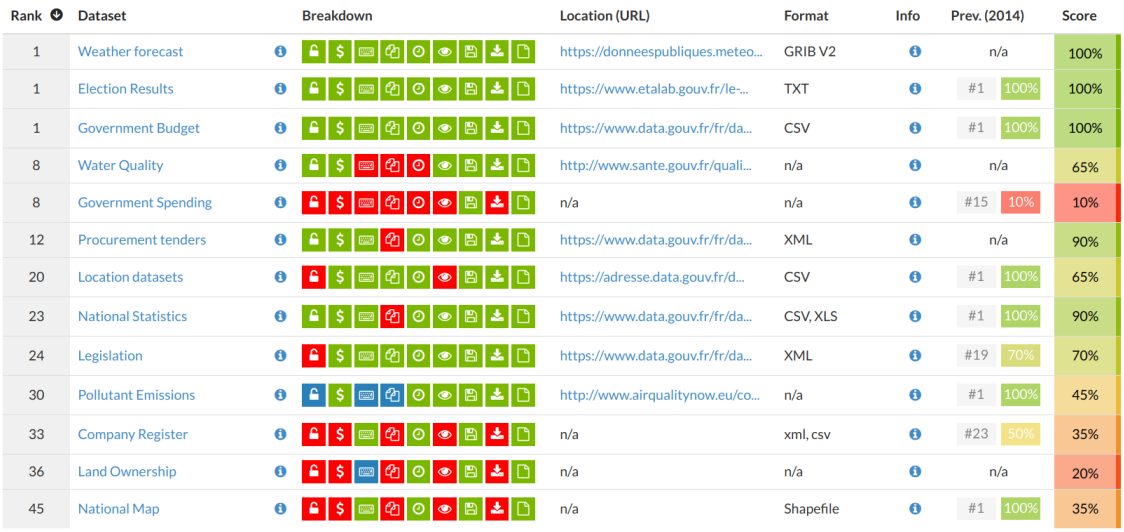
Le cas de la France

La France fait de réels efforts. Il ne lui reste plus qu'à faire une bonne psychanalyse pour régler ses problèmes vis à vis de l'argent pour arriver au niveau du premier. Notons que ce problème dépasse la France. Lorsque le ministre des finances italien a décidé de publier en 2008 les revenus et les impôts payés par ses citoyens, il a rapidement été désavoué et a du retirer l'information du Web.



Rank	Dataset	Breakdown	Location (URL)	Format	Info	Prev. (2013)	Score
1	Election Results		https://www.data.gouv.fr/fr/da...	XML		#14 90%	100%
1	Government Budget		https://www.data.gouv.fr/fr/da...	CSV		#11 90%	100%
1	Pollutant Emissions		https://www.data.gouv.fr/fr/da...	CSV		#13 60%	100%
1	National Map		http://professionnels.ign.fr/f...	TIFF ...		#14 70%	100%
1	National Statistics		https://www.data.gouv.fr/fr/da...	CSV		#13 75%	100%
1	Postcodes / Zipcodes		https://www.data.gouv.fr/fr/da...	CSV		#45 0%	100%
15	Transport Timetables		http://ressources.data.sncf.co...	GTFS		#4 80%	70%
16	Government Spending		n/a	n/a		#19 10%	10%
20	Legislation		https://www.data.gouv.fr/fr/da...	XML		#13 70%	70%
23	Company Register		http://www.sirene.fr/sirene/pu...	xml, csv		#34 40%	50%

FIGURE 7.8 – Détail du classement de la France – *source : Open Knowledge 2014*
rouge : mal, vert : bien, bleu : sans information



Rank	Dataset	Breakdown	Location (URL)	Format	Info	Prev. (2014)	Score
1	Weather forecast		https://donneespubliques.meteo...	GRIB V2		n/a	100%
1	Election Results		https://www.etalab.gouv.fr/le-...	TXT		#1 100%	100%
1	Government Budget		https://www.data.gouv.fr/fr/da...	CSV		#1 100%	100%
8	Water Quality		http://www.sante.gouv.fr/quali...	n/a		n/a	65%
8	Government Spending		n/a	n/a		#15 10%	10%
12	Procurement tenders		https://www.data.gouv.fr/fr/da...	XML		n/a	90%
20	Location datasets		https://adresse.data.gouv.fr/d...	CSV		#1 100%	65%
23	National Statistics		https://www.data.gouv.fr/fr/da...	CSV, XLS		#1 100%	90%
24	Legislation		https://www.data.gouv.fr/fr/da...	XML		#19 70%	70%
30	Pollutant Emissions		http://www.airqualitynow.eu/co...	n/a		#1 100%	45%
33	Company Register		n/a	xml, csv		#23 50%	35%
36	Land Ownership		n/a	n/a		n/a	20%
45	National Map		n/a	Shapefile		#1 100%	35%

FIGURE 7.9 – Détail du classement de la France – *source : Open Knowledge 2015*
rouge : mal, vert : bien, bleu : sans information

m.à.j. sur http://www.ricou.eu.org/e-politique.html

La CADA www.cada.fr

> *La loi n° 78-753 du 17 juillet 1978 reconnaît à toute personne le droit d'obtenir communication des documents détenus dans le cadre de sa mission de service public par une administration, quels que soient leur forme ou leur support.*

La Commission d'Accès aux Documents Administratif, CADA, peut être saisie suite à un refus de l'administration de transférer un document ou à une absence de réponse de plus d'un mois. Il s'agit en général de particuliers désirant un document les concernant (permis de construire d'un voisin, dossier médical d'un enfant...).

En moyenne une demande est traitée en 40 jours (cf rapport d'activité 2013). En 2013 56% des demandes ont reçu un avis favorable et 9% un avis défavorable, le reste étant incompétence de la CADA ou sans objet. Une fois l'avis favorable obtenu, l'administration concernée a un mois pour décider si elle suit ou pas l'avis de la CADA (dans seulement 4% des cas l'administration n'a pas suivit l'avis favorable de la CADA).

Si l'administration ne suit pas l'avis de la CADA, il est possible de faire appel au tribunal administratif.

Notons qu'une administration peut demander l'avis de la CADA. Ainsi la mairie de Grenoble a demandé début 2015 la possibilité et les modalités de mise en ligne, dans le cadre d'un projet d'open data, de l'ensemble des pièces communiquées par les associations subventionnées.

data.gouv.fr

> *data.gouv.fr contribue à rendre des comptes aux citoyens sur le fonctionnement de l'Etat et de ses administrations en permettant une plus grande transparence de leur fonctionnement.*

Les progrès de la France sont probablement dus au travail de la mission Etalab en charge de pousser les administrations à libérer leurs données. Or dans les ministères, mairies et autres organismes, le savoir (les données) est le pouvoir et toute demande d'information par un autre service est mal perçue. Alors ouvrir ses données...

Heureusement les mentalités changent comme semble le montrer les résultats même s'il reste du chemin à parcourir. Le site data.gouv.fr créé par la mission Etalab en est l'illustration. La figure 7.10 montre les jeux de données ouverts des plus gros fournisseurs avec la date de création x et celle de dernière mise à jour en y.

On voit que tous les ministères, villes ou administrations ne sont pas représentés, loin de là, mais l'important est l'évolution. Concernant l'introduction des bases de données dans le site de data.gouv.fr, on constate des périodes de création d'un grand nombre de base (un même x) avec des mis à jours pendant un certain temps (un trait vertical) puis des grandes périodes sans rien. Dans l'idéal on devrait avoir des bases de données sur la diagonale (elles représentent un événement comme le résultat d'une élection et n'ont pas à être mises à jour) et des bases sur la ligne du haut (elles sont maintenues à jour).

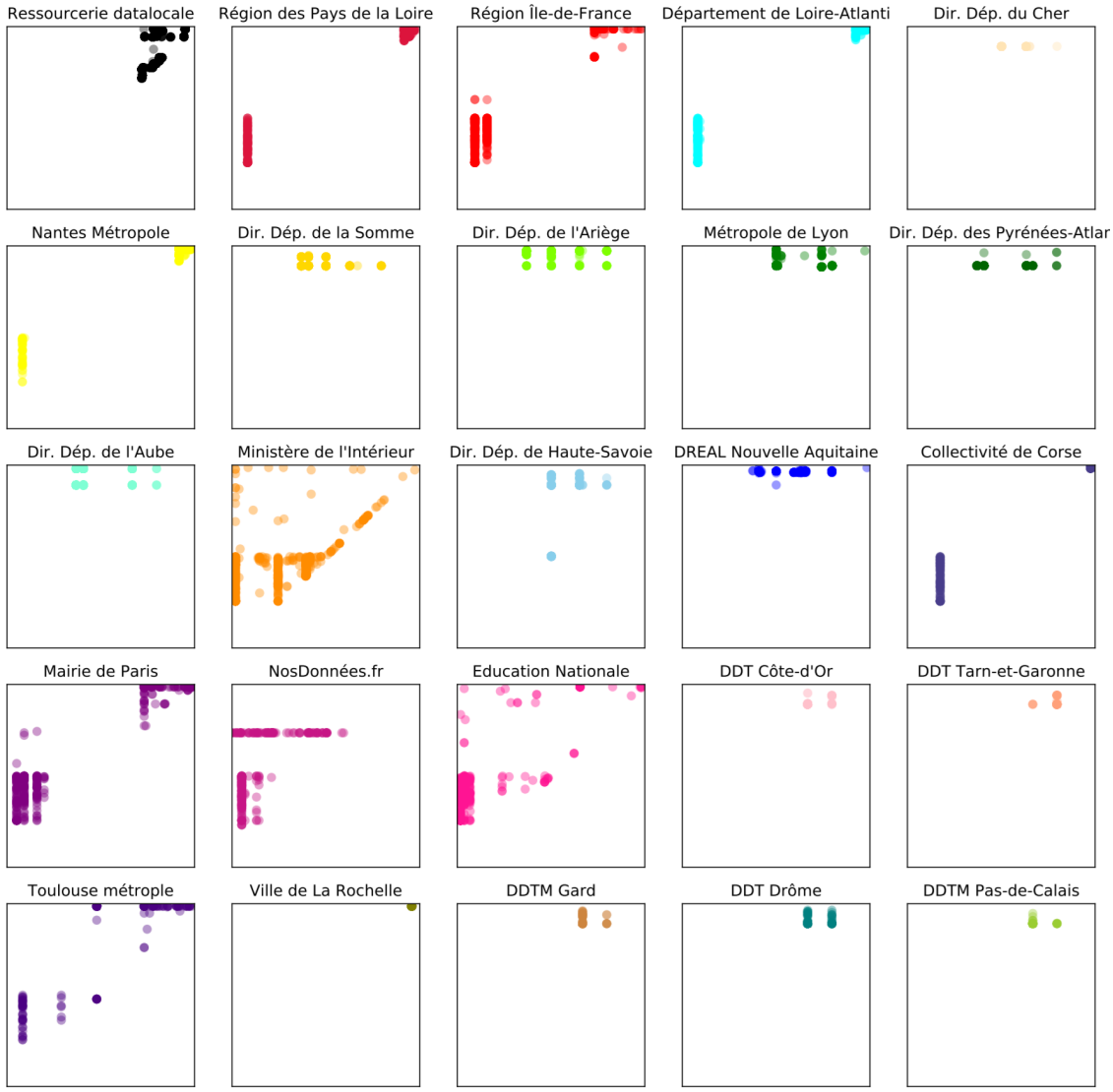


FIGURE 7.10 – Bases de données des 25 plus gros fournisseurs de data.gouv.fr

Un point = une base. En x la date de création (de 2014 à 2018), en y la date de dernière modification (même intervale)

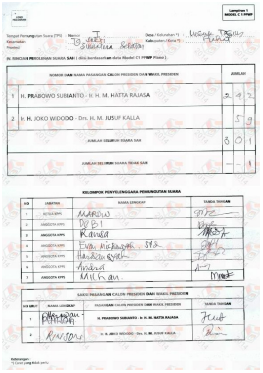
Une des failles de data.gouv.fr est la pérénité des jeux de données car le site ne propose que des liens et non des copies locales pour certains jeux. Cela permet à l'auteur de les faire disparaître, volontairement ou pas. Si une mairie ne publie sur son site web que les budgets des deux dernières années, même si data.gouv.fr référence tous les budgets précédents, les liens vers le site de la mairie ne sont plus effectifs et les données plus accessibles [16]. Il faudrait une bonne âme pour tout recopier, stocker et gérer les éventuels problèmes juridiques liés...

L'élection de 2014 en Indonésie

L'ouverture des données peut aussi être une arme démocratique lorsqu'un camp conteste le

16. Ce problème est connu, Etalab explique marcher sur des œufs et pratiquer la politique des petits pas.

résultat d'une élection. L'Indonésie a connue une longue dictature et l'élection de 2014 était certes libre mais un des deux candidats finaux était un militaire fils d'un ministre du dictateur Suharto. Aussi lorsque le soir de l'élection chaque camps a crié victoire, le risque de dérapage était sérieux.



L'Indonésie est un pays immense de 250 millions d'habitants. Les résultats des votes remontent des bureaux, aux villages, puis aux districts, aux arrondissements, aux villes, aux provinces pour finalement arriver au niveau national. Ces nombreuses étapes sont autant de possibilités pour falsifier les résultats. Aussi la commission électorale a décidé de publier sur son site web tous les compte-rendus du demi million de bureaux de votes afin que chacun puisse voir par lui même (cf image ci-contre).

Fort de ces données, quatre initiatives sont nées sur Internet pour compter toutes les voix et connaitre le résultat de l'élection avant que la commission ne l'annonce. Et ainsi, après un travail collectif impressionnant où les citoyens ont vérifié les données du site de la commission et entré tous les résultats locaux dans une base de donnée, ils ont pu avoir rapidement le résultat de l'élection soit entre 53,01 et 53,15 % pour Jokowi avec une marge d'erreur de 1,19 %. Ce travail a permis à la commission d'annoncer deux semaines après les résultats sans craindre les pressions. Jokowi a obtenu officiellement 53,15% des voix.

7.2.2 Le droit à l'oubli

La transparence et la vie privée vont de pair dès lors que l'on parle de personnes. Sans revenir sur la surveillance massive que mettent en place les États, il existe une autre *faille* dans la vie privée sur Intenet, celle de la mémoire implacable d'Internet. Ce que vous publiez aujourd'hui sera toujours visible, y compris le jour où vous n'aurez plus trop envie que cela le soit.

La question est donc de savoir si une personne peut retirer son passé d'Internet, y compris son passé public. Il s'agit du droit à l'oubli qui existe déjà pour les personnes condamnées qui ont purgées leur peine.

La cours européenne de justice a décidé que oui dans son arrêt du 13 mai 2014 [17] :

> *l'exploitant d'un moteur de recherche est obligé de supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages web, publiées par des tiers et contenant des informations relatives à cette personne, (...) même lorsque leur publication en elle-même (...) est licite.*

Notons que l'arrêt ne porte que sur le référencement par les moteurs de recherche et non pas sur l'information elle même. Le cas qui a déclenché cette arrêt est celui d'une personne, Mario Costeja González, qui désirait que Google ne référence plus une condamnation le concernant publiée sur un journal officiel [18]. Il est difficile de demander que les journaux officiels ne soient

17. http://eur-lex.europa.eu/legal-content/FR/TXT/?qid=1429715845859&uri=CELEX:62012CJ0131
18. effet Streisand réussi !

plus accessibles sur Internet mais il a obtenu que Google de référence plus cette condamnation.

Comme il s'agit de protéger la vie privée des individus, les entreprises sont exclues de cet arrêt.

