La prospective du caractère stratégique du cyberespace

Dominique Pignon

DELEGATION AUX AFFAIRES STRATEGIQUES
MINISTERE DE LA DEFENSE

La Délégation aux Affaires Stratégiques propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation.

Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la DAS a confié à monsieur **Dominique Pignon** cette consultance sur la prospective du caractère stratégique du web et du cyberespace, sous le numéro de marché 1502641476.

Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la défense et des anciens combattants

Délégation aux Affaires Stratégiques

Sous-direction Politique et Prospective de Défense

14 rue St Dominique

75700 PARIS SP 07

1. La technologie actuelle permet une connaissance en temps quasi réel, légale ou illégale, de toutes les activités des individus connectés ou non sur la Terre. Quelles peuvent être les conséquences politiques de cette connaissance, pour la première fois effective dans l'histoire de l'humanité ?

2. Il est possible pour des individus, des organisations, des institutions, des Etats:

- d'utiliser les informations des différents acteurs à leur insu,
- de modifier les informations disponibles sur le net,
- de détruire des informations.

Le web n'est pas un espace sûr où la confiance règne. Il est devenu une jungle, peu régulée.

3. Du fait du contrôle de plus en plus grand des systèmes matériels, financiers et industriels, par l'intermédiaire des réseaux, ces systèmes du monde réel sont eux aussi rendus vulnérables comme les contenus et les échanges d'informations des réseaux Ils peuvent être détruits à leur tour.

Un point essentiel et nouveau est que le coût marginal des interventions positives et négatives sur les réseaux est quasi nul. L'asymétrie règne en maître : un individu seul peut en principe se mesurer à un Etat ou une institution. Les conséquences de cet état de fait ont de grandes conséquences dans les domaines de la défense, de la sécurité et de la «cyberguerre ».

L'actualité récente montre que les protections contre ces nouvelles pathologies sont peu efficaces voire réellement inefficaces. Les raisons en sont en grande partie scientifiques.

Pratiquement les méthodes heuristiques pour contrer ces pathologies se heurtent à ce qui a fait le succès de cette révolution numérique: la standardisation.

Ainsi pour répondre à ces nouveaux défis les réponses classiques incrémentales ne sont pas adaptées.

I. Introduction

Le développement conjoint des technologies associées dans une spirale auto productrice et des nouveaux usages nous contraint à une description qui doit saisir les forces cachées, « obscures », qui sont en train de transformer notre paysage politique, intellectuel et culturel, au niveau mondial, avec une intensité qui peut se comparer à celle qui fut associée aux transformations des premières et secondes révolutions industrielles. Mais il est aussi difficile de ne pas penser par analogie aux transformations induites par l'invention de l'imprimerie.

En effet le premier Internet, celui qui s'est développé avec les ordinateurs et la microinformatique à la fin du XXème siècle, est lui-même pris à son tour dans un processus plus large, celui de la convergence qui régit dans un seul ensemble des technologies qui étaient restées jusqu'alors séparées. La radio, la télévision, les livres, la presse, les télécommunications et le téléphone sont réunis au sein d'un *Internet général* et doit conduire dans quelques années à une intégration mondiale des télécommunications de la planète dans un système numérique mondial.

Aujourd'hui personne n'est capable de prédire avec certitude les effets sociaux et politiques de cette évolution et, à terme, de cette transformation. Les acteurs de cette transformation, les industriels, les opérateurs des réseaux, les acteurs étatiques, sont pris au dépourvu devant sa violence.
Chacun surestime ou sous estime, c'est selon, l'importance des technologies et des réponses sociologiques et en méconnaît souvent les effets. Le paysage industriel et social s'est déjà considérablement transformé depuis cinq ans. Et personne ne peut appréhender l'allure que prendra ce paysage d'ici les cinq prochaines années. De la pertinence des prévisions dépendra le développement le succès ou le déclin des entreprises.
Les difficultés de prévisions viennent du fait que le *cybersystème* mobilise plusieurs secteurs très différents :

- la technologie de l'informatique, des puces aux systèmes,
- la technologie des usages des terminaux, des ordinateurs aux téléphones intelligents,
- la technologie des réseaux,
- le savoir-faire médiatique associé aux technologies de l'information.

Ce découpage fonctionnel se conjugue avec un découpage institutionnel et social. Chaque groupe social, gouvernement, autorité, industriel, public, utilise les technologies de l'information suivant ses intérêts propres et influence les usages et les évolutions techniques.

Ainsi une distinction fondatrice de la sphère politico-économique établie dans les années 1950, et qui perdura jusque dans les années 1980, la séparation secteur public/ secteur privé, a été progressivement mise en cause durant les quarante dernières années. Celle-ci s'accompagnait d'une hégémonie de fait du secteur public dans le domaine de la recherche et des technologies de pointe. Cette hégémonie a été supplantée progressivement par la recherche développement et l'innovation, déterminées de plus en plus par les usages sociaux grand public et les marchés associés à ces nouveaux usages. Ce déplacement des innovations technologiques du secteur public et en particuliers des secteurs étatiques régaliens comme la défense vers les usages sociaux grand public a des effets massifs dans les sphères politiques et au-delà, dans les domaines géopolitiques.

La numérisation (la digitalisation), de toutes les informations, quelles qu'elles soient, introduit, elle aussi, une transformation des usages que l'on a souvent comparée, depuis l'introduction de la microinformatique et de l'installation de sa domination, avec celle induite par l'invention de l'imprimerie de Gutenberg. En effet celle-ci, en remplaçant la copie manuscrite des textes (et les copistes qui lui étaient associés) par une copie automatisée, avait multiplié son efficacité par des facteurs énormes de plusieurs centaines. Les conséquences politiques de cette première industrialisation de la manipulation des signes écrits, avec la reproduction automatique imprimée des textes, se font encore sentir aujourd'hui et dans une large mesure définissent toujours l'espace culturel contemporain. La numérisation de l'information (d'abord écrite et ensuite étendue à toutes les formes, sonores, graphiques, vidéos) introduit une nouvelle généralisation de la transformation initiée par l'imprimerie. L'abandon du support matériel macroscopique (à la dimension de l'homme) qu'est la feuille de papier pour un support matériel microscopique, qu'il soit magnétique avec les disques classiques ou constitués par des transistors avec les nouveaux disques SSD et les clefs USB, permet de multiplier encore une fois l'efficacité du transport et du stockage de l'information par plusieurs ordres de grandeurs. La numérisation introduit un deuxième effet, économique, nouveau: le coût marginal de la copie tend vers zéro à la différence de la copie d'un livre matériel dont le coût marginal est déterminé par le prix du papier. De même avec la numérisation et la dématérialisation des échanges le coût marginal de la diffusion tend vers zéro alors que dans l'économie matérielle il représente une part importante du coût total.

La démocratisation des échanges et du savoir s'accompagne d'une nouvelle possibilité radicalement nouvelle: celle en principe, de conserver toutes les traces « sémantiques » laissées par les hommes et non réduites aux textes conservés dans les bibliothèques. Cette possibilité de principe est de plus en plus réalisée dans la pratique avec Internet.
Cette possibilité, conjuguée avec l'utilisation des réseaux, ouvre la possibilité d'avoir accès, d'une manière ou d'un autre, à une très grande quantité d'informations individuelles (à toutes les

informations disponibles) d'une grande partie des individus connectés qui utilisent les réseaux de communication. Les possibilités technologiques, qui vont de l'utilisation massive des caméras de surveillance, (par millions et même dizaines de millions !) à l'enregistrement des communications téléphoniques en passant par l'enregistrement de tous les courriers électroniques ainsi que les actions de consultations d'Internet ont déjà été imaginées par les auteurs de sciences fiction du siècle dernier. Le livre emblématique de ces fictions reste le livre d'Orwell, 1984. Ces possibilités deviennent aujourd'hui, avec les progrès de la technologie contemporaine, et encore plus avec les progrès attendus dans les prochaines années, une réalité. Cette réalité traverse aussi bien les régimes démocratiques que les régimes autoritaires et les dictatures. Les questions des libertés individuelles, de la liberté de la presse, du droit à l'oubli, sont à nouveau posées aujourd'hui avec la technologie numérique comme elles s'étaient posées avec l'invention de l'imprimerie. Mais l'efficacité des technologies numériques fait exploser le cadre juridique défini à la suite de l'invention et de la diffusion de l'imprimerie et nous oblige à reconsidérer la validité des cadres juridiques, droit commercial, droit des affaires internationales, droit géopolitique, dans leur plus grande généralité.