Enfin la cours a décidé que la véracités des faits est moins importante que la protection de la vie privée. Cependant elle a ajouté que l'intérêt public d'une information doit aussi être pris en compte :

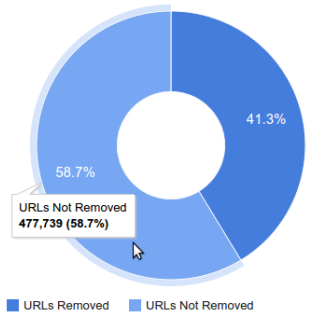
> *Si, certes, les droits de la personne concernée protégés par ces articles prévalent également, en règle générale, sur ledit intérêt des internautes, cet équilibre peut toutefois dépendre, dans des cas particuliers, de la nature de l'information en question et de sa sensibilité pour la vie privée de la personne concernée ainsi que de l'intérêt du public à disposer de cette information, lequel peut varier, notamment, en fonction du rôle joué par cette personne dans la vie publique.*

On imagine l'embarra des moteurs de recherches devant appliquer cet arrêt.

Après des appels à des comités de sages, les procédures de désindexation de pages portant atteintes à la vie privée d'individus ont été mises en place dans les plus grands moteurs de recherche :

— https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=fr
— https://www.bing.com/webmaster/tools/eu-privacy-request

Après un an d'activité, voici les statistiques de Google avec les raisons invoquées pour retirer des pages de son moteur de recherche :



Type de demande	% d'URL
Atteinte à la vie privée	58,7%
Atteinte à la réputation	11,2%
Atteinte à l'image	4%
Usurpation d'identité	3,2%
Procédure pénale	3,1%
Atteinte à la présomption d'innocence	1,3%
Homonymie	1%
Personne décédée	0,7%
Autres	16,9%
Total général	**100%**

FIGURE 7.11 – Désindexation des données privées par Google
source : Google et ITR News – mai et juin 2015

Notons que cette possibilité d'être désindexé de moteurs de recherche pour protection de la vie privée n'existe qu'en Europe. Soit que l'Europe est précurseur, soit que la ligne de séparation entre la vie privée et la transparence n'est pas la même suivant les pays.

7.3 Le citoyen contre-pouvoir

Si la transparence est nécessaire au niveau gouvernemental pour assurer une démocratie efficace, il est important que les citoyens n'oublient pas que sans eux il n'y a pas de démocratie, sans leur vote bien sûr mais surtout sans leur surveillance, sans leur participation associative, sans leurs critiques aussi.

FIGURE 7.12 – L'ancien journal semi-collaboratif Rue 89

Avec Internet le citoyen électronique devient un commentateur de l'actualité écouté (ou du moins audible), un analyste, parfois un penseur. Il peut aussi être un contrôleur, une mémoire ou un opposant. Le chapitre sur la communication souligne le nombre de nouvelles formes de média qui permettent à chacun d'exister et de transmettre à tous ses pensées.

Par contre le citoyen internaute n'est pas encore souvent consulté et n'a pas accès à la prise de décision [19]

7.3.1 Le contrôle des élus

On a déjà vu [20] déjà le poids des blogs en politique aussi regardons un aspect moins courant et peut-être plus intéressant pour permettre aux électeurs de choisir leur candidat : le contrôle des élus. Il ne s'agit plus d'écouter des promesses mais de regarder les actions.

Les institutions mettant de plus d'information sur Internet, il devient possible de suivre l'activité des élus. Cela a permis le développement d'outils qui extraient l'information, la structurent et la présentent graphiquement. Ainsi on a :

— des outils de suivi de l'action (qui vote quoi au parlement, qui est présent...),

19. sauf erreur de ma part et je serais ravi de l'apprendre.
20. cf chapitre sur la communication

— des outils de suivi des promesses (particulièrement adapté au président de la république),
— des outils de vérification des dires (utile en campagne lorsque les candidats annoncent tout et n'importe quoi pour déstabiliser l'adversaire ou convaincre le gogo).

FIGURE 7.13 – Suivi du travail des sénateurs et des députés
source : http://www.nossenateurs.fr/ et http://www.nosdeputes.fr/

Ces outils sont le plus souvent l'œuvre de bénévoles qui vont chercher l'information perdue au fin fond des sites web concernés. Si ce travail permet de montrer ce qu'il est possible de faire, la pérennité de ces sites n'est malheureusement jamais garantie (le premier site du genre en France, www.mon-deputes.fr, a décroché en 2013 après plus de 15 ans d'archivage).

Parmi ces sites outils notons

— nosdeputes.fr et nossenateurs.fr pour suivre les élus des deux chambres, cf figure 7.13,
— lafrabriquedelaloi.fr pour décortiquer le travail législatif dans son ensemble, cf figure 7.14,
— l'étude du lobying à l'Assemblée Nationale sur le site de Regards Citoyens,
— Thumbs of Europe qui présente en détail des projets de loi, offre la possibilité à l'internaute de voter et compatabilise les votes des députés européens.

FIGURE 7.14 – Présentation graphique compréhensible de l'évolution d'une loi
source : http://www.lafabriquedelaloi.fr/

Le crowdsourcing à la rescousse

Le principal problème pour suivre l'activité des élus est, outre le manque d'information, la présentation non structurée de l'information, écrite pour être lue par des humains (voire pour ne pas être trop lue) et ainsi difficilement récupérable automatiquement [21]. Le collectif Regards Citoyens a indiqué passer les ¾ de son temps à récupérer les données et à lutter contre

21. l'exemple extrême est l'information sous forme d'images, si un camembert est pratique pour un humain, c'est illisible pour un programme qui préfère les chiffres bruts.

la mauvaise volonté de l'administration [22].

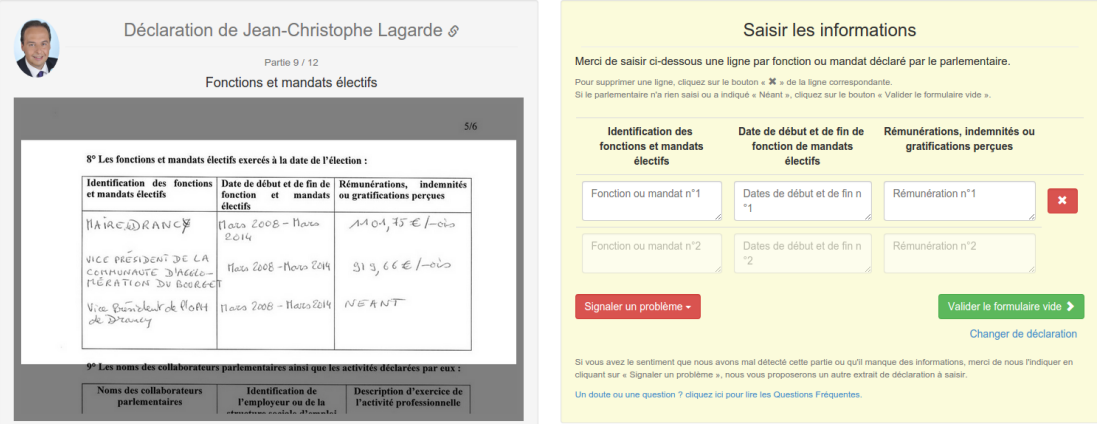


FIGURE 7.15 – Extraction des données manuscrites des déclarations d'intéret des élus
source : http://regardscitoyens.org/interets-des-elus/
(les députés ont bloqué la publication de leur patrimoine, seules les déclarations d'intérêt sont visibles)

Aussi pour lutter contre la mauvaise volonté de l'administration on utilise le *crowdsourcing* à savoir les petites mains de plein de bénévoles qui vont structurer l'information. Lorsque la loi sur la transparence a imposé aux élus de déclarer leur patrimoine et les possibles conflits d'intérêt que leur élection posait [23], l'administration en charge de la collecte et de la diffusion de l'information à demandé une déclaration manuscrite et à déposé les scans sur son site web. Un scan n'étant pas lisible par un ordinateur, cela interdit tout analyse statistique ou une recherche autre que manuelle [24]. En réaction, Regards Citoyens a mis en place un site web qui permet aux internautes d'entrer dans une base de données les informations écrites par les élus, cf figure 7.15. Les 11 095 éléments ont rapidement été numérisés par 7924 citoyens (en fait ils ont numérisé 86 239 fois, chaque élément étant proposé plusieur fois pour obtenir un résultat optimal).

Ce travail est un véritable gaspillage d'énergie lorsque l'administration a ou pourrait avoir l'information structurée mais ne la diffuse pas. Heureusement l'air du temps et la poussée d'Etalab font bouger les choses vers l'ouverture de plus en plus de données détenues par l'administration.

Les promesses n'engagent que ceux qui y croient

Le domaine des promesses est un travail plus délicat car une évaluation humaine est pratiquement toujours nécessaire. Les politiciens aiment promettre et aiment qu'on oublie ces promesses. Avec Internet, les chances pour qu'un individu se charge de faire le suivi et qu'il le

22. par exemple la mairie de Marseille qui refuse de donner l'adresse de ses bureaux de vote et qui le fait finalement, sous la contrainte de la CADA, via un document manuscrit.
23. certains élus appelle cela la tyrannie de la transparence. On a retrouvé cette expression lorsque le président du sénat a voulu mettre en place des fiches de présence pour les sénateurs.
24. ainsi avoir la liste des élus qui gagnent plus de 100 k€ ou qui emploi telle personne devient un long travail qui devrait en décourager plus d'un.

publie sont non négligeables. Ainsi le feu site www.observatoire-politique.fr a listé l'ensemble des promesses du président de la république Sarkozy et a noté au fur et à mesure celles tenues, en cours, non tenues ou non abordée. Le Figaro fait le même travail avec le président Hollande [25] et le site luipresident.fr le fait pour le président Macron (et l'a aussi fait pour François Hollande)

Concernant les promesses, une autre caractéristique d'Internet peut être exploitée, à savoir sa mémoire. Une promesse municipale filmée et déposée sur YouTube peut ressortir à tout moment. Une annonce sur un site web sera enregistrée par Internet Archive et restera visible longtemps après avoir été effacée du site web. Il est aussi possible pour un citoyen d'enregistrer les évolutions d'un site pour les ressortir aux élections suivantes.

L'art du mensonge

FIGURE 7.16 – Vidéo répondant au discours de Sarkozy sur la recherche
source : http://www.youtube.com/watch?v=iyBXfmrVhrk

Enfin concernant la véracité des dires d'un élu, là encore Internet joue un rôle important. Nous avons pris l'habitude de demander à Google ou à Wikipédia une information lorsque nous avons un doute, il est donc devenu très simple de faire de même lorsqu'on écoute un discours. Mais on peut aussi attendre 24h et espérer trouver directement une analyse factuelle du discours s'il est important (on peut aussi faire cette analyse et la déposer sur Internet). Un exemple d'analyse qui a eu son succès concerne le discours du 22 janvier 2009 du président de la république sur la recherche, cf figure 7.16. Les auteurs ont simplement inséré dans le discours des panneaux soulignant les mensonges.

Bien sûr la question est de savoir si tout cela peut avoir un impact sur notre démocratie. Rien ne prouve qu'il soit pénalisant, pour un homme politique, que l'on souligne ses mensonges ou que l'on comptabilise les promesses non tenues. La notion de camps et la possibilité de trouver les mêmes erreurs dans l'autre camps peuvent suffire à bloquer toute évolution vertueuse et à figer les électeurs dans leur camps. Enfin l'histoire à montré que les élus condamnés et rendus inéligibles pendant une période retrouvent souvent leur poste.

25. http://www.lefigaro.fr/assets/promesses-hollande/Promesses-Francois-Hollande.html

Il est incontestable que ce sont plutôt des menteurs éhontés et récidivistes qui parviennent à être élus aux plus hautes responsabilités.

Thomas Guénolé, auteur du Petit guide du mensonge en politique.

7.3.2 Avis de citoyen

Le citoyen électronique n'est pas que comptable des actions des élus, il est le plus souvent émetteur d'avis. Le chapitre sur la communication a montré le poids des blogs et des sites web collaboratifs, il existe aussi des site où les citoyens se comptent, des sites de pétitions destinés à faire bouger les dirigeants.

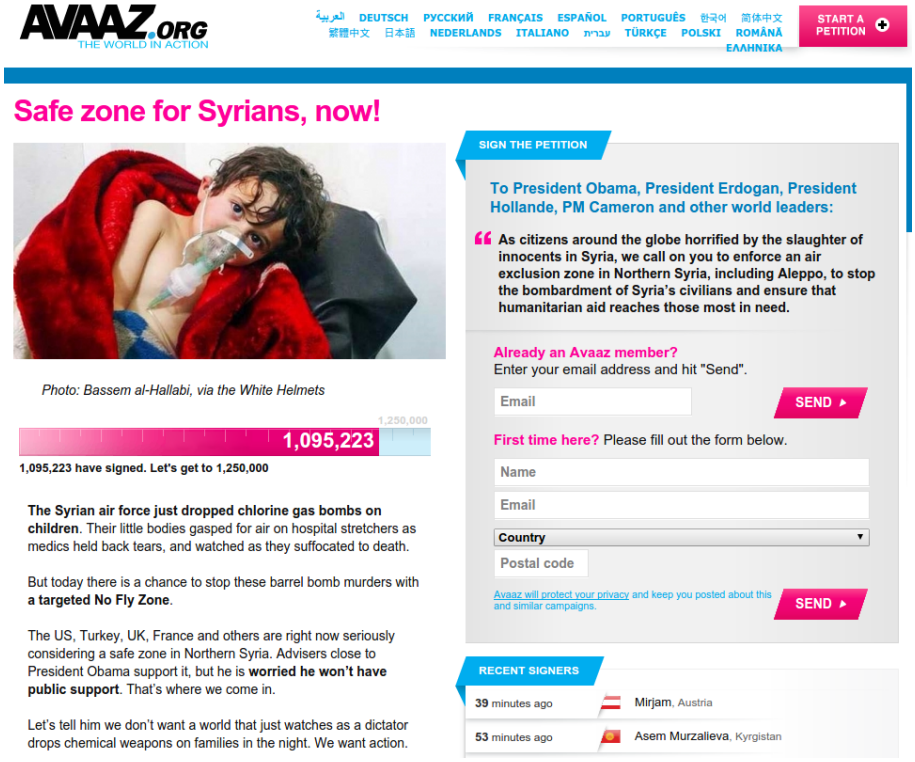


FIGURE 7.17 – Pétition d'Avaaz - 2015

Parmi ces sites, les plus importants en 2015 sont Avaaz et change.org. Ces sites obtiennent régulièrement plus d'un million de voix pour des pétitions.

Le fonctionnement est a priori simple, chaque internaute peut lancer une pétition et ensuite les internautes apportent leur soutien en signant virtuellement la pétition, cf figure 7.17. Pour créer le buzz nécessaire à un succès, les sites mettent en valeur les pétitions qui leur semblent les plus intéressantes, envoient des mails aux anciens signataires du site, utilisent les médias pour faire monter la sauce et finalement transmettent les signatures aux décideurs afin qu'ils prennent en compte la *volonté populaire*. Bien sûr les sites affichent leurs succès afin de motiver les internautes à continuer de participer.

Il s'agit donc du vieux système de la pétition modernisé qui utilise pleinement l'interactivité

d'Internet pour lever en quelques semaines des centaines de milliers voire des millions de signatures, ce qui suffit pour réagir à chaud sur un sujet de société et convaincre des élus.

Cependant on connait les biais des pétitions :

— le choix du sujet,
— la formulation du texte de la pétition,
— le décompte des signatures.

Concernant les sujets des pétitions, les sites peuvent tout à fait choisir ceux qu'ils acceptent ou même simplement ceux qu'ils mettent en avant. Par exemple le site d'Avaaz ne propose qu'une poignée de pétitions quand change.org en propose des centaines alors que les deux sites permettent à tout internaute de lancer sa pétition. Avaaz est par ailleurs largement critiqué par des sites aux extrêmes de l' échiquier politique d'être un instrument de propagande en proposant des sondages très orientés politiquement (tendance Bobo disons).

Concernant la rédaction du texte, regardons le cas du sondage sur l'interdiction aérienne en Syrie, cf figure 7.17. A priori il s'agit d'une action humanitaire puisqu'il s'agit d'empêcher les avions du régime de bombarder la population. Mais interdire un espace aérien au dessus d'un autre pays implique d'y envoyer des chasseurs pour faire respecter l'interdiction, détruire la DCA pour éviter de perdre des chasseurs et donc de déclarer la guerre. Habilement la pétition évite le mot guerre.

Enfin la comptabilité des votes sur Internet est d'autant plus difficile sur Internet qu'il est très simple de créer des faux comptes. Cependant ni Avaaz, ni change.org ne permettent de télécharger la liste des signatures même anonymisées pour que chacun puisse évaluer la qualité des signature. Pourtant l'analyse des données, le début des adresses IP et l'heure à laquelle a été signée une pétition serait pourtant déjà une indication sur la valeur des signatures.

Pour finir la critique, qui ne doit pas cacher le fait que ces sites sont de très beaux instruments démocratiques, regardons le modèle financier de ces sites. Leur chiffre d'affaire dépasse les 10 millions de dollars et leur dirigeants sont très bien payés au contraire de l'image des bénévoles qui tractent dans les marchés. Avaaz a commencé avec des aides de fondations dont celle du milliardaire Georges Soros et maintenant vit des dons des internautes. Change.org vend sa base de signataires aux ONG et l'accès au site web pour leurs pétitions. On peut dire qu'Avaaz et Change.org sont de belles startups.

Vote électronique

Peut-on avoir confiance dans un système de vote électronique ?

Pour répondre positivement à une telle question il est nécessaire d'avoir un système au moins aussi fiable que le système actuelle du bulletin papier. De plus il faut que le système soit assez simple pour que tout citoyen puisse vérifier par lui même que le vote est valide.

Actuellement les ordinateurs de votes utilisés dans certains bureaux de vote français ne répondent pas à ces prérequis. Pire, il a été prouvé qu'il est possible de falsifier les résultats et de savoir qui vote pour qui. Suite à ces révélations, les Pays-Bas sont repassés au vote papier, l'Allemagne a fait de même mais pas la France, malgré l'avis négatif du Sénat.

Pourtant il semble possible de construire un ordinateur à voter qui respecte toutes les conditions voulues. L'algorithme appelé Bingo Vote en est un exemple.

Mais lorsqu'il s'agit de voter à distance, par Internet, alors il semble impossible d'empêcher la triche. Par exemple comment interdire l'achat de vote puisque celui qui vous achète peut vous regarder voter voire prendre votre carte d'électeur et voter pour vous (cf encart ci-dessous sur l'identité électronique).

Référendum d'initiative populaire

L'étape suivante après la pétition est le référendum d'initiative populaire. Il existe dans différents pays avec différents pouvoirs. En Suisse et en Californie une proportion définie des électeurs [26] peut soumettre un texte aux votes des électeurs. Ce texte peut ensuite devenir loi. En Italie les lois votés par le parlement peuvent être abrogée par un référendum d'initiative populaire.

En France, le président Sarkozy a fait modifier en 2008 l'article 11 de la constitution [27] pour permettre le référendum d'initiative populaire mais en limitant nettement l'aspect populaire puisque l'initiative doit venir de 20 % des membres du Parlement et être supportée par 10 % des électeurs inscrits (un peu plus de 4,5 millions de personnes). De plus le référendum ne peut porter que sur quelques sujets bien limités, les sujets de sociétés en étant écartés. Il est difficile de vraiment parler de référendum d'initiative populaire, il s'agit surtout de permettre à l'opposition parlementaire de demander l'avis du peuple sur un sujet qui lui semble assez important pour mettre en branle cette machinerie.

On note l'écart avec la Suisse qui ne demande que 100 000 signatures sur plus de 5 millions d'électeur, donc moins de 2 % du corps électoral, et aucun soutient de parlementaires. Avec son système dit de votation, la Suisse soumet trois ou quatre référendums par an à ses électeurs.

26. 100 000 en Suisse, 8% des électeurs en Californie
27. Les décrets d'application on été publiés fin 2013 pour une mise en application au 1er janvier 2015.

Identité électronique

Internet n'a pas de méthode de base pour prouver son identité. Dans le cas d'un référendum et même d'une pétition c'est un problème crucial.

Avec la cryptographie [a] il est possible de signer une action et donc de prouver son identité dès lors que votre signature a été validée par quelqu'un en qui tout le monde à confiance. Ce quelqu'un pourrait être l'État.

La Belgique a mis en place un tel système d'authentification en 2009 en intégrant une puce sur les cartes d'identité [b] [c]. Cette puce peux être interrogée à distance sur Internet et il est donc possible de savoir que la personne connectée à un site web est bien celle qu'elle prétend être (sauf si elle a prêté sa carte et le mot de passe). Cette carte électronique est déjà utilisée par l'administration mais aussi pour signer des documents, enregistrer un achat important comme sa maison, s'inscrire à une association et bientôt voter. L'Estonie a aussi une telle carte et l'utilise déjà pour voter par Internet.

Mais tout n'est pas rose car les risques de sécurité des cartes électroniques sont réels : surveillance, usurpation d'identité ou plus simplement le piratage des données.

a. cf le chapitre 1 sur les aspects techniques en particulier sur PGP.
b. cette solution matérielle est plus lourde à mettre en place que la solution logiciel. De plus elle nécessite un lecteur sur le PC des utilisateur mais elle mieux maitrisée par la population habituée aux cartes de paiement.
c. http://eid.belgium.be/

FIGURE 7.18 – Y a-t-il trop d'initiatives populaires en Suisse ?
source : Mix et Remix pour l'émission suisse Infrarouge

7.4 Changement de démocratie

Le mode de gouvernance utilisé au sein d'une société dépend de nombreux paramètres dont le paramètre technologique. Les outils techniques permettent aux dirigeants de gouverner, de contrôler le peuple et inversement, au peuple de s'informer, de communiquer et de choisir ses dirigeants, quitte à passer par une révolution.

L'arrivée d'Internet est, de ce point de vue aussi, une étape importante. Nos démocraties sont déjà largement influencées par cet outils, cf chapitre sur la communication et la section sur la surveillance de masse. L'ouverture des données et les révolutions arabes du printemps 2011 sont d'autres exemples de cet impact d'Internet.

La question qui suit est comment aller plus loin, comment utiliser Internet pour améliorer notre démocratie. Notre système actuel de démocratie représentative date d'une époque où les communications était nettement plus difficiles et rendait impossible une consultation directe du peuple. D'autre part il n'est pas certain que les révolutionnaires de 1789 aient voulu mettre en place une telle démocratie. Le discours de l'un de ses penseurs en témoigne clairement :

> *Les citoyens qui se nomment des représentants renoncent et doivent renoncer à faire eux-mêmes la loi ; ils n'ont pas de volonté particulière à imposer. S'ils dictaient des volontés, la France ne serait plus cet État représentatif ; ce serait un État démocratique. Le peuple, je le répète, dans un pays qui n'est pas une démocratie (et la France ne saurait l'être), le peuple ne peut parler, ne peut agir que par ses représentants.*
>
> Discours du 7 septembre 1789 de l'abbé Sieyes

Aujourdhui la situation des outils de communication a radicalement changée mais il semblerait que les idées de la démocratie représentative soient toujours bien présentes. Malgré le rejet de plus en plus fort du système politique actuel dans les démocraties occidentales, malgré les propositions d'académiques pour réformer le système, malgré les rares tentatives locales, la classe politique actuelle ne désire pas scier la branche sur laquelle elle est assise. Si en France la monté régulière du Front National inquiète la classe politique traditionnelle, cela ne semble pas encore suffisant pour réformer notre démocratie en profondeur voire même tester en grandeur nature des démocraties alternatives.

Parmi ces alternatives regardons la démocratie liquide et la démocratie délégative.

7.4.1 La démocratie liquide

Le principe de la démocratie liquide est de permettre de voter directement ou pas et si on désire transmettre sa voix, de pouvoir la transmettre à qui on veut. À cela s'ajoute la possibilité de transmettre les voix que l'on a reçues à celui à qui on donne notre voix. Cela ressemble au vote par procuration sauf que l'on peut avoir plus d'une voix et surtout cela peut se faire à plus d'un niveau. La figure 7.19 montre comment certains électeurs délèguent leur voix et comment ceux qui n'ont pas délégué leur voix prennent finalement part au vote.

D'un certain point de vue il s'agit d'une démocratie directe où ceux qui le désirent peuvent se retirer de la prise de décision sans que leur voix ne compte plus.

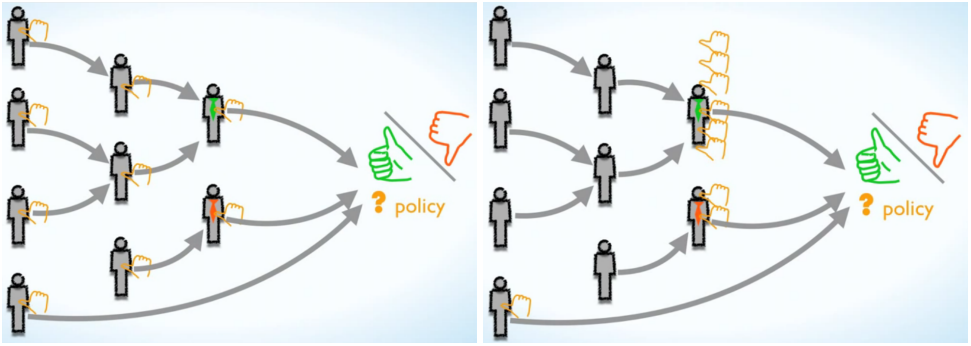


FIGURE 7.19 – Vote en démocratie liquide
source : Jakob Jochmann 2012, https://www.youtube.com/watch?v=fg0_Vhldz-8

Pour fonctionner à large échelle, un tel système doit utiliser une infrastructure informatique lourde qui permette de savoir qui vote pour qui afin d'informer chacun des voix dont il dispose et pouvoir faire les calculs lors des votes.

La pratique n'est pas aussi simple qu'on pourrait l'imaginer.

Mise en œuvre au parti pirate

Le parti pirate allemand a choisi d'utiliser ce principe de démocratie qui correspond plus à ses idéaux que la démocratie représentative. Il a, pour cela, développé une plateforme informatique appelée LiquidFeedBack qui permet à chacun de soumettre une proposition de vote, de donner son avis, de déléguer sa voix ou de voter.

Le résultat est que cela ne fonctionne pas à savoir seule une parti des membres l'utilise ce qui revient à dire que la majorité s'abstient d'exprimer ses choix. Le parti pirate français a déployé le même système mais il ne l'utilise pas, la sauce n'a jamais prise. Le parti pirate belge a vécu les mêmes problèmes et voici l'analyse d'un de ses membres :

> *En Allemagne, cette démocratie liquide a été installée par le biais d'une application web du nom de "LiquidFeedBack". Cette application permet à tout un chacun de faire des propositions, de les discuter, et de voter ou de déléguer son vote. Pleine de qualités, cette application a aussi ses défauts : son aspect non convivial et sa complexité d'implémentation. Mais surtout, son utilisation a créé une sorte de caste. En effet, si toutes les décisions sont prises via cette application, alors, et ce n'est pas une lapalissade, ceux qui ne l'utilisent pas ne participent pas à la décision. Or, la réalité, c'est que tout le monde n'est pas sur internet. Plus, tout le monde n'est pas capable, comme un informaticien, de faire abstraction de l'esthétique et de l'ergonomie pour utiliser un outil. Est ainsi apparu une oligarchie : les utilisateurs de LiquidFeedBack.*
>
> http://lepartipirate.be/tentative-dautopsie-dun-pseudo-naufrage

On voit donc que le premier inconvénient est la complexité de la chose. Un tel système informatique demande une ergonomie parfaite pour que les électeurs utilise. Ce travail est d'autant

moins évident que LiquidFeedBack introduit le principe d'amélioration des propositions ce qui permet à tout le monde de donner son avis et donc augmente la complexité du système.

Ceux qui utilisent les forums savent que des débats en ligne peuvent facilement dégénérer. Vouloir faire participer des électeurs à l'élaboration d'une proposition de vote est louable mais difficile. Les expériences de démocratie participative lors des appels au public pour les grands projets en France sont des processus lourds et encadrés par des animateurs spécialisées. Cela peut se justifier économiquement pour des projets qui se chiffrent en milliards, ce n'est n'est pas possible pour chaque prise de décision au sein de notre société.

Un autre point est la saturation. Autant un électeur peut prendre le temps de réfléchir à un problème de société de temps en temps, autant il ne peut pas le faire à plein temps, ni même à mi temps et probablement même pas une fois par semaine. Donc même avec un outil parfait, il est illusoire d'espérer qu'il sera massivement utilisé pour voter ou déléguer sa voix pour chaque prise de décision si l'on a besoin de plus d'une décision par semaine (ce qui est déjà le cas d'une municipalité).

Et pourtant on a vu par le passé des idées considérées comme irréalisable devenir réalité, en particulier sur Internet. Aussi de nombreuses personnes cherchent à rendre plus simple le système et développent de nouveaux logiciels. L'un des plus abouti en 2014 est getOpinionated développé par le parti pirate belge.

7.4.2 Mélanger les systèmes démocratiques

Il est possible de mélanger les types de démocratie pour essayer d'améliorer le système. Le tableau 7.1 montre les possibilités qu'offrent la démocratie représentative, participative, liquide et directe à l'électeur.

	représentatif	participatif	liquide	direct
élaboration du texte à voter	✗	✓ [28]	✓	✓
prise de décision, vote du texte	✗	✗	✓	✓
délégation de vote	✓	✓	✓	✗
choisir librement son représentant	✗ [29]	✗section 7.4.2	✓ [30]	✗
fréquence de consultation [31]	6 ans	mensuel	quotidien	quotidien

TABLE 7.1 – Possibilités d'un électeur suivant le système démocratique

On note que le système représentatif exclu relativement le citoyen de la vie politique [32]. À l'inverse la démocratie directe en demande (*a priori*) trop.

28. donne un avis seulement dans le cas de consultation ou concertation auprès du public qui sont les modes les plus courants. De plus seuls certains textes sont présentés, en fonction de la loi ou de la volonté des élus.
29. possible dans certains cas avec liste libre, en France pour les petites municipalités par exemple
30. presque, sachant que la personne à qui on a donné sa voix peut la transmettre.
31. estimation pour une municipalité
32. lequel lui rend bien en n'allant plus voter.

Le délégatif, entre le représentatif et le liquide

En partant de la constatation que seules certaines personnes sont intéressées par la politique mais que tout le monde aime bien donner son avis quand il veut, que le système des *followers* a beaucoup de succès tant sur Twitter que sur Facebook, que l'on ne trouve pas toujours un représentant acceptable parmi les candidats proposés et que notre représentant idéal pour la culture n'est peut-être pas le même que pour les aspects de sécurité, on peut penser à un système qui permette :

— de donner sa ou ses voix à qui on veut comme pour la démocratie liquide,
— de voter quand on veut et ainsi pouvoir changer son vote quand on veut,
— de communiquer régulièrement avec son représentant (dans les deux sens),
— d'avoir un vote par thématique (thématiques à définir).

Avec le système de délégation suivant le principe de la démocratie liquide, on a

— les *électeurs*,
— les *délégués* qui sont les personnes qui ont reçu des voix et qui les ont transmisses. Parmi eux on peut appeler les *grands électeurs* ceux qui disposent d'un pourcentage significatif des voix,
— les *élus* ou *représentants* qui ont le nombre de voix nécessaire et qui n'ont pas transmis les voix qu'ils ont reçues.

Un tel système remplirait ainsi les cases du tableau 7.1 :

	délégatif
élaboration du texte à voter	✗
prise de décision, vote du texte	✗
délégation de vote	✓
choisir librement son représentant	✓[33]
fréquence de consultation	libre

TABLE 7.2 – Possibilités d'un électeur suivant un système alternatif dit délégatif

Il est possible de fixer le nombre d'élus de différentes façons :

— un nombre fixe d'élu qui correspond aux besoins de la charge,
— un seuil en pourcentage de voix,
— un mélange des deux cas précédents (toute personne au dessus d'un certain seuil mais avec un minimum de tant d'élus).