L'explosion de l'éducation depuis les années 1970 et la spécificité des technologies informatiques[1] font que le nombre de personnes qualifiées pour produire des outils ou intervenir dans le champ numérique est très grand. Ce fait est renforcé par l'utilisation d'Internet et la mise en commun de savoirs partiels. Le développement de l'open source est l'expression de ce phénomène. La mutualisation du savoir-faire numérique introduit un couplage auto renforçateur très efficace. Cette mutualisation devient ainsi une stratégie de diffusion des savoirs et des savoir-faire informatiques. L'exclusivité des savoir-faire qui avait été maintenue avant le développement des réseaux à l'intérieur des institutions étatiques et industrielles est aujourd'hui perdue. L'autonomisation des chercheurs et des techniciens à travers la constitution de communautés de programmeurs ou des « hackers », de « sachants », constitue un changement radical[2]. A tel point que des firmes comme Google ont mis à la disposition des internautes des services pour renforcer à leurs profits cette mutualisation des savoirs en étendant aux codes informatiques l'outil de recherche général de Google[3]. Ce changement est d'autant plus profond que, à la différence d'autres technologies et de sciences, la pratique effective de l'informatique ne nécessite pas d'investissements coûteux.

Ces caractéristiques permettent d'appréhender, du moins partiellement, l'univers numérique. Elles mélangent les déterminations scientifiques, techniques, sociales et politiques. En interagissant entre

[1] L'informatique ne nécessite pas d'infrastructures coûteuses pour être développée. Un simple PC et une connexion à Internet suffit.
[2] Le savoir informatique n'est plus confiné à une élite institutionnelle. Des groupes comme anonymous, wikileaks et d'autres le démontrent amplement.
[3] Cf developpers.google.com

elles suivant un grand nombre de modes différents, elles constituent l'univers numérique comme un système hypercomplexe.

Cette hypercomplexité produit des pathologies qui ne peuvent pas se définir à l'intérieur d'une seule catégorie. Ces pathologies sont le fait d'interactions entre différentes catégories et sont elles mêmes hypercomplexes.

Le concept unificateur qui englobe toutes les caractéristiques qui nous avons décrites est le concept de cyberespace. Aujourd'hui ce concept, par la complexité de ce qu'il recouvre, est encore imprécis et peut être interprété de façon multiple. Le cyberespace est encore un "mot valise".

II. Introduction au Cyberespace

La caractérisation de l'ensemble définit par le terme cyberespace est fragmentaire et toujours incomplète. Le terme a été introduit aux Etats-Unis au milieu des années 1990 pour définir simultanément deux choses différentes.

Le cyberespace décrit le développement du réseau Internet public à partir des années 1992.

Il décrit aussi ce qui constitue le développement des réseaux d'information et l'informatisation des armées américaines. L'utilisation du terme « cyberspace » est concomitant avec l'introduction de la « révolution dans les affaires militaires(RMA) et son concept de « network centric warfare ».

Cette utilisation dans les affaires militaires fait implicitement référence à deux réflexions distinctes.

L'une est une analyse du rôle de la technologie dans les affaires militaires et l'autre est une analyse plus globale des conséquences de l'introduction de l'informatique et des réseaux de communication dans les forces militaires comme substrat général de tous les systèmes d'armes dans une « transformation globale ».

Ainsi le concept de cyberespace est un concept mixte, soit une description des nouveaux systèmes techniques au cœur des réseaux et des réseaux de réseaux (dont Internet est l'abréviation de inter networks), soit une référence à une nouvelle place globale, sociale et politique, bien au-delà des périmètres militaires.

Dans son usage le plus large on définit le cyberespace comme un nouveau médium dans lequel l'usage généralisé de l'électronique, des télécommunications numériques, des réseaux d'ordinateurs, constitue l'ossature, le fondement d'un nouveau monde, dans lequel les anciennes catégories, techniques, sociales, politiques, stratégiques[4] sont obsolètes.

Nous sommes désarmés devant les nouveaux usages que permet ce « cyberespace ». Le développement technologique est le plus souvent prévisible sur une échelle de temps de quelques années quand des technologies de rupture ne viennent pas tout bouleverser et rendre rapidement obsolètes les technologies en place. Ainsi les grands acteurs des microprocesseurs publient régulièrement des feuilles de routes qui sont en général respectées. Par exemple la loi de Moore qui prédit le doublement des performances des processeurs à coût égal tous les dix huit mois est respectée depuis une quinzaine d'années. Par contre les nouveaux usages que permet l'augmentation des performances des technologies sont souvent imprévisibles et constituent des ruptures sociologiques[5].

Cette question des usages est centrale. Les exemples des difficultés à les prévoir que les acteurs rencontrent sont très nombreux:

[4] l'actualité nous montre que les réseaux de réseaux, le cyberespace devient un enjeu stratégique.

[5] Cf Digital wars , Apple Google Microsoft & the battle for the Internet de Charles Arthur, KoganPage, 2012, le récit de la manière dont les grands acteurs industriels se comportent vis-à-vis des éventuels nouveaux usages.

1. Personne n'avait prévu le développement des micro-ordinateurs dans le public non professionnel. Ce fut le génie des créateurs de la micro-informatique, en particulier de Microsoft et d'Apple, sinon de les comprendre et de les anticiper, du moins d'accompagner les nouveaux usages.
2. Dans un phénomène de convergence des usages, les usages grand public ont cannibalisé les usages professionnels jusqu'à quasiment les remplacer.
3. Personne n'avait prévu le développement rapide d'Internet depuis les années 90. En fait quasiment personne, et en tout premier lieu les inventeurs d'Internet, n'avait prévu qu'Internet sortirait des lieux professionnels, militaires et universitaires pour lesquels il avait été inventé. Internet n'avait pas été conçu comme un système destiné au grand public. A tel point qu'en France, France Télécom ne voyait pas l'intérêt d'Internet face à son système du Minitel et n'imaginait pas une cannibalisation du Minitel par Internet[6].
4. Personne n'avait prévu l'usage grand public des SMS (Short Message Service), système de maintenance à l'usage des professionnels des réseaux de téléphones mobiles.
5. Personne n'avait prévu le rôle central joué par les moteurs de recherche dans l'usage d'Internet.
6. Personne n'avait prévu le développent foudroyant dans les années 2000 du Web2.0 et des blogs qui lui sont associés. L'innovation technologique qui avait contribué à leur développement, la technologie AJAX, était disponible depuis1995. Inventée par des chercheurs de Microsoft, cette innovation qui rendait plus rapide l'affichage des pages web chez l'internaute, est restée longtemps confidentielle avant qu'elle ne soit popularisée par un internaute qui n'était pas lié à Microsoft et devienne une technologie incontournable du web pour en faire un moyen de communication entre les internautes eux-mêmes.
7. Personne n'avait imaginé au début des années 2000 que les réseaux sociaux prendraient une telle place chez les internautes jusqu'à peut-être devenir le mode d'accès privilégié du web en transformant radicalement les usages d'Internet et son sens même.

Cette énumération des surprises dans les usages d'Internet, dans le rôle du cyberespace montre les difficultés à saisir les multiples dimensions de ce nouvel espace.
Comment à partir du système technologique des réseaux et des ordinateurs brancher les usages, c'est à dire les utilisateurs humains ? Comment comprendre la dynamique simultanée introduite par les acteurs et les systèmes technologiques ? Dynamique couplée dont chaque mouvement dans un secteur est amplifié par les réactions d'un autre secteur. Dynamique instable qui met en œuvre dans un couplage étroit tous les acteurs des sociétés civiles, institutionnelles, des communautés de défense.

[6] Le Minitel vient d'être supprimé cette année par France Télécom.

III. L'Internet, le cyberespace et la Défense

Pour illustrer la nouveauté conceptuelle du cyberespace, nous relevons ici quelques définitions :

Le cyberespace est un domaine caractérisé par l'usage de l'électronique et de sondes électromagnétiques pour enregistrer, modifier et échanger des informations par l'intermédiaire de réseaux de systèmes d'informations et d'infrastructures physiques.

C'est la définition donnée par le chef d'Etat-Major des armées américaines en 2006. L'accent est mis sur la technologie qui surdétermine les usages. Deux ans plus tard, en 2008, une nouvelle définition américaine élargit le concept :

Le cyberespace désigne le réseau des infrastructures techniques interdépendantes et inclut Internet, les réseaux de télécommunications, les systèmes d'ordinateurs, les contrôleurs et les processeurs embarqués dans les industries critiques.

Une troisième définition est donnée par les dirigeants de Google dont nous citons des extraits :

Le médium électronique des réseaux d'ordinateurs dans lesquels fonctionnent les communications en temps réel … C'est une métaphore pour le milieu non physique créé par les systèmes d'ordinateurs … L'impression d'espace et de communauté donnée par les ordinateurs, les réseaux d'ordinateurs et les utilisateurs (les usagers) … Le lien dans lequel une conversation téléphonique apparaît … Les distributions géographiques des téléphones…

Ce texte élargit le cyberespace, ce « médium électronique… », aux utilisateurs, aux usagers, à l'usage public, non militaire, des communications.

L'Etat Major des Armées françaises, donne lui aussi une définition du cyberespace[7] :

Le cyberespace informatique est un domaine global constitué du réseau maillé des infrastructures des technologies de l'information (dont Internet), des réseaux de télécommunications, des systèmes informatiques, des processeurs et des mécanismes de contrôle intégrés. Il inclut l'information numérique transportée ainsi que les opérateurs des services en ligne.

Cette définition française est cohérente avec celle de l'OTAN[8] :

---

[7] dans le document PIA-103 intitulé "Concept interarmées de lutte informatique" (CICDE, avril 2009)

[8] Référence AC/322(SC2-NC3TS)L(2007)0002, *Cyberwar Related Definitions*, 11 avril 2007.

Le cyberespace est un monde numérique, généré par des ordinateurs et les réseaux informatiques dans lesquels hommes et ordinateurs coexistent, et qui inclut tous les aspects de l'activité en ligne.

Les quelques milliers d'acteurs dans les mondes militaires et étatiques qui sont concernés par le cyberespace sont tous conscients que ces définitions sont provisoires et ne retiennent qu'une part de la singularité du cyberespace.

Les définitions purement fonctionnelles passent sous silence le caractère non linéaire de ce système.

Un réseau ne peut pas être seulement décrit par ses éléments. Le fait que ces éléments interagissent entre eux rend sa description très difficile. Les effets des interactions sont souvent encore inconnus ou très difficiles à caractériser. La description d'un système, fut-elle aussi logique que possible, ne garantit pas la connaissance de tous les états que peut atteindre le système. Ces états ne sont pas compris dans les descriptions des règles qui régissent les relations des éléments du système entre eux.

Le système technologique matériel doit être conjugué avec l'activité des acteurs, de tous les acteurs, militaires et civils. Il déborde les frontières institutionnelles.

La perception par Google du cyberespace, qui subordonne les technologies aux usages et ne distingue plus les ordinateurs (outils professionnels) des téléphones mobiles, montre que ce nouvel objet, le cyberespace, doit être saisi dans toutes ses dimensions, même si elles débordent les découpages institutionnels actuels, comme les séparations entre les domaines civils et les domaines militaires, et aussi entre les domaines gouvernementaux et les domaines "privés" (entreprises, individus…).

Il faut ajouter ainsi à cette définition une autre qui définit les usages et les usagers:

Le système de réseaux interdépendants et interconnectés définit simultanément un maillage mondial de systèmes physiques (satellites, câbles sous-marins, faisceaux hertziens…), un espace physique qui inclut la Terre dans son ensemble, et un espace virtuel des usages. Les usagers de ces réseaux vont des institutions gouvernementales à l'usager individuel en passant par tous les niveaux institutionnels étatiques et privés, dont en particulier les communautés informelles d'individus. L'utilisation des réseaux est la même, que l'utilisateur soit un représentant d'une institution ou une personne qui agit comme un individu.

IV. Les productions sémantiques des hommes

Que se passe-t-il quand on prend au sérieux le paradigme communicationnel de nos sociétés? Vers quelle société nous engageons nous? Comment celle-ci se fragilise-t elle, ou se rompt-elle? Quelles sont ses nouvelles instabilités dans un médium où toutes les personnes communiquent entre elles, avec toutes les autres personnes, chacune avec chacune ? Les technologies actuelles et à venir dans les prochaines années permettent cette « exaspération de la communication ». Mark Zuckerberg, le créateur de Facebook, a anticipé ces développements, contre presque tous les analystes. En quelques années, même si le modèle commercial n'est pas encore, ou ne sera pas au rendez-vous, plus d'un milliard d'internautes sont connectés à travers Facebook.[9]

Depuis les années 1975, il y a presque un demi-siècle, l'informatisation de la société se poursuit, à marches forcées, L'objectif est de traiter l'ensemble des informations, la totalité des signes produits par les hommes, numériquement. Cette dynamique régit en grande partie l'évolution récente des sociétés actuelles.

Avant de nous engager plus avant dans les effets sociaux et politiques et stratégiques de ces développements numériques nous tenterons ici, pour fixer le cadre de l'analyse, de quantifier les échanges d'informations entre les hommes.

1. Les communications interpersonnelles et l'information associée.

Chaque personne parle à d'autres personnes, soit directement face à face, naturellement sans outils technologiques, soit par l'intermédiaire du téléphone. Pour mesurer la quantité d'information en octets (bytes, 8 bits) on sait qu'une parole de qualité moyenne, compressée convenablement, nécessite 1600 octets par seconde pour être restituée de façon compréhensible. Une heure de conversation occupe un espace de 6 Mégaoctets.

Par comparaison une heure de musique haute fidélité réclame un CD de 600 Mégaoctets. Une photo de qualité moyenne demandera 50000 octets. Une heure de vidéo demandera, quant à elle, plus d'un gigaoctet et demi (1500 mégaoctets)[10].

---

[9] *The Facebook effect: the inside strory of the company that is connecting the world*, David Kirkpatrick. Simon & Schuster, 2011

[10] 1 kilooctet,1 Ko vaut 1000 octets (signes)
1 mégaoctet,1 Mo, vaut 1000 kilooctets
1 gigaoctet, 1 Go, vaut 1000 mégaoctets
1 téraoctet, 1 To, vaut 1000 gigaoctets
1 pétaoctet, 1 Po, vaut 1000 téraoctets. Etc….

Ainsi si on veut enregistrer toutes les conversations humaines d'une journée, à supposer que cela soit possible, et en supposant que cinq milliards de personnes parlent une heure par jour, la quantité d'information totale est de 300 millions de Gigaoctets (300000 téraoctets).

Un progrès significatif (et une rupture technologique), peut-être sur le point d'advenir, serait le codage de la parole en termes phonétiques, voire en texte. On réduirait ainsi l'espace de stockage d'un facteur de plusieurs centaines.

Aujourd'hui les disques durs standards ont une capacité de un à deux téraoctets (1000 à 2000 Gigaoctets). Pour stocker toutes ces conversations quotidiennes il faut disposer de 150000 disques.

Pour stocker un an de conversations mondiales il faut disposer de 50 millions de disques. Ces estimations sont des bornes supérieures. Il est difficile aujourd'hui de stocker des quantités aussi énormes d'information. Mais le filtrage raisonnable des conversations peut diminuer la quantité d'information d'un facteur 100 ce qui correspond à un stockage annuel de 500000 disques. Cette quantité de disques correspond aujourd'hui à un gros « datacenter » de cent mille serveurs. L'évolution technologique laisse entrevoir dans les prochaines années un stockage dix fois plus important des disques à volume et à prix égal.

On voit avec ces estimations et ces ordres de grandeurs que la technologie numérique commence à être capable d'enregistrer toutes les paroles, toutes les « traces sémantiques orales » produites par les hommes sur une durée annuelle.

La capacité actuelle mondiale de stockage que l'on peut mesurer en évaluant la capacité annuelle mondiale de production des disques durs est de l'ordre de un milliard de disques. Cette capacité est donc de mille fois supérieure aux capacités nécessaire pour stocker l'ensemble des conversations privées des humains pendant une année !

Nous ne discutons pas ici l'intérêt social, historique d'une telle conservation. Nous voulons montrer par cette estimation que la production sémantique des hommes est finie et non pas infinie comme on l'affirme souvent. Non seulement elle est finie mais elle peut être ou pourra être conservée, stockée et analysée, à terme par la technologie numérique.

2. Les productions de textes écrits et l'information associée.

La notation écrite du langage parlé est la première grande invention numérique. Elle permet une compression très efficace de l'information orale. Le cerveau est l'instrument qui permet cette compression. On lit environ deux cents mots à la minute ce qui correspond à 16 signes bruts par secondes. En fait à cause de la redondance de la notation écrite on peut comprimer facilement ces signes par un facteur de l'ordre de quatre (par exemple avec le programme zip).

La parole orale nécessite 1600 signes par secondes alors que la parole écrite n'en réclame que 4.2.

L'écriture de la parole correspond à un facteur de compression de l'information d'environ 350. Une technologie qui introduit un facteur d'efficacité de deux ordres de grandeurs, a toujours révolutionné la

société. Et l'on voit ici avec cette estimation que l'invention de l'écriture a eu une importance comparable, sinon plus grande encore, à celle de la révolution numérique !

Stocker le texte écrit qui peut être lu ensuite par un humain est 350 à 400 fois plus efficace que de stocker la parole vive. Une heure de parole occupe un volume de 6 Mégaoctets. Stockée sous forme de texte écrit elle occupe une place de 15000 octets soit un facteur de compression de 400. Dans le volume occupé par une heure de parole on peut stocker 300 livres ! Une heure de parole correspond à 1800 heures de textes lus. On comprend avec ces nombres l'importance de l'imprimerie, première industrialisation du stockage de la parole comprimée.

Les plus grandes bibliothèques nationales contiennent de dix à cent millions de livres. Cent millions de livres occupent un volume de dix téraoctets, dix disques de un téraoctets. L'ensemble des livres imprimés du monde entier peut être stocké sur un millier de disques de un téraoctet. L'ensemble du savoir livresque de l'humanité peut être stocké dans quelques armoires de serveurs.

On constate avec ces évaluations et ces ordres de grandeurs que la production humaine de signes écrits est limitée (on ne discute pas ici de la pertinence et de la qualité des signes écrits, seulement de leur quantité).