Notons qu'il est possible d'indiquer à chaque électeur quel est son élu (même s'il a voté pour une autre personne). Il peut ainsi vérifier que les prises de positions de ce dernier dans l'élaboration d'un texte lui conviennent.

Le fait qu'il y ait des intermédiaires entre les électeurs et les élus devrait fluidifier la com-

33. avec la même contrainte que pour la démocratie liquide

munication de haut en bas comme de bas en haut, chaque représentant ayant à cœur de tenir informer ceux qui ont voté pour lui et désirant comprendre son représentant. Comme chaque représentant aura un nombre de voix relativement réduit, y compris l'élu qui n'aura que quelques grands électeurs, il lui sera possible d'entretenir une communication régulière.

Une inquiétude naturelle avec un tel système est sa stabilité sachant qu'un électeur peut changer son vote quand il veut. Cependant la majorité devrait voter pour un proche ou une personne en laquelle elle croit vraiment ce qui devrait stabiliser le système. De plus la façon de désigner les élus peut aussi améliorer la stabilité. Par exemple on peut choisir qu'une personne est élue lorsqu'elle a le plus grand nombre de voix depuis un mois sans discontinuité. Ainsi remplacer la personne en poste demande d'avoir une marge de voix suffisante pour contrer les variations qui feraient que l'on passe second, premier, second trop souvent.

En pratique

Un système de vote permanent dont les résultats sont calculés par un ordinateur central donne envie d'avoir des outils numériques. Ainsi on peut imaginer voter depuis son ordinateur ou son téléphone portable. Ce système est acceptable dès lors qu'il est possible de garantir le secret du vote et la fiabilité des résultats. Il pose quand même le problème du vote sous contrainte comme on verra ci-dessous.

FIGURE 7.20 – Prototype d'interface pour un vote délégatif au sein d'un laboratoire

Si une interface de vote est simple à imaginer, cf figure 7.20, on a vu avec la démocratie liquide l'importance de son ergonomie. Aussi il est important de bien présenter les résultats courants, la délégation des votes, le suivi des actions de leur élu, les avis des grands électeurs... Le vote étant permanent, l'électeur doit toujours avoir en main les éléments qui puissent lui permettre de revoir son vote.

Le lien continu entre les citoyens et leurs élus serait probablement la plus grande *révolution* de ce système.

Les failles du système

La principale faille d'un système qui fait intervenir la démocratie liquide est la possibilité de perte du secret du vote. Il ne s'agit pas d'une faille pire que celle actuellement acceptée dans les bureaux de vote qui disposent d'ordinateur pour voter [34] et non d'urne papier, mais cela reste une faille gênante pour un système démocratique.

Les besoins pour qu'un système soit acceptables semble être :

— la garantie du secret du vote si demandé,
— la possibilité de vérifier des résultats du vote à tout niveau l'arbre des votes.

La vérification du vote peut être partielle, statistique, réservée à certaines personnes sous certaines circonstances. Le but est de vérifier que chaque voix est bien prise en compte comme elle l'a demandé et que les transferts de voix ont été effectué correctement. Il ne s'agit donc pas seulement de valider que la personne élue est la bonne.

Avec un système de vote permanent et la délégation des voix, il est nécessaire d'utiliser un ordinateur pour calculer les résultats. Dès lors qu'un ordinateur peut calculer le nombre de voix dont dispose chaque votant, cela implique qu'il sait qui donne sa voix à qui sauf à pouvoir chiffrer les données transmises de telle sorte que l'ordinateur puisse calculer les résultats sans pour autant pouvoir inférer qui a voté qui. On sent bien que si l'ordinateur n'a que les numéros d'électeur et que l'on considère que cette information est secrète, il sera quand même possible de reconstruire, au moins partiellement, la correspondance entre les numéros d'électeurs et le personnes en étudiant l'arbre des votes, le réseau social du corps électoral, les dates de vote, etc.

Heureusement les progrès en cryptographie, en particulier dans le domaine de la cryptographie homomorphique, permettent d'espérer pouvoir résoudre ces problèmes.

Un autre problème concerne le vote sous contrainte ou l'achat de vote. Si je peux voter depuis chez moi sur Internet, alors rien ne garantit qu'il n'y a pas une personne à coté de moi qui dirige mon vote. C'est le même problème que pour le vote par correspondance qui est actuellement utilisé pour les français vivants à l'étranger. La seule garantie actuelle de pouvoir voter librement est l'isoloir, mais il va devenir de plus en plus difficile d'empêcher une personne de filmer son acte de vote, ce qui rend le vote sous contrainte possible y compris dans l'isoloir.

Plus

Voici quelques liens pour avoir plus de détail sur les points abordés.

34. la faille est due aux systèmes commerciaux actuellement utilisés, elle pourrait être corrigée comme on l'a vu dans l'encart page 262

Surveillance

— le dossier du Guardian sur les révélations de l'affaire Snowden http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded
— l'interview de William Binney sur la surveillance de la NSA http://www.democracynow.org/blog/2013/6/10/inside_the_nsas_domestic_surveillance_apparatus_whistleblower_william_binney_speaks_out
— NSA Observer, un beau travail de recherche qui, en particulier, liste tous les programmes référencés de la NSA, https://www.nsa-observer.net/

Nouvelle démocratie

— Le think-tank Décider Ensemble promeut la démocratie participative.
— Le blog de à propos de la démocratie délégative : http://bford.github.io/2014/11/16/deleg.html

Chapitre 7

La cyber-guerre

En 2007 l'Estonie, pays déjà très connecté, a mis un genou à terre suite à une attaque informatique massive de la part de la Russie probablement.

En 2010 un virus *a priori* israélo-américain détruisait les centrifugeuses du programme nucléaire iranien et retardait ainsi de quelques années le programme. C'était probablement la première fois qu'une cyber-attaque détruisait une cible physique.

En mai 2019, l'aviation d'Israël bombardait un immeuble de Gaza pour arrêter une cyber-attaque en cours. C'était probablement la première fois qu'une attaque physique était utilisée contre une attaque dans le monde virtuel.

La cyber-guerre est bien réelle et déjà utilisée par de nombreux pays. La frontière entre le monde physique et le monde virtuel n'a plus beaucoup de sens dans nos sociétés hyper-connectées aussi c'est sans surprise que les polices, les services secrets et les armées sont entrés dans la danse et qu'on parle de plus en plus de cyber-guerre.

Mais de quoi parle-t-on ? Où commence la cyber-guerre ? Est-ce que le piratage des données d'un ministère d'un pays étranger est un acte de guerre ou simplement d'espionnage ? Est-ce que casser l'infrastructure informatique d'une entreprise majeure est un acte de cyber-guerre ? Est-ce que la propagande entre dans la guerre ? Est-ce que perturber significativement une élection dans un pays étranger peut être considéré comme un acte de cyber-guerre ?

On voit que la définition n'est pas simple tant elle dépend de l'intention, de la réussite et de la portée de l'acte. Mais une ligne rouge existe.

> *Une attaque informatique majeure, par les dommages qu'elle causerait, pourrait ainsi justifier l'invocation de la légitime défense au sens de l'article 51 de la Charte des Nations Unies.*
>
> Revue stratégique de défense et de sécurité nationale 2017

La difficulté ne s'arrête pas là car si l'acte est défini comme un acte de cyber-guerre ou de guerre, deux questions restent en suspense : comment réagir et contre qui ? Une réaction

physique avec destruction peut sembler disproportionnée et pourtant les dégâts d'une cyber-attaque peuvent être bien plus importants que ceux d'un bombardement. Enfin trouver qui est à l'orgine d'une attaque est nettement plus difficile dans le monde virtuel que dans le monde physique.

Tout ces aspects font que la cyber-guerre est non seulement nouvelle structurellement puisqu'elle touche de l'immatériel, mais aussi dans son mode opératoire. Lorsque l'aviation a été utilisée comme une arme, il ne s'agissait, comme pour les autres armes, d'approcher de une cible physique pour la détruire. La bombe atomique, qui a soulevé bien des problème dans son usage, fonctionne aussi suivant le même principe. Mais ce n'est pas le cas des cyber-attaques qui touchent à distance l'immatériel lequel contrôle de plus en plus notre économie, nos modes de vie mais aussi le monde physique voire nos vies. La cyber-guerre comme la guerre économique peut mettre un pays à genou sans l'attaquer physiquement [1] mais elle peut aller plus loin.

Dans ce chapitre nous commençons par regarder des exemples de cyber-attaques qui peuvent être assimilées à de la cyber-guerre. Puis nous regarderons d'autres attaques qui sont plus proches de la propagande mais que certains, comme les russes ou les chinois, intègrent dans une définition plus large de la cyber-guerre.

La seconde partie de ce chapitre se concentre sur les moyens mis en œuvre par les différents pays pour mener cette guerre. Pour commencer nous verrons que s'il est à la portée de presque tous les États de développer une cyber-force pour attaquer les infrastructures de l'ennemi, peu peuvent espérer couvrir l'ensemble du spectre des cyber-armes. Enfin nous regarderons les cyber-forces mises en place par différents pays.

7.1 Histoires de cyber-guerre

Depuis premier ver [2] lancé sur Internet en 1988 [3] l'histoire des agressions sur Internet a largement évolué pour arriver au niveau des armées qui préparent toutes les formes d'agressions possibles.

> *[Le cyberespace est un] lieu d' immense violence [dans lequel] tous les coups sont permis. [...] Le cyber est une arme d' espionnage, mais [c']est aussi une arme que des Etats utilisent pour déstabiliser, manipuler, entraver, saboter.*
>
> Florence Parly, ministre des armées – 2019

De fait, les attaques sont nombreuses et leur évolution montre l'implication de plus en plus importante des États. Le rapport impact/prix imbatable de ces attaques et l'importance grandissante d'Internet dans nos sociétés en sont les raisons premières. À cela s'ajoutent les innovations possibles dans l'usage de cette nouvelle arme. Aussi il n'y a pas de raison que la

1. ce qui se passe actuellement, en 2019, avec les États-Unis qui interdissent à toutes les entreprises mondiales de commercer avec l'Iran en est un exemple.
2. Un ver est un programme informatique malveillant qui se propage tout seul sur Internet.
3. Le ver de l'étudiant Morris qui a fait très mal à Internet à l'époque, à un niveau jamais atteint depuis heureusement. L'ironie est que ce ver n'était pas conçu pour faire mal mais un bug l'a rendu dangereux.

cyber-guerre baisse en intensité, pas tant que le rapport impact/prix ne chute au niveau de celui des armes conventionnelles, pas tant que les défenses et réponses des attaqués ne feront pas exploser le prix d'une cyber-attaque, pas tant que l'indentification de l'attaquant ne sera pas efficace.

7.1.1 Estonie 2007

L'Estonie est un ancien pays du bloc soviétique d'un peu plus d'un million d'habitants.

En avril 2007 le gouvernement estonien décide de déplacer la statue du *Soldat de bronze* qui représente la libération du joug nazi par l'Armée rouge en 1944. Cette statue en plein centre ville n'était pas trop apprécié par les lituaniens qui y voyaient plus le symbole de l'occupation russe que celui d'une libération. Par contre pour la forte minorité russophone d'Estonie, environ 25% de la population, cette statue représente le combat soviétique contre les nazis.

La décision a donc soulevé des vagues de protestations tant de la part de la minorité russophone que des russes. Le 26 avril des manifestations font un mort et de nombreux blessés. Le lendemain les cyber-attaques commencent.

Les cyber-attaques

Les cyber-attaques utilisées en Estonie ont été principalement des dénis de service [4]. On a pu compter des centaines de milliers de botnets de plus de 50 pays, dont les États-Unis, ont envoyé des attaques sur les serveurs estoniens.

Les dénis de service peuvent être aussi de simples mails envoyés par millions à des adresses bien déterminées comme celles des députés listées dans un document partagé avec tout ceux qui désirent participer à l'attaque, voir figure 7.1.

Les cibles de la cyber-attaque de 2007 contre l'Estonie ont été :

— le parlement, les sites ministériels, le parti politique au pouvoir ;
— les journaux principaux ;

4. Denial of Service en anglais, DoS, à savoir interroger un serveur (web par exemple) depuis des milliers voire millions de machines en même temps pour qu'il s'effondre, ne pouvant pas répondre à tous. On parle aussi de Distributed DoS, DDoS. Pour avoir un tel nombre de machine à sa disposition on pirate des machines sur lesquelles on installe des programmes dormants qui feront les attaques lorsqu'on leur demandera. Ces programmes, les *bots*, sont groupés en *botnets* pour synchroniser les attaques.

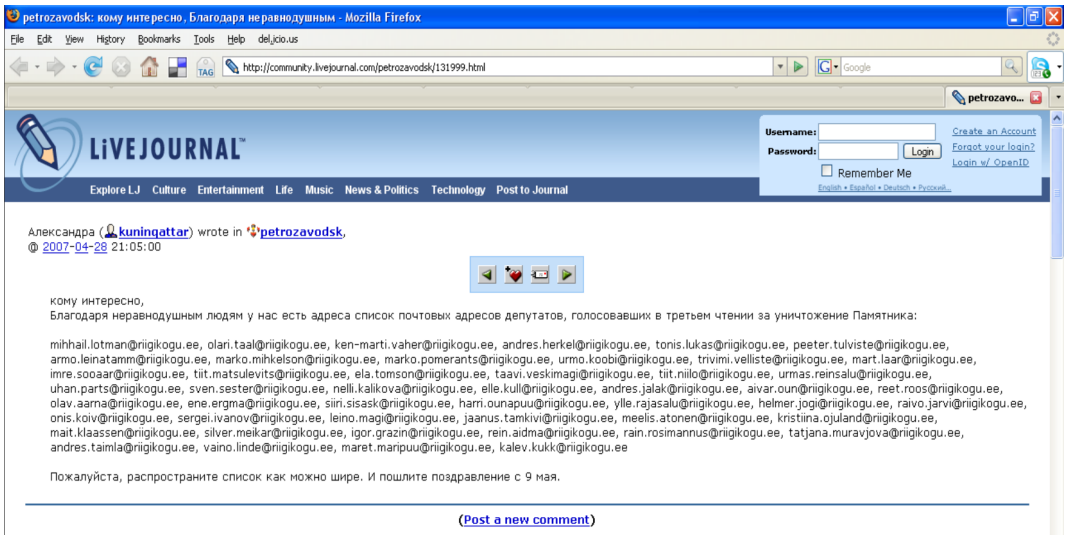


FIGURE 7.1 – Mails des députés estoniens publiés sur un site russe

— les deux plus grandes banques, la Hansabank et la Eesti Ühispank ;
— des universités ;
— les infrastructures télécom du pays, le FAI [5] du gouvernement.

Dans un pays aussi connecté que l'Estonie cela a eu des conséquences terribles. Ainsi les clients de l'Hansabank n'avait plus accès à leur compte via Internet, service utilisé par 97% des clients, mais aussi le système de vérification des transactions était hors service ce qui a perturbé fortement le fonctionnement des distributeurs de billets et a bloqué les connexions avec les banques à l'étranger donc interdit aux clients de cette banque à l'étranger d'utiliser leur carte de paiement. Les services institutionnels étaient bloqués pour un grand nombre et l'infrastructure télécom elle même a été touchées à des endroits pourtant pas connus du grand public normalement.

La défense estonienne a mis en place une cellule de crise pour gérer la défense. Cette cellule a obtenu l'aide de pays étrangers comme l'Allemagne, l'Italie ou l'Espagne et bien des pays baltes voisins la Lituanie et la Lettonie. Elle a aussi été assistée par les FAI étrangers qui ont bien voulu couper la communication aux ordinateurs les plus agressifs qui passaient sur leur réseaux. Mais surtout, après 3 semaines d'attaques et de chaos, le gouvernement estonien a pris la décision de couper les connexions à l'international ce qui a coupé l'Estonie de l'Internet mais ce qui a réussi à réduire assez les attaques pour réagir et remettre en état le réseau.

Le 19 mai les attaques ont arrêté.