Depuis quatre siècles moins d'une centaine de millions de livres différents ont été écrits. Aujourd'hui le web contient des milliards de pages, certains parlent de centaines de milliards de pages, mais ils incluent dans ce nombre les pages générées automatiquement et les répétitions de pages, complètes ou partielles. On estime ce taux de répétition entre cinq et dix sinon plus. Pour un mail il peut être de cinquante.

Si on considère que deux milliards d'internautes sont capables d'écrire une page web, en fait, il n'existe que moins de 200 millions de blogs personnels. Ces 200 millions de blogs correspondent à un volume de 200 gigaoctets. Si chaque bloggeur génère cent pages de blogs par an, le volume annuel de ces blogs est de 20 téraoctets par an et correspond à 20 milliards de pages. On voit que cette estimation de quelques dizaines de milliards de pages, voire quelques milliards de pages, constitue une borne supérieure du web. Dix millions de personnes produiront l'équivalent de un téraoctet textuel par an. On peut multiplier cette estimation par dix ou par cent. Dans les cas les plus optimistes « la production sémantique » écrite d'une année par les internautes parlant français pourra être stockée sur une centaine de disques. Ainsi la production des textes par les humains est maîtrisée par la technologie actuelle. C'est cette possibilité de maîtrise qui a fait la fortune de Google.

La francophonie représente moins de 5% de l'activité du Web. Pour avoir un ordre de grandeur de la borne supérieure de la quantité de textes stockés sur le web il faut multiplier les estimations francophones par 20 ce qui correspond à quelques dizaines de disques.[11]

[11] Le code html qui définit une page web et sa mise en page peut occuper jusqu'à dix fois la quantité réelle du texte.
Beaucoup de pages du web sont des copies plus ou moins exactes les unes des autres. Cette redondance peut aller jusqu'à un facteur 10. Ainsi ces évaluations des quantités de textes peuvent être multipliées par un facteur de 10 à 100 sur le web réel.

3. La production multimédia, photos vidéos et son

La production sémantique humaine par l'acte de parole ou par l'acte d'écriture (manuelle ou à travers des machines à dicter) est limitée par le temps et le travail nécessaires à la fabrication des textes et est donc limitée par le nombre d'hommes sur la terre. Par contre la production d'images fixes ou animées, de photos et de vidéos, n'engagent pas les hommes dans les mêmes conditions de temporalité. Une photo ne mobilise le photographe que quelques secondes. La vidéo réclame, si elle n'est pas automatisée, une mobilisation des acteurs en temps réel. Avec le multimédia la quantité d'information change de dimension par rapport aux évaluations précédentes : une photo occupe un espace de quelques dizaines de kilooctets à un mégaoctet. Une heure de vidéo occupe un espace de l'ordre de un gigaoctet.

Une seule photo en terme d'information est équivalente à celle d'un livre ou à dix minutes de parole. Une heure de vidéo occupe la même place que des milliers de livres. Ainsi l'usage des photos et des vidéos multiplie par un facteur de plusieurs centaines ou de milliers les capacités nécessaires de stockage.

La multiplication des caméras de surveillance et des prises de photos automatisées contraint à ne stocker les informations recueillies que sur des périodes de temps limitées.

L'usage des photos satellites est analogue à celui des caméras de surveillance, surveillant la terre et non plus un parking. Il conduit à l'explosion des moyens de stockages. La technologie actuelle limite l'usage des multimédias.

Pour évaluer les quantités d'informations associées avec ce multimédia et établir des bornes supérieures on peut associer à chaque point du globe, à chaque kilomètre carré, voire à chaque mètre carré, un certain nombre de Gigaoctets chaque seconde ou chaque minute. On obtient ainsi la production d'information fournie par la nature[12]. La Darpa[13] avait, il y a quelques années, dans le cadre du Network Centric Warfare estimé que la défense devait disposer de dix téraoctets (10000 Gigaoctets !) par kilomètre carré de champ de bataille.

Les volumes textuels réels restent malgré ces facteurs défavorables très en dessous des capacités de stockage et de traitement de l'informatique actuelle.

[12] Cette course à la quantité d'information associée à un lieu est sans fin : pourquoi s'arrêter au kilomètre carré, au mètre carré etc…

[13] La Darpa est l'organisme du Pentagone chargé de la prospective scientifique et technologique pour les usages de la défense.

V. Du texte à la personne

Le web s'est développé à partir des années 1990 grâce à une innovation destinée à faciliter les collaborations scientifiques des équipes du Cern, le centre européen de physique des hautes énergies de Genève. Bernars Lee a construit un langage, un codage de l'information, pour permettre d'échanger facilement des informations mises en pages sur un écran d'ordinateur, en fait une généralisation des traitements de textes en vigueur à l'époque. Ce langage, HTML, est devenu très vite un standard mondial qui a débordé la communauté scientifique pour s'imposer comme le langage standard de toutes les communications sur Internet. Ce langage comportait une innovation par rapport au traitement de texte classique, les mots soulignés qui renvoyaient à une nouvelle adresse de page web. Cliquer avec la souris sur ces mots soulignés (les ancres) renvoyait automatiquement sur une autre page à laquelle les mots soulignés faisaient référence à une nouvelle page n' importe où sur le web, sur n'importe quel serveur dans le monde. Cette innovation a été le premier acte de socialisation du net en transposant une pratique classique dans les communautés savantes et scientifiques, inaugurée au 17ème siècle dans les correspondances de savants, la citation et la référence, la note de bas de page. C'est cette innovation qui a permis au web d'obtenir un succès mondial en moins de dix ans. Un mot ou une suite de mots d'une page web renvoie à une autre page web du web. Chaque texte est mis en réseau avec d'autres textes partout dans le monde sans être limité par des frontières géographiques. Les textes des pages web s'inscrivent alors dans un réseau virtuel qui est constitué par l'ensemble des liens entrants et sortants des différentes pages du réseau. Ce réseau n'est pas visible globalement mais il peut être expérimenté pas à pas par un internaute qui clique sur les liens sortants successifs des pages qu'il consulte. Cette innovation est la transposition d'une innovation antérieure, avant le web, popularisé par Apple sans succès avec son logiciel hypertalk qui faisait la même chose avec les textes stockés sur un ordinateur. Cette innovation a imposé un nouveau style aux pages du web. Aujourd'hui une page n'existe vraiment que si elle est connectée et si elle possède des liens avec d'autres pages. La connectivité d'une page à d'autres pages est devenue de fait la marque de sa lisibilité et de sa viabilité.

En moyenne une page contient une à deux dizaines de liens sortants. Les liens constituent ainsi un réseau virtuel qui relie entre elles les milliards de pages du web. De fait, en moins d'une dizaine de clicks successifs, on peut atteindre à partir d'une page du web n'importe laquelle d'une autre page du web.

Plus les liens ont pris de l'importance, plus une nouvelle appréhension du web a vu le jour. L'ensemble des textes, des contenus sémantiques du web, n'est pas seulement perçu à travers la transposition numérique d'une bibliothèque classique, mais aussi comme l'ensemble des liens entre les pages des textes. Ainsi une certaine dualité entre les contenus et les liens s'est imposée. Suivant les cas un des termes de cette dualité, contenus et liens, prend le pas sur l'autre. L'information qui réside dans les liens peut excéder l'information contenue dans les textes eux-mêmes. Les liens et les pages du web

doivent être considérés comme deux objets sémantiques différents dans un rapport symétrique. C'est d'avoir bien compris cette dualité que Page et Brin, les fondateurs de Google, ont pu développer en une dizaine d'année seulement leur moteur de recherche jusqu'à en faire un outil indissociable du web au point que l'on ne peut plus concevoir Internet sans lui. Au point aussi que Google est devenu un instrument essentiel de la géopolitique américaine.[14] Google s'est imposé comme leader mondial (plus de 70% de part du marché) de l'analyse du web à tel point que le mot Google est devenu un verbe : on « Google » un nom sur le net pour trouver les pages qui contiennent ce mot.

De simples outils de recherche avant les années 2000, où il y avait plus d'une centaine de moteurs de recherche (Altavista, Askjeeve etc…) les moteurs de recherche dominants se confondent avec le web. On ne peut plus dissocier Internet des moteurs de recherche. Le web n'est plus utilisable sans les moteurs de recherches qui ne sont plus aujourd'hui que quelques uns dans des positions hégémoniques mondiales Par ordre d'importance Google, Yahoo et Bing (Microsoft) sont les trois moteurs de recherches qui dominent le monde occidental. Yandex, le moteur russe est hégémonique en Russie et Baïdu est le moteur de recherche chinois hégémonique en Chine. Il n'existe pas de moteur de recherche important européen.

Les moteurs de recherche, par leur position de portes d'entrées du web sont devenus ainsi des acteurs géopolitiques incontournables.[15]

Nous avons présenté ici le web comme un ensemble de textes liés entre eux sur le modèle de la bibliothèque, dans une continuité historique avec la structure du livre savant avec ses citations (ses liens). Mais cette vision d'Internet est sans doute datée, contingente et historique. Cette manière de voir les choses est due à la genèse d'Internet développée dans le public avec les universités et donc suivant un schéma où le savoir objectif est primordial et où l'auteur, dans les textes scientifiques, s'efface devant le contenu. Dans les sciences l'auteur est quelquefois un marqueur, mais pas toujours.

Les théories de la relativité restreinte et de la relativité générale ne font pas référence par leur nom à leur inventeur Albert Einstein.

Pour des raisons culturelles le contenu est resté jusqu'au début des années 2000 au centre d'Internet. Un basculement culturel s'est effectué avec la popularisation du web qui a abandonné de plus en plus toute référence culturelle au contenu livresque initial pour privilégier la relation, non plus le contenu mais les relations entre les items, les liens.

[14] Google et la NSA ont fondé un laboratoire de recherche commun de 300 chercheurs. La position hégémonique de Google en fait un acteur essentiel du web et de la géopolitique tout comme l'autre acteur hégémonique Microsoft.

[15] cf l'étude *Géopolitique d'Internet* André Brigot et Dominique Pignon, DAS 2009.

VI. L’entrée en scène de l’individu

Un fait central n’avait pas été apprécié à sa juste valeur jusqu’au début des années 2000: l’importance du courrier électronique. Le « mail » est en général stocké sur les serveurs des fournisseurs d’accès ou ceux des entreprises, institutions, universités etc…Le mail est plus utilisé que la consultation d’Internet par un facteur de dix ou de cent. Jusqu’à une date récente, le mail était relativement rustique. L’éditeur de texte du courrier était minimal et la manipulation des listes de correspondants et des documents par l’intermédiaire des pièces jointes était peu pratique.

Un effet externe qui a handicapé l’usage des mails a été le développement des spams, courriers intrusifs non sollicités, version numérique de la publicité envoyée par la Poste. Ces spams sont générés automatiquement et envoyés à des millions d’internautes d’une manière souvent clandestine ou quasi-clandestine. Ils peuvent constituer plus de 90% de la totalité des mails. Les courriels volontaires ne représentent que 10% du trafic. A l’inverse de la publicité postale, le coût d’envoi est nul et donc leur nombre n’est pas limité par le coût. Envoyer un courriel ou un million de courriel coûte la même chose. L’impératif économique ne limite pas les courriels et donc les spams. La seule limite est l’ensemble des adresses mail des internautes. Il n’existe pas d’annuaires des courriels des internautes, à l’inverse des annuaires téléphoniques.

Malgré cette pollution numérique ou à cause d’elle, une deuxième innovation, après celle de l’hypertexte et des liens associés aux mots d’un texte, a vu le jour. Cette nouvelle innovation a été l’association, non pas d’un mot à une page par un lien, mais d’un nom d’une personne à une autre personne, ou à un ensemble de personnes. Par cette innovation, une généralisation des listes de destinataires des courriels, on faisait sortir le web du carcan culturel du texte écrit qui limite son extension aux personnes qui lisent. Trivialité dira-t-on. Cette innovation réinvente la poste traditionnelle en une poste numérique. Cette remarque critique est exacte mais s’inscrit dans un contexte radicalement différent. Le coût marginal nul des communications permet de réaliser le « phantasme des chaînes postales du bonheur », ces chaînes qui demandaient à celui qui recevait une lettre de l’envoyer à trois ou quatre amis pour constituer une explosion postale exponentielle et « virale » avant la lettre. De fait les contraintes pécuniaires et matérielles ont toujours empêché ces « explosions postales ». Il n’en est pas de même dans le monde numérique.

On voit ainsi se développer depuis les années 2000 une nouvelle économie sociale du net qui coexiste ou supplante ses usages traditionnels.

Mark Zuckerberg, le créateur de Facebook, énonce explicitement le changement de paradigme du passage des liens entre pages web et liens entre personnes :

« Nous avons réfléchi et nous avons décidé que la vraie valeur de Facebook résidait dans l'ensemble des connections, des liens entre les amis[16] ».

Le réseau des relations entre les différents amis d'une page Facebook constitue de proche en proche ce que Zuckerberg a appelé le « graphe social ». C'est la carte des relations entre les personnes, le même type de graphe que celui des liens des pages web qui à partir d'un mot d'une page renvoie à une autre page et ainsi de proche en proche constitue un immense graphe des relations des pages entre elles.

Ainsi Internet, dans sa version moderne, représente un ensemble d'items quelconques, textes, photos, vidéos, musiques, paroles enregistrées, et enfin personnes, et plus précisément amis, qui peut être représenté comme un immense graphe des relations entre les différents items du Web. Le Web des pages et le graphe social ne sont pas identiques.

Dans un premier temps, seules les institutions et les auteurs produisaient une page web sur un serveur. Dans un deuxième temps, avec le développement du Web2.0, les individus qui n'avaient pas le statut d'auteur pouvaient écrire un « blog » ou une page web facilement sur des sites consacrés aux blogs, en fait il n'y a pas de différence entre une page web classique et une page de blog si ce n'est le statut du blog, moins officiel plus personnel et la signature du blog d'un nom véritable ou d'un pseudo. Dans un troisième temps une page d'un réseau social est une page du web réservée à des internautes particuliers et autorisés par l'auteur de la page. En principe l'accès à une page de Facebook n'est pas public. Une page de réseau social est donc une généralisation d'un courrier électronique, intermédiaire entre une page web classique et un courriel classique. Cette page a tout du Web classique mais elle s'oppose radicalement au principe d'ouverture du Web hérité de la communauté scientifique. On ne peut la voir que si on est agréé par l'auteur. C'est cette réserve qui a fait la fortune de Facebook. Plus d'un milliard d'internautes Facebook sont connectés entre eux, peu ou prou par l'intermédiaire de Facebook. Mais seul Facebook dispose ainsi de l'ensemble des données de connections, des liens entre les internautes. Le graphe social de Facebook n'est vu que localement autour de lui par un internaute branché sur Facebook. Aucun moteur de recherche ne peut indexer les pages de Facebook à part Facebook lui-même. Un moteur de recherche ouvert qui analyserait Facebook n'est pas possible. On assiste ici à la première privatisation du Web. Zuckerberg a réussi son pari: il a réussi à construire une plate-forme privée, mais gratuite, qui est ouverte à tous les internautes dont il contrôle seul la gestion de l'ensemble.

Même si le modèle commercial de Facebook n'est pas encore établi, sa réussite a élargi l'emprise de l'économie numérique, après beaucoup d'autres tentatives moins fructueuses depuis le début des

[16] Page 217 dans *The Facebook effect. The inside strory of the company that is connecting the world* David Kirkpatrick. Simon & Schuster 2011

années 2000 en introduisant dans cette économie non seulement les contenus, textes et multimédia, mais aussi les personnes et leur identité[17].

[17] Dès la fin des années 90 le concept de réseau social connectant des personnes est né avec des sites de rencontres comme Match, avec des buts spécialisés; puis Friendster en 2003, puis Tribe et LinkedIn, à but professionnel, puis MySpace dont beaucoup d'analystes prédisaient le plus bel avenir voyant en ce site le successeur de Google.. Tous ces sites ne se sont pas développés comme Facebook. Personne n'a expliqué leur succès limité et le succès fulgurant de Facebook

VII. L'irruption de la mobilité ou la communication partout et tout le temps pour tout le monde

Dès l'an 2000, Bill Gates avait prévu au Comdex, le grand salon mondial de l'informatique individuelle à Las Vegas, la fin du PC et l'apparition des tablettes avec un écran tactile toujours connectées au Web. Pour reprendre un slogan publicitaire: Microsoft l'avait rêvé en 2000, Apple l'a réalisé en 2010 avec l'Ipad. Avant les tablettes, les smartphones sont en train de révolutionner les usages de l'économie numérique. Un téléphone intelligent n'est en effet rien d'autre qu'un petit ordinateur avec écran tactile connecté au réseau Internet par l'intermédiaire du réseau des mobiles, partout et tout le temps.

Dès la fin des années 90 les acteurs principaux du web étaient conscients de l'importance de la mobilité et de la révolution qu'allait provoquer le développement des téléphones mobiles, puis des tablettes, connectés à Internet. Eric Schmidt, l'ancien PDG de Google déclarait lors d'une conférence[18] : « mobile first », sous-entendant qu'à terme la majorité des accès Internet se feraient par l'intermédiaire des mobiles et donc que Google était concerné au premier chef par cette évolution. Préoccupation actée commercialement avec l'entrée de Google dans l'industrie du mobile, dans le software avec le système open source Androïd qui a conquis plus de la moitié du marché des smartphones et dans le hardware avec l'achat de la division téléphone Motorola et la fabrication de tablettes.

On estime que dans une dizaine d'année le nombre de smartphones et de tablettes aura dépassé le nombre de PC. Après les *main frames*, après les stations de travail, après les PC une nouvelle époque s'ouvre, avec de nouveaux acteurs et de nouveaux usages. La majorité des personnes sera connectée au réseau partout et tout le temps. La première étape de la révolution numérique sera achevée.