Les responsables

Si la coordination des attaques était visible sur des sites web russe où il était indiqué les adresses IP des cibles et les dates des attaques, rien n'indiquait a priori que le gouvernement

5. Fournisseur d'Accès Internet

russe était aux commandes. Des activistes auraient pu être à l'initiative des attaques comme, plus tard, les Anonymous l'ont fait lors de l'Operation Payback contre les entreprises ayant, de leur propre initiative, bloqué les comptes de Wikileaks.

Cependant l'ampleur de l'attaque et son excellente coordination rendent plus probable l'implication des autorités russes avec a priori au moins un accord implicite de la présidence. Le gouvernement estonien a déclaré avoir relevé des adresses IP d'ordinateurs de l'administration centrale russe parmi les attaquants. Pour l'Estonie, l'implication de la Russie est évidente.

Mais aujourd'hui il n'y a toujours pas de preuve formelle du niveau d'implication des autorités russes. De plus ces dernières ont toujours déclaré officiellement ne pas être liées à ces attaques. Seuls des officiels russes ont déclarés en leur nom que tel ou tel groupe d'activistes avait mené l'attaque avec eux, mais rien de convainquant a priori.

On trouve ici une caractéristique de la cyber-guerre à savoir la difficulté de nommer l'agresseur et surtout d'apporter les éléments qui le prouvent. Dans certains cas l'agresseur peut désirer qu'on sache que c'est lui sans toute fois qu'on puisse le prouver. Dans notre cas on peut supposer que les russes ne sont pas mécontents que l'Estonie les considère responsables de l'attaque.

Les réactions

La statue a été transférée dans le cimetière militaire conformément à la volonté des autorités estoniennes.

L'Estonie a profité de l'ampleur de l'attaque pour s'afficher en victime et bénéficier de la sympathie occidentale. Elle a pu également se servir de l'évènement pour pousser sa demande de cyber-défense au niveau de l'OTAN.

CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

En 2008 le Centre d'Excellence de Coopération en Cyber Défense de l'OTAN a été créé à Tallinn. Les pays qui ont aidé l'Estonie durant la crise ont rejoint le centre dès le début. Les États-Unis l'ont rejoint en 2011, la France et l'Angleterre en 2014. Son but est de partager entre ses membres les connaissances en cyber-défense.

Tant à travers ce centre que par des accords avec les entreprises privées et les citoyens, l'Estonie a depuis développé sa cyber-défense. Un des éléments visibles est la réserve citoyenne d'informaticiens certifiés par l'OTAN qui peut être mobilisée en cas de nouvelle cyber-guerre.

7.1.2 Géorgie 2008

En 2008 la Géorgie décide d'attaquer la région d'Ossetie du sud qui fait preuve de sécessionisme mais la Russie choisit de protéger cette dernière et envahit la Géorgie. La région d'Abkhazie profite de l'occasion pour se rebeller et trouve aussi le soutien de la Russie. La guerre a duré 9 jours, du 7 au 16 août 2008 pour finir sur la sécession *de facto* de l'Ossetie du sud et de l'Abkhazie.

FIGURE 7.2 – Cartographie de la deuxième guerre d'Ossétie du Sud – 7-16 août 2008
source : Wikipedia – 2019

L'intérêt de cette guerre dans le cadre de la cyber-guerre est qu'elle est la première guerre qui couple l'attaque cyber à l'attaque physique. On a pu noter non seulement une concordance temporel, des cyber-attaques ont commencé en même temps que les mouvements de troupe, mais aussi géographique avec des cyber-attaques localisées. Le but était non seulement de rendre le réseau internet géorgien inopérant mais aussi de le détourner dans un but de propagande.

Les cyber-attaques russes

On retrouve le même mode opératoire que pour l'Estonie à savoir des DoS (Dénis de services) probablement lancé par les personnes externes au gouvernement russe [6] et probablement coordonnées par le gouvernement russe. Le site `stopgeorgia.ru` a apporté son aide aux attaques en offrant au téléchargement des logiciels d'attaques. Ainsi toute personne à travers le monde qui désirait aider la Russie pouvait le faire très simplement. Ce recrutement gratuit couplé au faible coût d'achat de cyber-attaques fait que cette campagne de DoS a eu un coût ridiculement faible (un expert a chiffré l'ensemble de la campagne au prix d'une chenille de char).

Une autre attaque a consisté à pirater le réseau géorgien et rediriger ses connexions sortantes

6. Le groupe de pirate Russian Business Network basé à St Pertersbourg a été montré du doigt.

vers la Russie et la Turquie où elles étaient bloquées. Ainsi la Géorgie n'avait plus accès au reste du monde.

Cependant la Géorgie étant nettement moins connectée que l'Estonie, l'impact a été moins fort. La perte pour le gouvernement géorgien de ses canaux numériques de communication n'était pas vitale tant vis à vis de ces citoyens que de l'étranger.

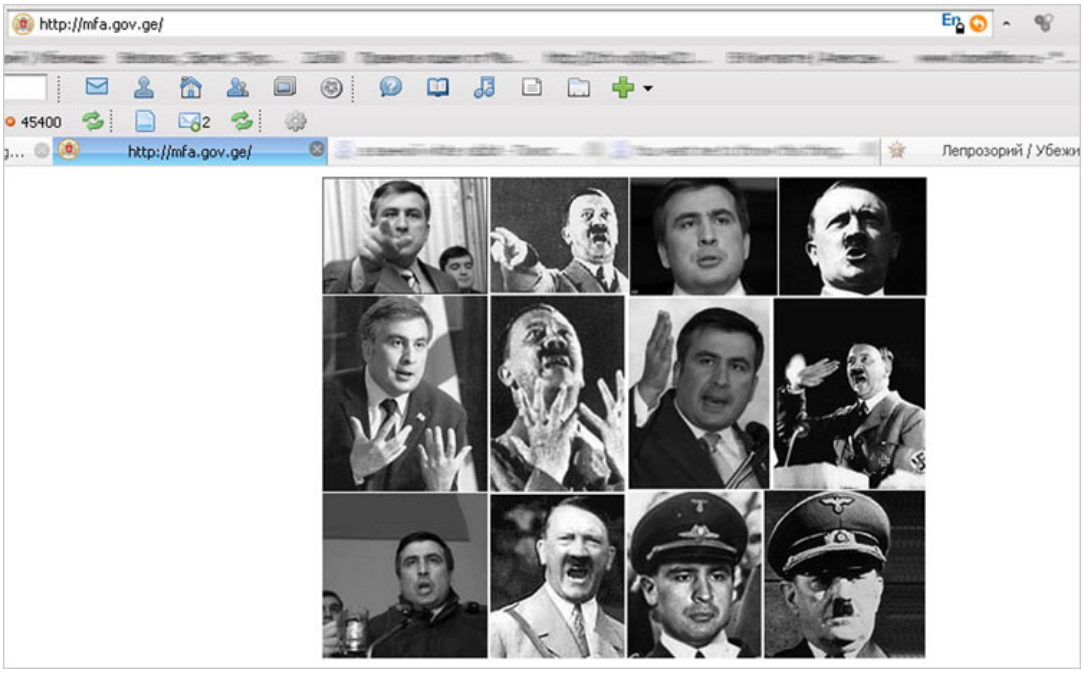


FIGURE 7.3 – Le site de l'assemblée nationale géorgienne piraté
Le président de la Géorgie, Mikheil Saakashvili, comparé à Hitler.

Les autres cyber-attaques entrent dans le cadre de la guerre de l'information. Il s'agit de justifier l'invasion de la Géorgie en dénigrant l'adversaire (on notera en particulier la comparaison du président géorgien avec Hitler figure 7.3) tout en soulignant l'aide qu'apporte la Russie aux peuples d'Ossetie et d'Abkhazie. Pour la Russie cette guerre de l'information est un des piliers de la cyber-guerre.

Les cyber-attaques géorgiennes

Les russes ont aussi déclaré avoir été piratés et ont accusé les géorgiens. Le premier site à avoir été piraté par les géorgiens semble être celui de l'agence de presse d'Ossetie du sud, OSInform News Agency, qui a vu son contenu remplacé par celui d'une agence favorable à la Géorgie. L'agence de presse russe RT a aussi déclaré avoir été attaquée ainsi que des sites web russes officiels.

Mais ce qui a le plus marqué les russes, ce sont les attaques sur leur réseau militaire de communication. Il semblerait qu'avec l'aide des américains, les géorgiens aient réussi à perturber suffisamment ce réseau pour que des officiers russes doivent utiliser leurs téléphones personnels pour communiquer.

D'autre part l'armée russe a clairement fait preuve d'un manque d'équipement numérique dans cette guerre comme l'usage de drones pour éviter de tomber dans des embuscades.

Ces points négatifs pour les russes sont à l'origine de la prise de conscience de l'armée russe du besoin d'intégrer en son sein la cyber-guerre et de ne plus la laisser exclusivement aux services secrets.

7.1.3 Iran 2010

L'attaque des installations nucléaires de l'Iran a été une véritable surprise. Pour la première fois des pays ont utilisé un virus pour détruire des appareils d'un pays ennemi. On a découvert que le virtuel pouvait être utilisé pour détruire du matériel physique ultra protégé.

Avant d'examiner la cyber-attaque regardons le contexte géopolitique. En 2010 l'Iran est un pays en marge de la communauté internationale qui affirme vouloir détruire Israël. Les tensions avec les États-Unis et Israël sont très fortes. L'Iran cherche à se doter de l'arme nucléaire, seule protection efficace en cas de guerre contre ces pays et probablement la seule façon de rayer Israël de la carte [7].

Pour les États-Unis et Israël il faut agir avant que l'Iran ait la bombe atomique. Les israéliens aimeraient lancer des bombardements aériens comme ils l'ont fait jadis contre la centrale nucléaire syrienne, mais l'Iran est nettement plus loin, plus grande et ses centres nucléaires sont dispersés et fortement protégés.

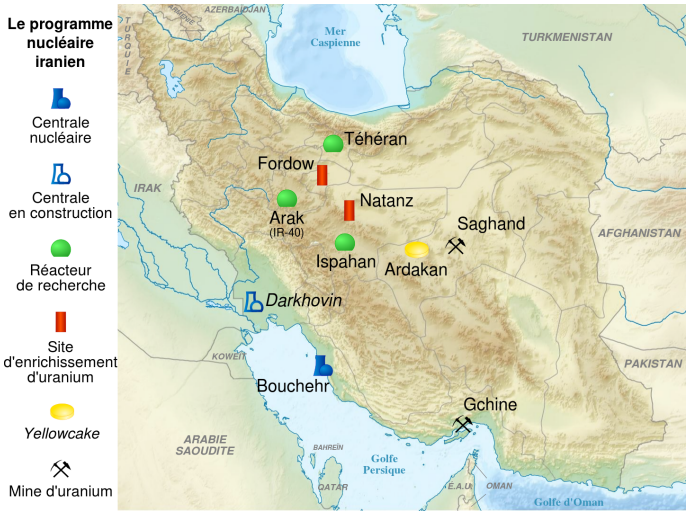


FIGURE 7.4 – La programme nucléaire iranien
source : Wikipedia – 2012

De son coté, la communauté internationale cherche une solution qui ne dégénère pas en guerre.

7. Officiellement l'Iran développe un programme nucléaire civil.

Stuxnet

Une cyber-attaque directe contre les installations nucléaires iraniennes n'était pas possible pour la simple et bonne raison que ces installations n'étaient pas reliées à Internet. Pour les toucher il fallait donc déposer dans le réseau local un programme qui puisse attaquer, un virus. Si ce virus peut se débrouiller tout seul pour se diffuser et dans, notre cas trouver le réseau local des centres nucléaires visés, c'est encore mieux. C'est le principe du ver. Dans le cas d'un réseau non connecté à Internet, un ver passe le plus souvent par des clefs USB qui ont été connectées aux deux réseaux.

L'attaque est donc d'un ver qui a probablement été conçu vers 2005 mais qui n'a été découvert qu'en 2010 par l'entreprise de sécurité informatique Kaspersky Lab. Ces ingénieurs ont découvert le ver sur Internet sans rien comprendre initialement de ce programme très sophistiqué qui n'avait aucun comportement agressif. Ce ver appelé Stuxnet est un programme de très haute qualité :

— son code est très dense et très difficile à comprendre ;
— il n'a pratiquement pas de bug ;
— il exploite 4 failles de sécurité dites *zero-day* à savoir inconnues, une pour se diffuser via USB, une pour exécuter du code à distance et deux pour obtenir des privilèges d'exécution ;
— il a été signé par des certificats officiels de Microsoft, lesquels certificats ont été volés, *a priori* physiquement, dans des entreprises taïwanaises.

Le coût pour développer un tel ver est énorme, tant par le temps humain nécessaire pour le développer, 27 hommes/an d'après Microsoft, que par la valeur marchande des failles *zéro-day*, ½ M$ sur le marché noir, et le besoin d'intervention physique pour le vol des certificats. Il semble donc qu'il s'agisse d'un programme étatique ou d'une organisation criminelle de grande envergure.

Pour les ingénieurs de Kaspersky, tant que la cible de ce ver inoffensif n'était pas trouvée, il était difficile de connaître son origine. Cela pouvait être une bombe à retardement dans le but de faire un chantage à grande échelle, une attaque tellement bien ciblée qu'on ne la voit pas si on n'est pas la cible, ou encore autre chose.

En analysant le code, la cible a finalement été trouvée, il s'agissait de contrôleurs industriels bien spécifiques fabriqué par Siemens, les contrôleurs qui commandaient les centrifugeuses iraniennes de leur programme d'enrichissement de l'uranium. Une fois que Stuxnet avait trouvé sa cible, il s'activait pour faire tourner les centrifugeuses trop vite jusqu'à ce qu'elles cassent, tout en indiquant aux différents appareils de contrôle un comportement normal.

FIGURE 7.5 – Centrifugeuses inspectées par le président Ahmadinejad

Une fois la cible découverte, les coupables ont rapidement été désignés à savoir les États-Unis via la NSA et le Cyber Command avec les Israëliens via leur unité 8200 spécialisée dans le cyber. Bien sûr ces pays nient leur participation.

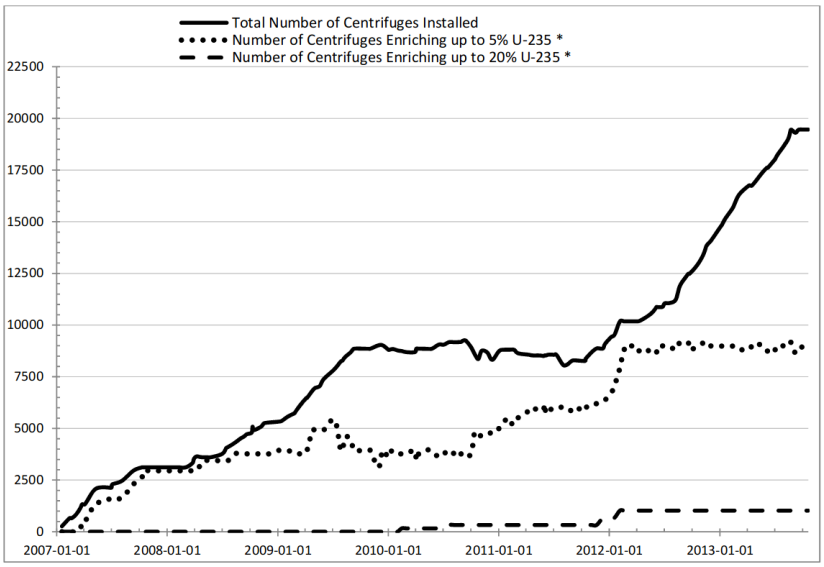
Conséquences

Stuxnet a eu de nombreuses conséquences. Tout d'abord c'est un succès militaire puisque plus d'un cinquième des centrifugeuses ont été détruites ce qui a fortement pénalisé le programme nucléaire iranien. On soupçonne d'ailleurs la démission en juillet 2009 de M. Aghazadeh, responsable du programme nucléaire iranien, d'être due aux retards générés par Stuxnet.

La seconde conséquence est la découverte publique qu'on peut faire du sabotage physique via le monde virtuel.