[18] Sur la manière dont les acteurs on perçu les développements technologique et sur la manière dont ils ont voulu y répondre consulter: *Digital wars, Apple Google Microsoft & the battle for the Internet* de Charles Arthur, KoganPage, 2012.

VIII. La nouvelle économie numérique et les nouvelles médiations

Nous avons jusqu'ici conduit une analyse statique sans prendre en compte les conséquences des transferts et des circulations des informations. Nous devons passer d'une analyse cinématique à une analyse dynamique.

L'économie numérique a quatre fonctions :

- Une fonction autonomie de circulation des contenus, en fait de fichiers d'octets quelles que soient leurs destinations finales, textuelle, audio, photo, vidéo. Cette circulation est régie dans la plus grande part par le protocole TCP/IP d'Internet qui gère le trafic des paquets de bits sur les réseaux à travers les serveurs.

Cette fonction de circulation s'adresse in fine à des hommes. On met à disposition une information pour un individu qui regarde écoute, lit, manipule, enregistre le contenu. Ces contenus, ces signaux immatériels, ne sont pas des choses macroscopiques mais des électrons et des photons qui circulent dans les réseaux et les processeurs. Ces contenus restent dans l'univers des réseaux sauf qu'en dernière analyse, ils retrouvent le monde de l'économie matérielle en activant des yeux, des mains et des oreilles, voire des machines[19].

- Une deuxième fonction, peut-être plus importante que la première, est une fonction de médiation entre les individus. Alors que la première fonction associe une information à une personne, la fonction de médiation fait que le contenu est un prétexte à établir une communication entre deux personnes. Cette fonction de médiation est en train de concurrencer, voire supplanter, la première à travers le développement des réseaux sociaux.

Elle n'est pas nouvelle: la conversation n'est pas une activité nouvelle! Le téléphone non plus.

- Une troisième fonction, intermédiaire entre les deux précédentes, devient à son tour importante. Celle-ci associe à une personne un bien matériel, réel physique. Cette fonction est celle du e-commerce.
- Une quatrième fonction de plus en plus importante. L'information peut s'adresser, et elle va s'adresser de plus en plus, à des machines et ne nécessite pas une intervention humaine. Photos de satellites enregistrées, contrôles de processus, informatique industrielle….

Le smartphone réunit les trois premières fonctions, relation à des contenus, relation avec des personnes, relations au monde marchand, partout et tout le temps. C'est le nouvel objet qui assure l'immersion dans le nouveau monde numérique.

[19] De plus en plus de systèmes industriels sont contrôlés, via Internet, par des logiciels de contrôle délocalisés appelés SCADA. SCADA est l'acronyme de Supervisory Control And Data Acquisition..

IX. Les caractéristiques particulières de l'économie numérique

La spécificité de l'économie numérique, contrairement à l'économie réelle, matérielle, est l'apparition du coût marginal quasi nul. Non pas son coût de production, le coût de ses investissements peut être très élevé, mais le coût, à la marge, de son usage. Les coûts sont mutualisés pour les utilisateurs, le coût d'un envoi ou de la réception d'une information est quasi nul. Une fois le ticket d'entrée dans de monde numérique acquitté, le coût de réception et de diffusion est en principe très faible. Cette propriété n'est pas uniquement le fait de l'économie numérique mais elle est ici radicalisée. Déjà l'économie des biens intellectuels, livres, presse, radio, télévision, échappe pour une part à l'économie matérielle, pour les mêmes raisons. L'influence, l'audience des idées ne sont pas principalement liées à leurs coûts de production. L'influence de la presse papier, même si elle est étroitement imbriquée dans les contraintes de l'économie « réelle » à cause des supports matériels de l'information, le papier et de leur manipulation physique, échappe en partie à ces contraintes dans la manipulation des contenus symbolique qu'elle réalise. Elle peut ainsi être considérée comme un « Internet archaïque », une première exception culturelle aux lois de l'économie classique. La diffusion d'une bonne idée coûte le même prix que la diffusion d'une mauvaise.

Le paradoxe de l'économie immatérielle est qu'elle brise la loi d'airain de l'économie : «tout se paye, il n'y a pas de « free lunch », comme disent les anglo-saxons, pas de « repas gratuit ». Dans le mode numérique la devise pourrait être au contraire, « presque rien ne se paye »[20].

L'information qui circule dans les réseaux représente des contenus qui représentent en dernière analyse des choses réelles. L'économie numérique est une économie des représentations. Ce n'est pas la première fois dans l'histoire qu'une pareille chose arrive. L'argent, les monnaies, sont depuis très longtemps une représentation des choses qui permet la circulation des choses elles-mêmes. En supposant que toutes les choses réelles, matérielles ou immatérielles, se valent, qu'elles ont un prix, un équivalent monétaire, on permet leur manipulation virtuelle. Ainsi on utilise souvent la représentation virtuelle d'une chose qui ne correspond pas, pas encore, ou jamais, à une chose matérielle réelle avec l'invention d'une monnaie virtuelle, l'autre nom donné au crédit. C'est donc dans la sphère financière, bien avant la naissance de l'informatique, que naît la première économie immatérielle, la finance. On comprend ainsi pourquoi l'informatisation de la société et le développement numérique a eu lien en premier dans le domaine de la finance[21]. Il y a une proximité de nature entre les manipulations des monnaies scripturales et la manipulation de l'information. La

[20] Cette affirmation est partielle puisque la mise en place d'une économie numérique nécessite de gros investissements. Mais ces investissements sont très vite mutualisés. Ainsi avec l'automobile, l'usage des routes est gratuit et n'est pas lié au nombre de kilomètres parcourus.

[21] Cette proximité de l'information et de l'argent peut se voir dans la naissance dans certains réseaux sociaux , réseaux de joueurs, univers virtuels, d'une monnaie fictive qui n'existe la plupart du temps que dans ces univers et s'échange entre les membres des différents acteurs de ces réseaux. Quelquefois cette monnaie est convertible dans une monnaie réelle.

réunion des deux représentations, numérisation et argent, a entraîné une des plus grandes crises économiques du XXème siècle et la mise à jour de nouvelles instabilités systémiques liées à la circulation de l'information et ignorées jusque là. Cette proximité est aussi le point d'entrée de la nouvelle délinquance financière, la cyberdélinquance. La cyberdélinquance est la variation moderne, numérique, du pillage classique des banques.

X. Une petite sociologie du web

Les différents contenus, textes, sons, vidéos courriers, sont corrélés aux modes de consultations de ces contenus.

L'hégémonie à terme de l'Internet mobile, déjà entrevue il y a dix ans par Bill Gates et Eric Schmidt, a été mise au centre de la stratégie de Google dès 2004. En achetant YouTube, le serveur de vidéos, et la division téléphone de Motorola, Google essaie, avec succès, de sortir du ghetto de l'Internet classique en développant le système Androïd qui gère aujourd'hui plus de la moitié des téléphones mobiles. Ces mouvements montrent que les principaux acteurs d'Internet anticipent et prennent acte de cette hégémonie à venir. La mobilité s'accompagne de nouveaux usages. Elle entraîne le déclin de l'écriture alphabétique au profit de la musique, des photos et de la vidéo. On passe d'une écriture alphabétique à une écriture idéographique. Ce passage accompagne un changement générationnel mis depuis quelques années en exergue par les sociologues américains avec le concept de « digital natives » et de « digital immigrants »[22].

Ils divisent les internautes en deux catégories :

- La première catégorie est constituée des internautes qui étaient adultes à la naissance d'Internet grand public, dans les années 90-2000. Ils avaient au moins 20 ans en 1990. Ils ont plus de 35 ans aujourd'hui. On les appelle les « digital immigrants », les immigrants numériques.
- La deuxième catégorie est constituée des internautes qui étaient des enfants à la naissance d'Internet et qui ont vécu leur adolescence alors qu'Internet était déjà devenu un média de masse. On appelle ceux-ci les « digital natives », les natifs ou encore les « indigènes du numérique ». Ces internautes qui ont aujourd'hui moins de 25-30 ans ne peuvent pas concevoir un monde sans téléphone portable, sans Ipod, sans tablette graphique, sans mail, sans connexion à Internet. Ils sont décalés d'une génération technologique par rapport à leurs aînés les immigrants numériques qui eux ne peuvent pas imaginer un monde sans voitures, sans téléphone fixe et sans télévision. Ces différences qui définissent le rapport à l'écriture et à l'image définissent un véritable schisme culturel[23]. Le clavier d'ordinateur et la souris seront bientôt relégués au magasin des antiquités technologiques, comme le fut la machine à écrire mécanique, remplacés par la dictée orale de texte et les écrans tactiles, sauf pour les usages spécialisés. Cette mutation techno-culturelle organise les nouveaux usages des réseaux sociaux.

Les parcours de trois des grands acteurs, Bill Gates fondateur de Microsoft, Brin et Page fondateurs de Google et Zuckerberg fondateur de Facebook, montrent assez bien le couplage d'un état historique de la technologie avec les déterminations culturelles de chacun:

---

[22] *www.marcprensky.com/.../prensky%20-%20*

[23] On pourrait ajouter la catégorie des dinosaures numériques: ceux qui avaient plus de 20 ans à la naissance de la micro-informatique en 1975.

- Bill Gate est né en 1955, il a 57 ans. Il a fondé Microsoft en 1975.
- Sergey Brin et Larry Page sont en nés en 1973 respectivement à Moscou et aux Etats-Unis. Ils ont 39 ans. Ils ont fondé Google en 1999.
- Mark Zuckerberg est né aux Etats-Unis en 1984. Il a 27 ans. Il a fondé Facebook en 2004.
- Gate pourrait être le père de Zuckerberg.
- Bill Gate est le représentant des scientifiques et des ingénieurs des années 80. Son obsession: mettre un PC dans la maison de chaque américain. Son programme phare est « word », un logiciel de traitement de texte. Les utilisateurs doivent avoir le besoin d'écrire. Bill Gate est un immigrant numérique.

Brin et Page sont les petits frères de Gate. Ils sont les premiers indigènes numériques. Mais ils ont été éduqués dans le respect du livre par leurs parents professeurs. Ils sont révérends de la culture écrite, du savoir et des livres. Ils veulent construire la plus grande bibliothèque numérique du monde. Ils restent dans un premier temps dans l'ordre du livre et de la culture écrite. Ils évoluent ensuite vers la culture multimédia en achetant YouTube et en entrant dans le monde du téléphone en reconnaissant l'importance de l'image et du divertissement. A leurs débuts ils associent aussi savoir et pourvoir. Ils créent un laboratoire de recherche commun avec la NSA[24]

Mark Zuckerberg est un vrai autochtone numérique. Il appartient de plein pied à la nouvelle génération numérique. Pour lui Gate est une figure tutélaire de père qui est venu faire des conférences alors qu'il était étudiant à Harvard.

Zuckerberg s'intéresse d'abord aux réseaux et aux relations plutôt qu'aux contenus, à l'inverse des trois acteurs précédents. C'est ce déplacement culturel qui, en mettant la relation au centre et en abandonnant les textes au profit des personnes lui assure un succès fulgurant, encore plus rapide que celui de Google, qui était lui aussi plus rapide que celui de Microsoft. Cette nouvelle orientation a donné à Facebook un milliard d'adhérents et un nombre de consultations de son site supérieur à celui de Google en moins de cinq ans.

Mais parallèlement à cette description culturelle on peut analyser ces trois périodes en ne considérant que les évolutions technologiques.

Microsoft vend des logiciels spécialisés et un système d'exploitation avec un monopole assis sur 80% du marché mondial.

Google donne accès à un service d'accès gratuit au web et se rémunère par la publicité. Il exerce lui aussi une position de monopole avec plus de 70% du marché

[24] National Security Agency.

Facebook donne accès à un service de mise en relation des internautes gratuit. Son modèle économique est encore incertain. Son milliard d'adhérents le place lui aussi dans une position de monopole dans les réseaux sociaux.

Ces trois types d'entreprises, de logiciels et de services sont pris dans la tourmente de l'évolution technologique avec le déplacement vers l'Internet mobile. Leur survie dépend de leur adaptation à ce changement.

XI. La question de l'identité et les données personnelles : la servitude volontaire et involontaire

La nouveauté des réseaux sociaux, qui a surpris tous les observateurs, est la facilité avec laquelle les internautes divulguent leur vie privée réelle, supposée ou rêvée. Le succès de Facebook dans ses débuts est venu de son refus d'attribuer plusieurs identités à un internaute et au contraire d'exiger de lui qu'il dévoile sa véritable identité. Les internautes, surtout les jeunes indigènes numériques, ont mis et mettent toujours complaisamment sur leur page personnelle de Facebook, non seulement leur identité réelle mais aussi leurs goûts, leurs préférences culturelles, sexuelles, leurs exploits réels ou supposés, qu'ils soient sociaux ou sexuels, par une sorte d'exercice narcissique de servitude volontaire, sans que personne ne leur réclame cette mise à nu d'eux-mêmes, comme si cette exhibition était la contrepartie d'un surplus d'existence et leur donnait plus de réalité. Beaucoup veulent tout dévoiler d'eux-mêmes. Alors que ces dévoilements et ces informations ne sont disponibles en principe que pour les amis proches à un click de l'internaute, souvent ces informations peuvent dériver au-delà du cercle des amis. De toute façon Facebook dispose de toutes les informations et du graphe social de tous ses membres extrêmement bien documentés. Cette information explicite sur les identités, propre à Facebook, se double pour tous les internautes d'une identité implicite cachée que les internautes construisent au gré de leur utilisation d'Internet et du courrier électronique et qui par-là en révèle souvent plus sur eux-mêmes que les déclarations explicites.

Les bénéficiaires de ces informations sont en premier lieu les moteurs de recherches et les fournisseurs d'accès.

Ils enregistrent toutes les actions des internautes, les questions, les appels de sites, les temps de lecture d'une page web la navigation à l'intérieur du web. Si l'internaute communique avec Internet par l'intermédiaire d'un mobile, ils enregistrent aussi la position géographique de l'internaute à quelques dizaines ou centaines de mètres près.

Il est en principe illégal, en France, de conserver ces informations plus de trois mois et de les utiliser à d'autres fins que judiciaires. En pratique ces informations sont très précieuses pour dresser un profil marketing de chaque internaute et il est très difficile de contrôler leur utilisation. Dans le monde numérique ces informations sont des fichiers comme les autres stockées n' importe où sur le globe sans considération de frontières. Il est donc quasiment impossible de vérifier si ces données sont conservées, utilisées ou non. Les fournisseurs d'accès sont placés dans une position plus favorable que les moteurs de recherche car ils ont accès à toutes les demandes des internautes, pas seulement les appels de moteurs de recherche. Les moteurs de recherche ont contourné cette limitation en mettant à la disposition des internautes des systèmes de mails qu'ils hébergent et ils peuvent donc contrôler non seulement les adresses mail pas aussi le contenu des messages et ceci malgré leurs dénégations

récurrentes sur la lecture des mails. Cet « espionnage » tacite des internautes par les groupes privés participe lui-aussi d'une servitude volontaire encouragée par la facilité d'emploi. Les applications gratuites des smartphones demandent pour pouvoir être téléchargées l'acceptation d'une ouverture complète du téléphone, ses mémoires, ses listes d'appels, sa localisation, pour fournir en principe à l'opérateur toutes les informations possibles sur les pratiques des usagers. Cette identité numérique discrète de l'utilisateur, que certains appellent l' «ombre numérique» (the digital shadow) de l'internaute est l'objet de toutes les convoitises privées et publiques, en particulier des Etats. Nous analyserons plus loin les conséquences de ces convoitises.

Toutes ces informations ne sont pas accessibles au public. Comme le « deep web », les sites protégés, les sites payants, ces informations ne sont pas disponibles pour chacun. Mais en les oubliant pour un temps et en se restreignant aux informations publiques, le contenu informatif a une valeur immense et c'est la première fois dans l'histoire qu'une telle activité humaine, d'une telle ampleur, peut être traitée par des moyens automatiques qui dépassent les possibilités humaines. L'analyse de ces contenus révolutionnera sans doute l'étude de nos sociétés et permettra de donner à la sociologie un nouvel élan. Aujourd'hui on ne dispose pas d'évaluations globales de la qualité de ces informations et de leurs relations au monde réel. Il n'existe pratiquement pas, à notre connaissance, d'études qui examinent la correspondance de ce qui est dit sur le web et de ce qui se passe dans le monde réel. Ces études devraient permettre de construire les « matrices de transfert » du monde numérique au monde réel.

Les seules institutions qui traitent de cette question, du moins partiellement, sont les services de renseignement qui tentent d'acquérir des informations par l'étude du web. L'OSINT, l' « open source intelligence » est le nom donné à cette entreprise analogue à celle des moteurs de recherche.

La National Security Agency est l'institution américaine qui pratique l'OSINT sur une grande échelle et est la plus documentée. Le concept de Big Data, l'analyse et le traitement de toutes les informations disponibles dans le monde numérique, est développé depuis quelques années dans le monde civil, pendant public du travail des services de renseignements et en particulier de la NSA[25].

Nous abordons ici le deuxième volet de l'analyse. Après avoir considéré les potentialités du web et ses usages normaux, nous examinons maintenant ses pathologies, ses maladies et ses dysfonctionnements, que ceux-ci soient naturels, sur le mode de l'accident, ou provoqués par des adversaires privés ou étatiques et les remèdes qui ont été jusqu'ici apportés à ces dysfonctionnements.

[25] cf le dossier de la revue Nature : http://www.nature.com/news/specials/bigdata/

XII. La réponse de la NSA

La NSA s'est appuyée sur une analyse analogue à celle qui précède pour mettre en œuvre son dispositif d'OSINT et de SIGINT en se donnant pour objectif l'interception de tous les signaux produits par les internautes et les usagers du téléphone.