La troisième conséquence a été l'accélaration de l'installation de de centrifugeuses par l'Iran afin de combler le retard comme le montre la figure 7.6. Si Stuxnet a pu retarder le programme nucléaire iranien, il ne l'a pas arrêté.

Figure 1: Status of Centrifuges in Iran



Note 1: Centrifuges involved in R&D activities are not included.
**Not all of the centrifuges fed with UF_6 may have been working.*

FIGURE 7.6 – Évolution et affectation des centrifugeuse d'enrichissement d'uranium en Iran
source : Agence Internationale de l'Energie Atomique – 14 nov. 2013

La quatrième conséquence a été le cyber armement de l'Iran. Deux ans après la révélation de Stuxnet, des cyber-attaques ont visé la Saudi Aramco qui a eu 30 000 ordinateurs effacés soit 75% de son parc informatique avec toutes les répercussions imaginables en termes de production. La même année, en 2012, l'opération Ababil a bloqué la Bank of America, JP Morgan, Citigroup, US Bank, Wells Fargo et PNC aux États-Unis. Sans se déclarer à l'origine des attaques, l'Iran a pu faire passer le message de l'équilibre de la terreur à savoir "Moi aussi je suis armé maintenant".

7.1.4 États-Unis – 2016

L'histoire retiendra peut-être que le 45ième président des États-Unis a été choisi par les russes.

On a vu dans le chapitre sur la communication comment la Russie a acheté des publicités sur Facebook pour pousser certains groupes à voter (les catholiques traditionalistes qui n'appréciaient pas que Trump ait divorcé deux fois) et certains groupes à rester chez eux (les afro-américains qui votent démocrate généralement), cf 7.7. L'enquête effectuée après l'élection a révélé que plus de cent millions d'américains ont été touchés par ces publicités ciblées (il y a eu 130 M d'électeurs).

Ces messages sur Facebook ne sont bien sûr pas la seule action imputée aux russes. Les fuites sur le contenu des e-mails d'Hilary Clinton révélées par Wikileaks avant les débats avec Donald Trump sont probablement des documents piratés par les services russes. Les informations s'y trouvant ont eu un poids important dans le premier débat mettant la candidate démocrate

FIGURE 7.7 – Publicités russes sur Facebook durant l'élection aux E.U. en 2016

dans une situation délicate. Voici deux exemples qui montrent comment l'impact que peuvent avoir de telles fuites.

Hilary Clinton a indiqué dans un de ces documents fuités qu'elle approuve la phrase de Lincoln dans le film du même nom, qui indique que parfois les politiciens doivent avoir des discours différents en privé et en public. Lors du débat un des modérateurs lui demande s'il est acceptable pour un politicien de jouer un double-jeu. Sachant que la candidate avait déjà refusé d'évoquer des discours privés, son image d'hypocrite en était renforcée.

Dans un autre document elle indique rêver d'un espace nord américain ouvert commercialement et sans frontière. Lorsque durant le débat Donald Trump l'accuse de vouloir ouvrir les frontières et donc favoriser l'immigration elle s'en défend mais le modérateur cite ce document ce qui sous-entend qu'elle ment.

On voit comment des documents privés révélés au bon moment peuvent aider le candidat adverse. Les MacronLeaks, à savoir les boites mails de son équipe de campagne piratées et diffusées juste avant le débat du second tour allaient dans le même sens.

L'élection présidentielle 2016 était particulièrement serrée avec un taux d'indécis très élevé, 15% une semaine avant l'élection. Sachant que Donald Trump a gagné de justesse, des universitaires [8] et officiels [9] pensent que la Russie a réussi à faire basculer l'élection.

Dans cet exemple le terme de cyber-guerre est moins évident. Il n'y a pas eu de dégradation du

8. Voir le livre de la chercheuse K.H. Jamieson "Cyberwar. How Russian Hackers and Trolls Helped Elect a President - What We Don't, Can't, and Do Know".
9. J. Clapper, directeur du renseignement national d'alors, a affirmé que la Russie a fait basculé l'élection.

réseau informatique américain ni de destruction matérielle, pourtant l'impact est immense. Il est évident que les américains ont été pris par surprise et qu'ils feront tout pour que ce genre de situation ne se reproduise pas. Toute la question est de savoir ce que ce *tout* va couvrir. Si cela peut mener à des représailles guerrières, on pourra considérer que manipuler une élection de cette importance est un acte de cyber-guerre.

7.1.5 La suite

À travers ces exemples on a vu différents types d'agression avec différents buts :

— des DoS pour paralyser le réseau ennemi,
— du piratage pour la même raison (mais aussi pour espionner dans d'autres cas),
— de la propagande pour justifier une opération miliaire traditionnelle,
— un virus utilisé comme arme pour détruire du matériel ennemi,
— de la manipulation d'opinion pour faire basculer une élection.

On retrouve ces types d'attaque et d'autres en dehors des cas présentés. Par exemple l'Ukraine, en guerre larvée avec la Russie depuis 2014, est un terrain de cyber-guerre actif et a déjà accumulé un bon nombre de cyber-attaques (sabotage du réseau électrique, le virus NotPetya pour bloquer les réseaux informatiques de nombreuses entreprises ukrainiennes, propagande en ligne pour l'élection sur le rattachement de la Crimée à la Russie...).

Un des points qui ressort de ces différentes attaques est que la notion de cyber-guerre n'a pas la même portée suivant les pays. Pour les russes et les chinois, la guerre de l'information fait partie de la cyber-guerre ce qui n'est pas le cas pour les occidentaux qui se focalisent sur les infrastructures. L'information est un enjeu bien plus critique pour les régimes autoritaires en particulier en interne, mais l'exemple de l'élection américaine de 2016 montre qu'un bon contrôle de l'information et savoir manipuler l'opinion est aussi une force d'attaque contre d'autres pays.

La suite va vers une militarisation de l'Internet. Les grands acteurs préparent le terrain pour d'éventuels conflits. Cela se fait en prenant le contrôle d'ordinateurs, en cartographiant l'architecture des réseaux ennemis, en "minant" le réseau :

> *Ce qui nous préoccupe le plus aujourd'hui, ce sont des attaques où l'on ne voit pas quel est l'objectif. Ce n'est pas de l'espionnage, du détournement de données personnelles. Ce n'est pas encore du sabotage, [mais] des gens de très haut niveau qui préparent les conflits de demain.*
>
> Guillaume Poupard, directeur de l'ANSSI – 2018

La cyber-guerre se prépare aussi en isolant son réseau de l'Internet. Les chinois sont connus pour leur muraille virtuelle appelée aussi le grand parefeu de Chine [10] et les russes sont en train de faire de même. Une loi dite de sécurité informatique oblige l'infrastructure Internet russe à être autonome et donc de ne pas dépendre de serveurs étrangers, y compris du DNS ou de nuages non russes. Cette loi doit entrer en vigueur en novembre 2019.

10. The Great Firewall of China

Les États-Unis étant à l'origine de l'Internet et ayant de facto le contrôle dessus, on peut donc diviser l'Internet actuel en trois zone, la chinoise, la russe et l'américaine, l'Europe étant un vassal des américains.

7.2 L'armement cyber

Les exemples de cyber-guerre présentés permettent d'avoir une idée des armes utilisées mais il ne s'agissait que d'armes relativement basiques en dehors de Stuxnet. Regardons ce qui permet à un pays de développer une cyber-force de qualité.

7.2.1 Niveau 1 : pirates et virus

La première cyber-arme est relativement accessible, peu chère et efficace. Vous embauchez une vingtaine de bons informaticiens, vous leur donnez une bonne connexion et vous avez votre commando prêt à faire plein de choses terribles à travers toute la planète. Il n'existe pas d'arme qui soit plus rentable. Alors pourquoi s'en priver ?

C'est probablement ce que se disent les dirigeants. D'ailleurs en 2019 on compte déjà plus de 30 pays qui ont annoncé avoir une cyber-force. Bien sûr tout le monde n'est pas au même niveau. Les grandes puissances et les pays les plus développés sont déjà bien équipés tout en étant aussi les plus vulnérables car les plus connectés.

En effet Internet a changé notre monde, en particulier dans les pays les développés. Nous sommes devenus numériques et interconnectés. Cela a changé fondamentalement nos façons de travailler, les interactions entre les entreprises, avec l'administration. Sans Internet nos économies s'effondreraient.

La logique voudrait que ces acteurs/pays se protègent. Malheureusement la défense est chère et pas suffisamment efficace. Aussi la majorité met en place des mesures de sécurité raisonnablement efficace contre des pirates occasionnels mais rarement suffisantes contre des experts motivés. Pour le monde économique le réseau doit fonctionner. Le coût de se couper de l'Internet à des fins de protection est bien trop élevé par rapport au coût du risque d'une cyber-attaque [11].

Aussi avoir une cyber-armée pour attaquer tout ces acteurs économiques mal protégés est très tentant. Que cela soit pour du simple espionnage, pour du sabotage plus ou moins léger ou pour mettre hors jeu l'adversaire, l'arme cyber s'intègre parfaitement dans la guerre économique. Et lorsqu'on n'attaque pas, on peut préparer le terrain.

Dans ce domaine les américains sont les rois. Depuis la fin de la guerre froide en 1989, ils ont réaffecté leurs capacités d'espionnage à la guerre économique. On a vu qu'avec l'avènement de l'Internet cet espionnage a pris de plus en plus d'importance et a permis une surveillance globale non seulement des gouvernements et des acteurs économiques mais aussi des citoyens.

11. Le coût du risque étant le coût des dégats infligés par l'attaque multiplié par la probabilité d'être attaqué avec succès. On peut l'assimiler au prix d'une assurance tout risque.

La NSA de la guerre froide est devenu le Big Brother mondial pour le plus grand bénéfice des États-Unis.

La Chine aussi est accusée d'utiliser Internet afin de pirater des entreprises occidentales pour récupérer leurs secrets industriels. L'administration Trump a déclaré en 2019 que la Chine lui vole entre 200 et 600 milliards de dollars par an de secrets technologiques.

7.2.2 Niveau 2 : savoir

L'information est le nerf de la guerre et c'est doublement vrai sur Internet, premier outil d'information.

Les GAFAM sont connus pour être des monstres économiques mais ils sont aussi les gestionnaires de nos vies numériques. Ils savent ce nous faisons en tant qu'individu mais aussi en tant que groupe de personnes. Ils ont une vision comme peu ont de l'activité de nos sociétés, des modes, des maladies, des évolutions. Ils ont aussi pour certain la vision du fonctionnement de l'Internet.

Ce dernier point est un véritable atout stratégique en cas de cyber-guerre puisqu'il permet de connaître le terrain de combat. Les points précédants sont aussi importants puisque le but d'une cyber-guerre est de toucher un pays ennemi et pour cela, la compréhension des comportements humains et sociétaux permet non seulement de mieux toucher sa cible mais aussi d'anticiper les réactions de l'ennemi et de son propre peuple.

Comme aucune armée n'a les moyens de developper ses GAFAM, on comprend qu'au niveau d'un pays, avoir de telles entreprises chez soi offre un avantage évident. Bien sûr faut-il que les entreprises collaborent avec les autorités mais c'est toujours le cas. Ainsi les services secrets des États-Unis, grâce au programme PRISM, peuvent légalement accéder aux données des GAFAM avec une facilité qu'aucun autre pays n'a.

En Chine ce sont Baidu, Alibaba, Tecent et Xiaomi, les BATX, qui sont les équivalents des GAFAM. Elles aussi sont liées à leur État et doivent lui transmettre les informations dont il a besoin. La domination totale de ces entreprises en Chine lui offre une bonne connaissance de sa population et de son réseau tout en réduisant la capacité de forces étrangères d'avoir accès à ces informations.

La Russie, avec Yandex et VK, est dans le même cas que la Chine avec néanmoins une pénétration des GAFAM significative d'où la volonté des autorités russes d'avoir un contrôle local sur ces entreprises américaines.

L'Europe enfin est dans la situation la plus délicate. Ses citoyens et entreprises reposent essentiellement sur les GAFAM et ces dernières répondent à la justice des pays européens. Ainsi la police peut obtenir auprès des GAFAM l'accès à des informations nécessaires à une enquête mais la procédure sera plus compliquée et l'accès aux donnés plus limité que pour les autorités américaines. De plus il est probable que les GAFAM ne répondent pas aux demandes des armées et des services de renseignement européens (pas de PRISM pour l'Europe). Pire, en cas de tensions entre l'Europe et les États-Unis, l'Europe peut perdre tout contrôle sur ces données.

Les câbles

L'accès à l'information peut aussi se faire en interceptant les communication directement sur le réseau, aux points d'interconnexion ou directement sur les dorsales de l'Intenet. Les fibres sous-marines par lesquels passent la quasi totalités de communication entre les continents voire pays sont des éléments stratégiques de première importance.

Dans ce domaine encore les États-Unis ont une longueur d'avance. En plus d'avoir sur leur sol la majorité des câblo-opérateurs et donc de pouvoir les contraindre à permettre l'interception des communications, ils ont aussi la capacité d'aller écouter les câbles au fond de l'eau. Notons que les russes savent aussi aller espionner les câbles au fond de l'eau.

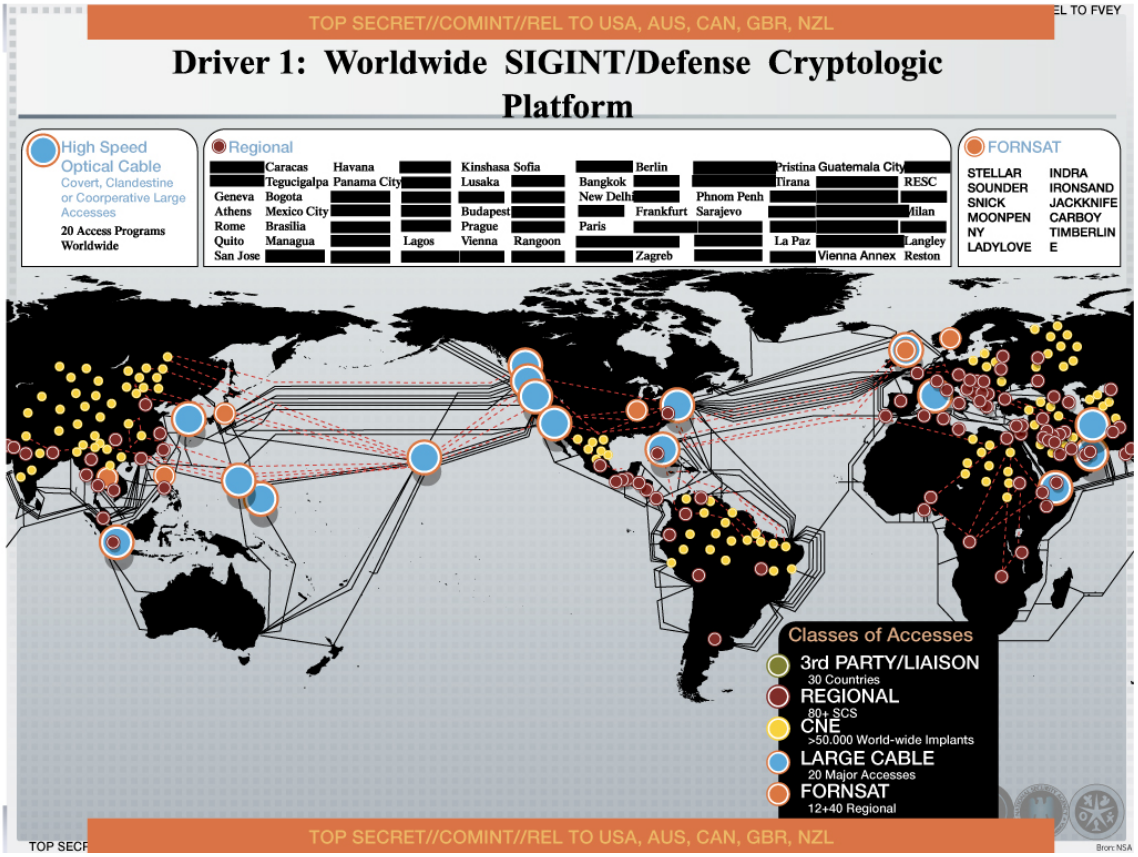


FIGURE 7.8 – Points d'écoute de la NSA en 2012
source : Edward Snowden – 2013

Cela étant espionner les câbles est plus difficile que d'utiliser la loi pour demander à ses GAFAM de fournir les données. Il faut pouvoir poser des appareils d'espionnage sur chaque câble, être capable de déchiffrer ce flux d'information et pouvoir organiser et stocker cette quantité astronomique d'information pour l'exploiter. On n'est plus du tout dans les mêmes ordres de grandeur en terme de coût par rapport à la petite équipe d'informaticiens.

Si les câbles sont intéressants pour obtenir de l'information, ils sont aussi une source de vulnérabilité. Casser un câble est relativement simple et l'impact est tout de suite très important. Pour certains pays qui n'ont pas de redondance, la perte d'un tel câble revient à être coupé de

l'Internet [12]. Pour les autres, la redondance les protège des accidents mais en cas de guerre, on voit mal comment protéger tout ces câbles, sachant qu'il n'est pas nécessaire de les couper tous pour saturer Internet.

7.2.3 Niveau 3 : pirater le matériel

Si des informaticiens peuvent infiltrer des réseaux informatiques et y déposer des bombes ou simplement écrire des virus qui feront le travail tout seul, il est possible de faire nettement mieux. Il est possible de contrôler le matériel informatique.

La crise actuelle sur la 5G et le choix américain d'interdire à Huawei l'accès à son marché en est l'illustration [13]. Le contrôle des infrastructures informatiques est devenu vital pour les pays, ce qui fait passer les considérations économiques au second rang. Même si Huawei présente la meilleure solution technique pour le prix le plus faible, le risque que son matériel puisse être activé à distance par la Chine pour espionner ou saboter le pays client devient trop grand étant donné l'importance d'Internet dans nos sociétés. Le coût du risque devient significatif voire trop important par rapport à la différence de prix entre une technologie locale et celle d'une compagnie étrangère en laquelle on n'a pas confiance. Pour l'Europe, le coût de refuser le matériel de Huawei pour la 5G est estimé à 55 G€ et 18 mois de délais par Reuters [14].

Cette guerre de la 5G est visible mais elle n'est pas la première dans le domaine matériel. Les États-Unis d'Obama avait déjà banni cette entreprise chinoise et sa consœur ZTE des réseaux filaires américain. L'Australie avait déjà refusé un marché de fibre sous-marine à Huawei pour des raisons de sécurité.

Le contrôle du matériel informatique dans une cyber-guerre est bien sûr un atout de luxe mais dont le coût est nettement moins abordable puisque le pays doit avoir des entreprises compétitives dans le domaine. De fait seuls les États-Unis, la Chine et l'Europe semblent en mesure de jouer sur ce terrain.

Il est possible d'aller plus loin dans le contrôle du matériel. On peut mettre des instructions pour détruire un processeur ou permettre d'en prendre le contrôle à distance. Sachant que les appareils informatiques d'un réseau en ont un très grand nombre, il devient possible de tuer voire de contrôler ces appareils et donc le réseau à distance. Ainsi il suffit de fabriquer un des processeurs d'un appareil pour pouvoir au moins abimer ce dernier à distance. On soupçonne l'aviation israélienne d'avoir utilisé un tel procédé pour rendre inopérant les radars syriens lors d'une attaque aérienne en 2007.

Là où l'affaire devient terrible c'est qu'un processeur peut être modifié à l'insu de ses concepteurs. Cela peut avoir lieu lors de la fabrication, l'usine peut modifier discrètement le processeur sans rien changer des fonctionnalités attendues. Dans un monde où la majorité des processeurs sont fabriqués en Chine, le risque devient immense pour les autres pays.

12. En 2017 la Somalie a été ainsi coupée du monde pendant 3 semaines après qu'un porte-conteneurs a coupé le câble sous-marin qui reliait le pays à Internet. Le coût de la perte d'accès à Internet a été évalué à 9 M€ par jour soit presque la moitié de son PIB journalier.

13. En juin 2019, le Japon, l'Australie et la Nouvelle-Zélande avaient déjà emboité le pas des USA et banni Huawei pour la 5G.

14. Nokia, solution de remplacement à Huawei, estime que le coût serait nettement inférieur.

Enfin, après que le processeur ait été fabriqué, des modifications peuvent encore être effectuées à l'aide de faisceaux ioniques. Snowden a montré que la NSA intercepte du matériel informatique pour y placer des mouchards avant livraison. Elle pourrait aussi intecepter des livraisons de processeurs pour y mettre des portes dérobées. Les pays peuvent aussi vouloir modifier des processeurs du grand public avant de les intégrer dans du matériel sensible vendu à l'étranger.

On est donc dans une situation où :

— une faille logicielle permet une intrusion voire le contrôle ;
— une porte dérobée d'un appareil permet son contrôle à distance ;
— un processeur peut être conçu pour altérer l'appareil qui le contient ;
— un processeur peut être piraté pour permettre au pirate d'en avoir le contrôle.

7.2.4 Niveau 4 : l'intelligence artificielle

Si les humains ne peuvent pas appréhender ce qui ce cache derrière des flux de données et réagir immédiatement, les ordinateurs peuvent le faire à condition d'avoir l'algorithme qui permet de traiter les données et d'indiquer comment réagir. Écrire un tel algorithme pour analyser des données qui peuvent être aussi variées que du texte, du son, des images, des films, des codes binaires, des données chiffrées et plus est mission impossible. La seule possibilité d'y arriver semble être d'utiliser l'intelligence artificielle (IA).

Les progrès de l'IA depuis le début des années 2010 sont fulgurants. Alors qu'un ordinateur ne pouvait pas comprendre ce qu'il y a dans une image en 2010, l'IA permet aujourd'hui de décrire une scène en indiquant ce qui s'y trouve. L'IA commence aussi à comprendre le sens des phrases ce qui permet non plus de rechercher le mot "bombe" dans tous les mails mais de lui demander si elle détecte une volonté de préparer une attaque terroriste comme pourrait le faire un humain qui lirait tous les mails. Mais là où l'IA devient indispensable c'est pour lire les données binaires qui circulent sur Internet afin de repérer les virus ou autres formes d'attaques numériques.

L'IA ne s'arrête pas à l'analyse, elle peut aussi apprendre à agir. Les voitures autonomes en sont l'exemple le plus connu mais les majordomes virtuels, les publicités en lignes, les drônes autonomes sont autant d'exemples d'IA qui agissent. Aussi il est tout à fait envisageable de laisser le contrôle des cyber-attaques et de la défense à des IA [15]. Leur vitesse d'exécution et leur capacité à analyser des flux d'information énormes devrait pouvoir dépasser les capacités humaines. Le monde des jeux stratégiques a déjà montré la supériorité de la machine pour de plus en plus de jeux. La marche suivante ne semble pas inaccessible.

15. Mais aussi laisser à l'IA le contrôle des armes conventionnelles et développer des blindés, avions, navires, soldats et généraux autonomes.

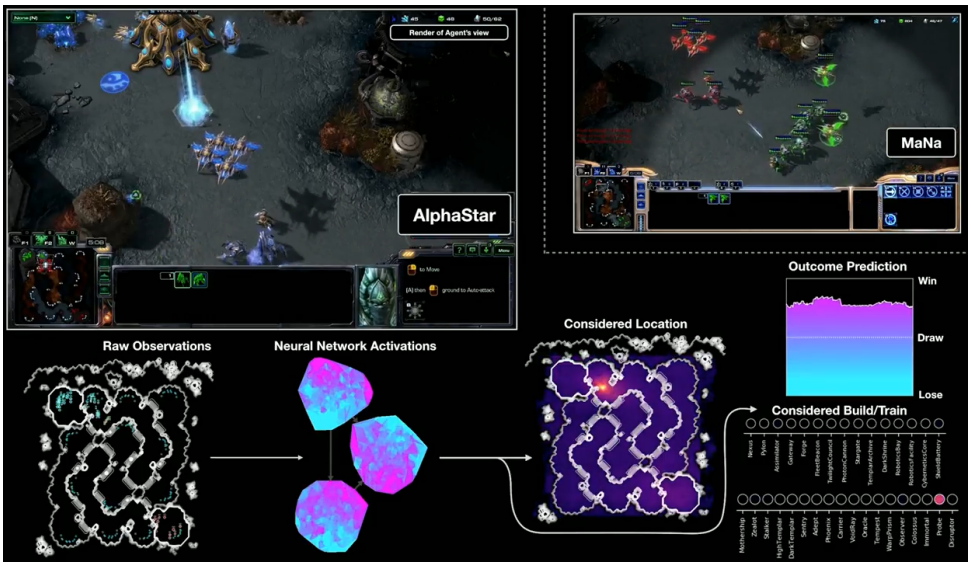


FIGURE 7.9 – Victoire facile d'Alphastar, l'IA de Google, contre un des meilleurs humains

Si on combine l'avantage stratégique qu'offre l'intelligence artificielle à l'avantage économique, on comprend que sa maîtrise soit considérée comme de toute première importance par les pays. Dans ce domaine les États-Unis et la Chine sont en position favorable mais les pays européens ainsi que la Russie affichent aussi leurs ambitions.

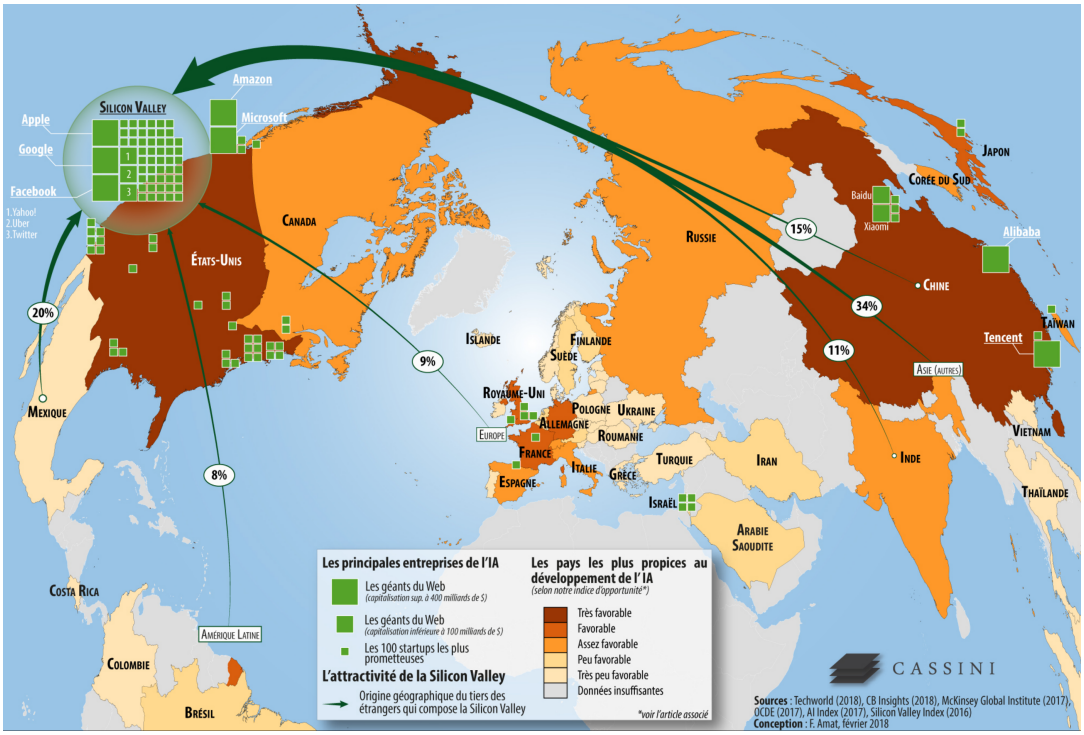


FIGURE 7.10 – Chances des pays dans la course à l'intelligence artificielle
source : Florent Amat et Cassini Conseil – 2018

7.3 Les cyber-armées

Cette dernière partie est la plus délicates car les informations sur les cyber-armées sont bien sûr protégées. Aussi on peut extrapoler des déclarations, des budgets demandés, des analyses faites par les autres pays. On peut ainsi connaître l'existence de cyber-forces mais il est difficile d'en connaitre les détails.

7.3.1 Les États-Unis

Sans surprise les États-Unis sont considérés comme la cyber-force la plus importante. Non seulement ils ont créé Internet et ils en contrôlent une bonne partie, mais aussi ils ont la plus grande armée conventionnelle. Les États-Unis ont dépensé 650 G$ en 2018 pour leur armée contre 250 G$ pour la Chine, 64 G$ pour la France et 61 G$ pour la Russie.

Il est difficile de connaître le budget dédié à la cyber-guerre tant par les aspects secrets des budgets dédiés au renseignement que par la dispersion de la cyber-arme US. Si le commandement, le USCYBERCOM, est un des 10 centre de commandement unifié des États-Unis, ses unités [16] sont en partie intégrées aux autres armes comme le montre l'organigramme figure 7.11. Son budget personnel n'est que de 600 M$ en 2019 à comparer au 190 G$ de chacune des trois armes principales, l'armée de terre, la marine et l'aviation.

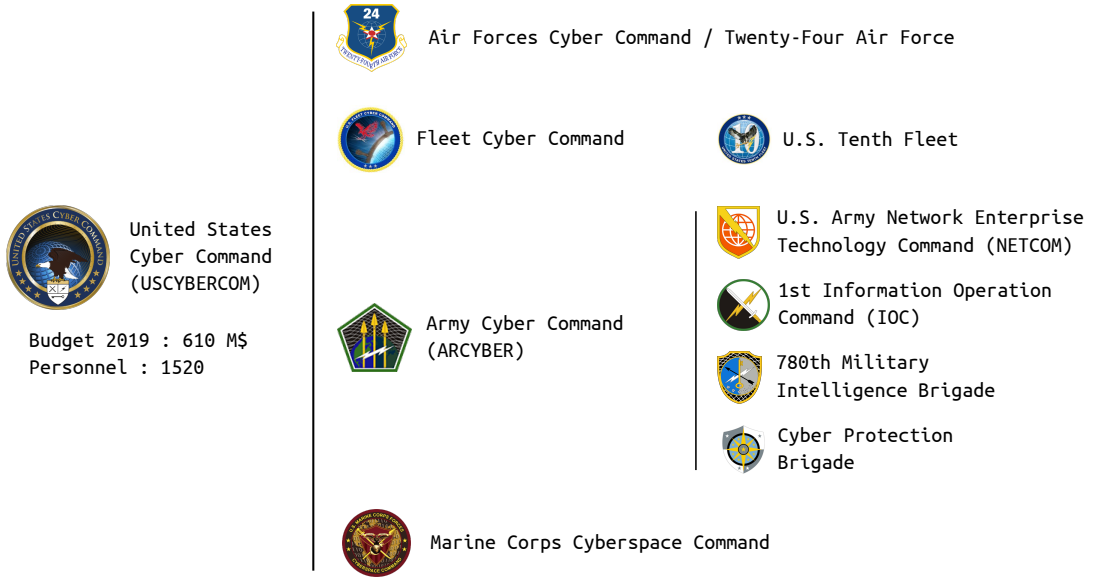


FIGURE 7.11 – Organigramme de la cyber-armée des États-Unis – 2019

Cette dispersion, tout comme la dispersion des unités de renseignement, se comprend dès lors qu'on ne pense pas qu'attaque mais aussi cyber-défense. Pour cela il est important que le cyber intègre tous les niveaux des armées dès lors qu'il y a communication et données numériques, c'est à dire partout aujourd'hui.

16. unités sous double commandement

Si on pense uniquement en capacité d'attaque, il est probable qu'en 2019 la principale cyber-force des États-Unis soit encore la NSA [17].

7.3.2 La Russie

La Russie est probablement le pays qui a utilisé le plus visiblement la cyber-arme en particulier lors d'attaques globales contre d'autres pays [18]. En même temps la Russie mène des cyber-opérations plus discrètes mais pas toujours heureuses comme l'a montré l'arrestation du cyber-commando chargé d'infiltrer le réseau de l'Organisation pour l'interdiction des armes chimiques (OIAC) à La Haye.

Une spécificité supposée de la Russie est d'avoir utilisé à plusieurs reprises des groupes de pirates autonomes pour mener ses cyber-attaques. Outre le gain économique d'utiliser des mercenaires, cela a permis aussi au gouvernement russe de jouer les innocents. Dans le monde cyber où il n'est pas simple de savoir qui fait quoi, passer par des organismes indépendants sans laisser de trace complique la tâche de la victime pour dénoncer l'agresseur. Il est aussi possible que le gouvernement russe manquait de moyen pour lancer des cyber-attaques en 2007 et 2008.

Il est probable que la Russie continue d'utiliser des cyber-mercenaires mais elle a aussi développer des cyber-forces en interne. Le FSB, le successeur du KGB [19] semble avoir été la première force a intégrer l'arme cyber. Si le FSB est chargé principalement des affaires intérieures, il inclut également le Service fédéral des communications et informations gouvernementales (FAPSI), impliqué dans la surveillance électronique à l'étranger. D'autre part la notion d'intérieur est assez souple pour intégrer les anciens membres de l'URSS. Enfin notons que le FSB semble aussi chargé de la guerre de l'information, domaine que les russes intègrent dans la cyber-guerre [20].

La seconde composante de la cyber-guerre russe est le GRU. Après la guerre de Géorgie en 2008, l'armée a décider de coupler la guerre de l'information avec la guerre physique.

> *Net wars have always been an internal peculiarity of the Internet—and were of no interest to anyone in real life. The five-day war showed that the Net is a front just like the traditional media, and a front that is much faster to respond and much larger in scale. August 2008 was the starting point of the virtual reality of conflicts and the moment of recognition of the need to wage war in the information field too.*
>
> Sharov et Shevyakov [21] – 2009

De ce point de vue l'annexion de la Crimée en 2014 a été un véritable succès pour les russes. Le GRU a su utiliser les réseaux pour promouvoir leurs discours et faire de sorte qu'ils soient

17. cf chapitre sur la démocratie pour la présentation de la NSA
18. L'Estonie, la Géorgie et l'Ukraine pour les plus grands.
19. Le KGB qui gérait l'esionnage intérieur et extérieur a donné naissnace au FSB pour l'intérieur et au SVR pour extérieur. Le FSO qui gère la protection des officiels de l'État vient aussi du KGB. L'armée dispose du GRU pour son renseignement.
20. cf Russia' s Approach to Cyber Warfare – 2106 – https://apps.dtic.mil/dtic/tr/fulltext/u2/1019062.pdf
21. cités dans le livre "Inside Cyber Warfares" de Jeffrey Carr

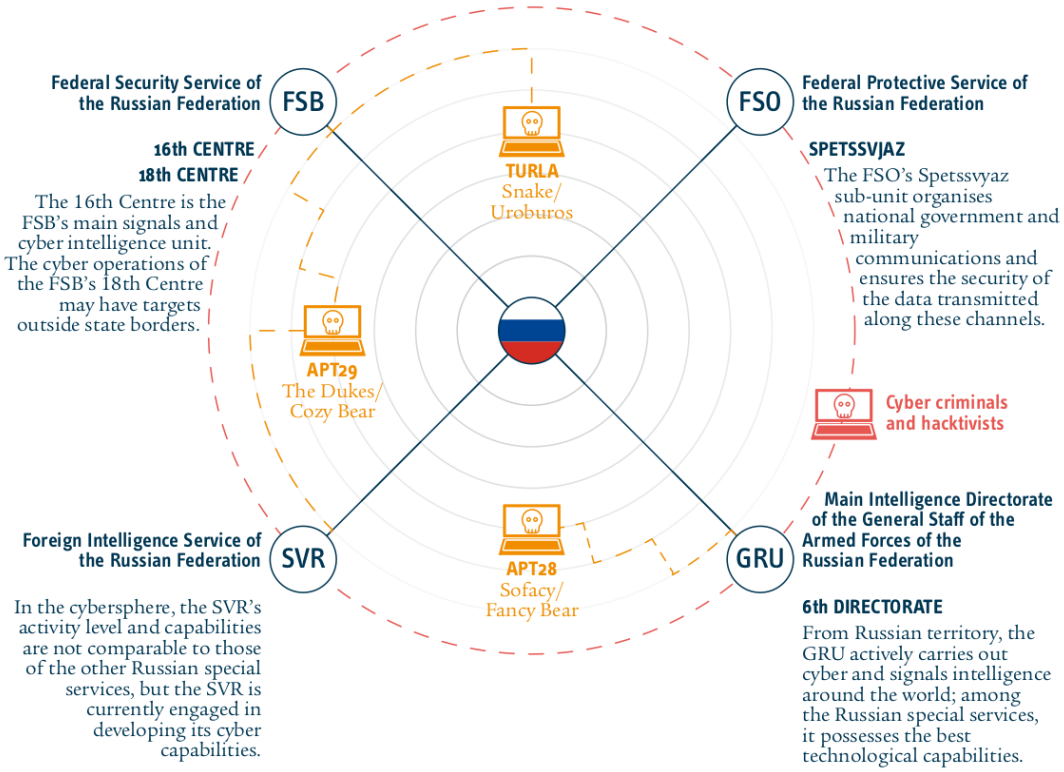


FIGURE 7.12 – Organisation des cyber-forces russes
source : Estonian Foreign Intelligence Service – 2018

acceptés par la plus grande partie possible en y intégrant les contextes culturels nécessaires pour chaque groupe visé. Le vote qui a suivi sur le rattachement de la Crimée à la Russie a montré le succès de la propagande russe (ou sa capacité de défense sur le terrain des idées suivant le camps où on se trouve).

Mais le GRU ne fait pas que de la guerre de l'information. Il agit aussi à l'étranger dans une cyber-guerre à l'occidentale avec des piratages de réseaux. Ainsi il est reproché au GRU d'avoir piraté les données du parti démocrate pour les faire fuiter lors de l'élection présidentielle américaine de 2016. En 2018, le Royaume-Uni a accusé le GRU d'avoir mener de nombreuses cyber-attaques à travers le monde, y compris en Russie, et croit voire une volonté d'ébranler la stabilité mondiale [22]. Le GRU est aussi montré du doigt pour le piratage de nombreuses organisations internationales en particulier dans le domaine sportif.

Toute cette suractivité déplait aux occidentaux.

> *La Russie doit cesser son comportement irresponsable, incluant l'usage de la force contre ses voisins, des tentatives d'immixtion dans des processus électoraux et des campagnes massives de désinformation.*
>
> Déclaration du chef de l'OTAN dans un communiqué de 2018

22. https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed

7.3.3 La France

Comme tous les pays occidentaux, la France développe des forces cyber tant au niveau civil que militaire depuis les années 2000. Bien sûr il s'agissait de cyber-défense puisque la doctrine militaire de la France est basée sur la défense [23]. Ainsi l'ANSSI a pris la suite de la DCSSI en 2009 pour protéger les réseaux informatiques civils

En 2017 l'armée a intégré le cyber au plus haut niveau en créeant le Commandement de la cyberdéfense, COMCYBER, placé directement sous les ordres de l'état-major des armées.

Cepeandant en 2018 la France a affiché sa volonté d'agir aussi de façon offensive dans le cyberespace à traver sa nouvelle doctrine. Elle acte le fait que le cyber est une arme à part entière et s'autorise le droit de l'utiliser aussi pour attaquer tant dans le cadre d'opérations militaires que pour répondre à les offensives cybers [24].

Dans le cadre d'opérations militaires le but offensif est d'obtenir du renseignement, de perturber le bon fonctionnement du matériel adverse ainsi que de l'induire en erreur.

Aujourd'hui les cyber-forces françaises s'articulent donc autour de l'ANSSI pour le civil et du COMCYBER pour le militaire. Plus secrètement les services de renseignement, la DGSE pour l'extérieur et la DGSI pour l'intérieur, ont développés leurs capacités cyber. La direction technique de la DGSE est l'équivalent français de la NSA.

L'ANSSI

L'Agence Nationale de la Sécurité des Systèmes d'Information assure la mission d'autorité nationale en matière de défense et sécurité des systèmes d'information. Cela comprendre la protection des réseaux informatique des administrations mais aussi d'apporter son expertise aux entreprises et au particuliers. Dans ce cadre l'ANSSI a aussi une mission pédagogique.

Pour mener à bien ses missions elle dispose, en plus de ses ressources propres, d'une autorité sur les entreprises stratégiques. Elle peut imposer aux opérateurs d'importance vitale des mesures de sécurité et des contrôles de leurs systèmes d'information les plus critiques. De plus ces entreprises ont obligations de tenir l'ANSSI informée des incidents constatés sur leurs systèmes informatiques.

L'ANSSI résume sa mission en quatre points :

— faire de la France une des première puissance mondiale de cyberdéfense ;
— garantir la liberté de décision de la France ;
— renforcer la cybersécurité des infrastructures vitales nationales ;
— assurer la sécurité dans le cyberespace.

L'ANSSI est rattaché au secrétariat général de la défense et de la sécurité nationale sous l'autorité du premier ministre. En 2018 son effectif était de 600 personnes et son budget de 100 M€.

23. cf Le livre blanc sur la Défense et sécurité nationale de 2013
24. cf https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-de-florence-parly/communique_la-france-se-dote-d-une-doctrine-militaire-offensive-dans-le-cyberespace-et-renforce-sa-politique-de-lutte-informatique-d

Le COMCYBER

Le commandement des forces de cyberdéfense des armées françaises, COMCYBER, est l'unité opérationnelle commandant, de façon organique ou fonctionnelle, l'ensemble des forces de cyberdéfense des armées françaises. Placé sous l'autorité directe du chef d'état-major des armées, le COMCYBER est responsable de la manœuvre cyber globale.

Créé en 2017, le COMCYBER exerce une tutelle opérationnelle sur près de 3 400 cyber-combattants au sein du ministère en 2019 avec un objectif de 5 000 cyber-combattants en 2025 [25].

Pour l'exercice de ses missions, le COMCYBER dispose d'un état-major et a une autorité sur trois organismes interarmées :

— **CALID** Centre d'analyse en lutte informatique défensive
Crée en 2006, basé à Paris & Rennes
— **CASSI** Centre d'audits de la sécurité des systèmes d'information
Crée en 2008, basé à : Maisons-Laffitte, Brest, Orléans, Toulon & Rennes.
— **CRPOC** Centre de la réserve et de la préparation opérationnelle de cyberdéfense
Crée en 2015, basé à Rennes, il gère 4400 réservistes

7.3.4 La Chine

Durant les années 80 les dirigeants chinois ne connaissaient pas Internet au point d'avoir coupé toutes les communications vers l'extérieur durant les événements de Tiananmen en 1989, toutes sauf Internet ce qui a permis aux quelques étudiants ayant Internet d'informer le monde. Depuis les choses ont bien changé et la Chine a su développer son Internet pour devenir la pays ayant le plus d'internautes et possédant des entreprises majeures dans le domaine. À l'extérieur elle a su aussi pleinement utiliser Internet, aux point de se faire une grande réputation de cyber-voleuse de secrets industrielles auprès des occidentaux.

Aujourd'hui la Chine est une puissance majeure du cyber-espace. Elle contrôle parfaitement de qui se passe dans l'Internet chinois et dispose d'une frontière bien gardée. À l'étranger son arme principale réside dans ses appareils qui inonde le monde en particulier ses ordiphones Huwai, Oppo et Xiaomi.

Du point de vue militaire, la Chine a réorganisé son armée en 2015 pour établir la Force Stratégique de Support (战略支援部队) au plus haut niveau de l'organigramme, voir figure 7.13. Cette force opère suivant trois axes : le spatial, le cyber-espace et le domaine de l'électromagnétique. Son département des systèmes réseaux (网络系统部) est en charge de la guerre cyber, électronique et psychologique (dans la veine de la guerre de l'information). Comme pour les armées des autres pays, des cyber-forces se retrouvent aussi dans les armées de terre, air et mer.

25. source : https://www.defense.gouv.fr/ema/commandement-cyberdefense-comcyber

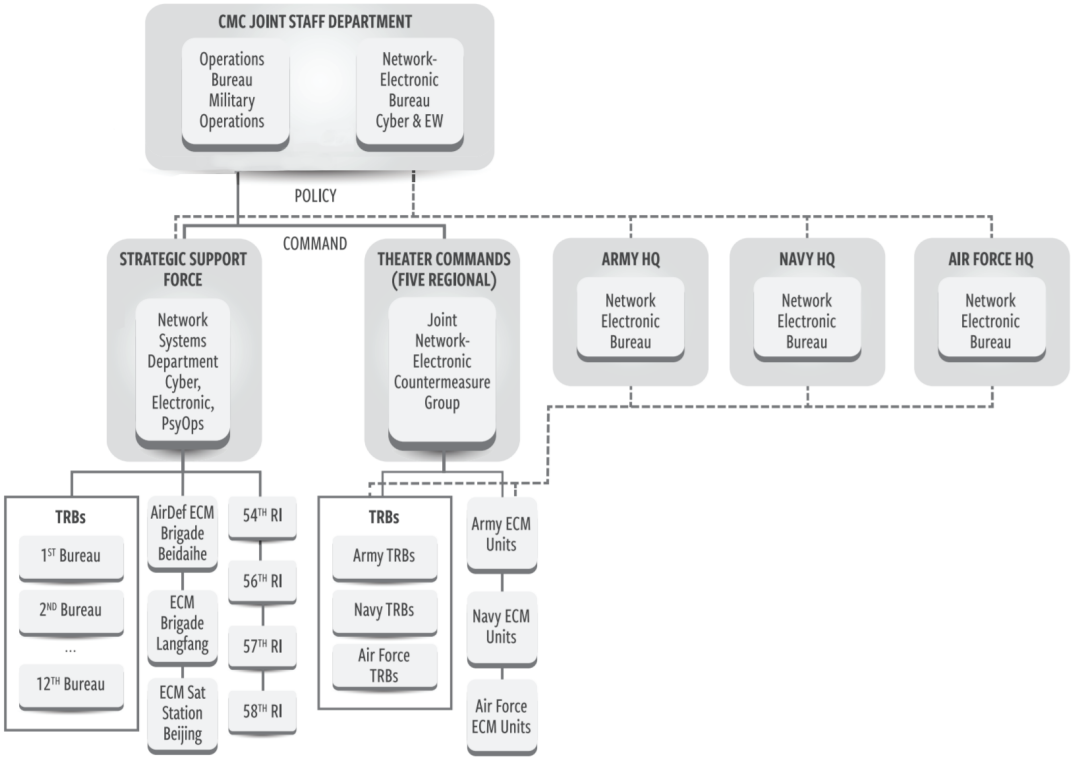


FIGURE 7.13 – Organigramme de la cyber-armée de la Chine – 2017
source : Elsa B. Kania et John K. Costello – 2017

La raison d'être des cyber-forces chinoises est clairement de participer pleinement à un guerre conventionnelle, avec les missions de reconnaissance et de cyber-attaques usuelles. Cependant, pour les chinois comme pour les russes et probablement comme pour les occidentaux de plus en plus, le cyber-espace est un espace-temps différent de l'espace physique :

> *Le jeu stratégique dans le cyber-espace n'est pas limité dans l'espace ou dans le temps, il ne fait pas la différence entre la paix et la guerre, [et] n'a pas de ligne de front et de bases.*
>
> Ye Zheng, Stratège de l'armée chinoise – 2013

Plus

- Les publications du CCDCOE de l'OTAN, https://ccdcoe.org/library/publications/
- La revue de cyber-défense de West Point, https://cyberdefensereview.army.mil/
- La section cyber de l'International Institute for Strategic Studies (IISS) https://www.iiss.org/topics/terrorism-and-security/cyber-space-and-future-conflict