Avant l'avènement du monde numérique, les Etats Unis ont mis en place au lendemain de la 2ème guerre mondiale un réseau mondial d'écoute.

1. Le réseau Echelon et les « five eyes »

Avant la création de la NSA et avant le développement d'Internet et des communications numériques, le réseau Echelon, premier réseau mondial d'écoute SIGINT[26], préfigurait l'observation du cyberespace actuel dont la mission incombe à la NSA. Ce réseau a fait l'objet d'un rapport du Parlement européen[27].

Le réseau Echelon est né en 1947 et il est une prolongation de la collaboration anglo-américaine de la Seconde guerre mondiale pour casser les codes allemands ENIGMA de la Kriegsmarine. Le réseau Echelon d'écoute et d'interception des communications satellites s'appuie sur un accord entre les Etats-Unis et les quatre pays du Commonwealth, l'Australie, le Canada, la Nouvelle-Zélande et le Royaume Uni. Les Anglo-saxons nomment cette collaboration les « *five eyes* ». Elle fonctionne toujours. Cette alliance a été étendue par des accords bilatéraux à la Norvège, l'Allemagne, le Danemark et la Turquie. Des stations d'écoute sont aussi installées en dehors des « *five eyes* » au Japon et en Allemagne.

Dans sa volonté d'intercepter et d'analyser l'ensemble des communications hertziennes mondiales, le réseau Echelon était prémonitoire. Il préfigurait le réseau Internet et sa convergence avec le réseau téléphonique, fixe et mobile, puisque d'emblée Echelon a eu pour objectif d'écouter, d'enregistrer et d'analyser toutes les informations échangées dans le monde et pouvant être interceptées en temps réel.

La NSA aujourd'hui se fixe deux objectifs :

- Le premier objectif est d'essayer d'anticiper l'évolution de la technologie du cyberespace, dans un horizon très incertain du à l'évolution très rapide des technologies.
- Le deuxième objectif est d'anticiper les usages sociaux, en particulier depuis 2001 avec le terrorisme, mais pas uniquement, que les technologies permettent. Elle se veut le leader d'une « nouvelle frontière » après celle de l'atome dans les années 40 et celle de l'espace dans les années 60. Elle veut répondre à la question qui a été posée après le 11 septembre par Bush et développée

[26] SIGINT : *Signal Intelligence*, ou Renseignement d'Origine ElectroMagnétique (ROEM), par opposition notamment au renseignement d'origine humaine.

[27] Gerhard Schmid, *Rapport sur l'existence d'un système d'interception mondial des communications privées et économiques, système d'interception ECHELON*. Parlement européen, 11 juillet 2001. 202 pages. Rapport A5-02-64/2001.

par Obama : quel est l'enjeu stratégique de ce début de siècle ; est-il celui du contrôle du cyberespace ?

La NSA et son chef le général Keith Alexander veut faire de la NSA, budget oblige, le projet Manhattan du début du XXIème siècle[28].

2. Les développements récents de la NSA

L'objectif de la NSA est de recueillir et d'analyser tous les messages paroles, textes, vidéos, échangés dans le monde. Pour réussir cet objectif la NSA a mis sur pied dix centres principaux dispersés à travers les Etats-Unis qui regroupent environ 40000 personnes.

Parmi ces dix centres on peut citer :

- quatre satellites géostationnaires d'écoute, et leurs stations de guidage et de réception (Buckley air force base Colorado),
- Un grand centre d'écoute et d'analyse basé à Hawaï,
- Des centres d'interceptions du trafic Internet chez les opérateurs sur le territoire des Etats-Unis (de dix à vingt),
- Des centres d'interception hors les Etats-Unis[29],
- Le nouveau centre en construction « Utah Data Center » à Bluffdale près de Salt Lake City, d'un coût évalué de deux milliards de dollars et qui doit constituer le data center du système de « nuages » de la NSA. L'énergie électrique nécessaire au fonctionnement de ce centre est évaluée à 200 Mégawatts ce qui correspond à l'énergie nécessaire pour alimenter 500000 serveurs.
- Et enfin de quartier général de la NSA près de Washington à Fort Meade, dans le Maryland.

En plus de ces centres des accords ont été passé avec les principales compagnies de télécommunications, en particulier ATT, pour avoir accès aux communications et aux archives des communications. 320 millions de communications par jour sont archivées et analysées.

Ainsi ATT a plus de 2800 milliards de communications archivés dans une base de données.

Cette version moderne de « bigbrother » est développée dans un cadre légal incertain car il est interdit d'écouter un citoyen américain sur le territoire américain. Mais ce statut incertain de la NSA n'est pas questionné, ou rarement, et n'est pas l'objet d'un débat aux Etats-Unis.

---

[28] C'est l'amiral John Pointdexter, compromis dans le scandale de l'Irangate sous l'administration Reagan, qui a proposé au président Bush au lendemain du 11 septembre un projet d'écoute global du monde pour faire face au terrorisme, le "projet Manhattan du XXIème siècle" comme il l'a lui même surnommé. Devant la version brutale de ce projet de BigBrother, l'administration avait initialement refusé le projet avant que la NSA en hérite.

[29] Par exemple le centre d'interconnections de Mumbai: le Centre de Mumbai (Indes) est un endroit stratégique pour intercepter les données qui circulent sur le câble. Mumbai contient les routeurs qui assurent la connexion de tous les câbles qui desservent le Moyen-Orient et une grande partie de l'Asie. Ainsi, le câble SEA EWE3 a 39 points de raccordements dans 33 pays répartis sur quatre continents, dont les pays d'Europe occidentale (Allemagne, Royaume-Uni, France) jusqu'à l'Extrême Orient (avec la Chine, Singapour et l'Australie). Mumbai assure aussi l'interconnexion avec l'Iran et le Pakistan. Cité dans James Bamford, the shadow factoryDoubleday 2008

3. Les équivalents privés de la NSA.

Les grands opérateurs du Web, Google, Yahoo, Microsoft et Amazon ont eux aussi construit des data center pour regrouper leurs données.

Google construit lui aussi des data centers, moins importants que celui de la NSA de Buffdale.

Mais les data centers sont nombreux. Google investit plusieurs milliards de dollars, comme Microsoft dans ces centres. Et Google se targue d'être le plus grand réseau de data centers interconnectés à travers le monde et disposer de réseaux privés entre ses ordinateurs[30].

[30]Voir l'étude sur Google note 15.

XIII. La vulnérabilité des réseaux et la médecine des systèmes numériques

La presse se fait l'écho depuis plusieurs années de multiples piratages des réseaux et des ordinateurs reliés à ces réseaux. Ces piratages sont attribués à la délinquance et aux mouvements de hackers d'une sensibilité anarchisante et qui s'inquiètent de l'inquisition des Etats et des entreprises privées sur le net. Quelques ouvrages donnent des informations sur ce monde des hackers et leurs prouesses[31]. L'industrie de la sécurité est un acteur important du monde du numérique avec les principaux fabricants d'antivirus, comme Symantec ou Kaspersky.

Les annonces régulières de piratages ou d'attaques des systèmes informatiques démontrent que les protections contre ces attaques sont insuffisantes et toujours en retard. A chaque amélioration des sécurités, de nouvelles attaques réussies démontrent leurs insuffisances.

Les vulnérabilités des systèmes sont de plusieurs ordres. Le système Internet lui-même n'a pas été conçu avec un souci de sécurité. Il est vulnérable.

Les logiciels des ordinateurs sont eux aussi vulnérables, pour des raisons contingentes et pour des raisons profondes.

Les raisons contingentes sont les défaillances humaines. Les codes sont mal écrits, ont des erreurs et on peut souvent utiliser ces erreurs pour pénétrer dans le système d'exploitation d'un ordinateur et lui faire exécuter des taches qu'il n'est pas censé exécuter. La Darpa a estimé le nombre d'erreurs, ou de malfaçons, à une tous les milliers de lignes de codes. Les réponses apportées à ces erreurs contingentes, meilleure organisation du travail de codage, meilleurs protocoles et normes de constructions des codes, multiples contrôles n'ont pas résolu le problème.

Il existe une deuxième raison, peut-être plus grave que la première, théorique celle-ci. On ne peut pas prouver en examinant seulement le texte d'un programme sans l'exécuter que ce programme fait ce qu'il est censé faire. L'analyse statique des programmes qui certifie qu'un programme fait telle tâche et celle-ci seulement ne peut s'appliquer qu'à des programmes ou des parties de programmes relativement simples. La complexification croissante des systèmes d'exploitation et des programmes d'applications, quelques milliers de lignes de codes aux débuts de l'informatique et aujourd'hui quelques millions, voire dizaines de millions de lignes de codes, rend cette vérification statique, sans exécuter les programmes, quasi impossible. C'est le fonctionnement des programmes dans leur version béta préliminaire et le retour vers les concepteurs de leurs erreurs par les utilisateurs qui permet de mettre au point un programme et de réduire les erreurs de fonctionnement à un niveau raisonnable et

[31] Voir en français, *Hacker's guide* de Eric Charton Pearson 2011; voir aussi sur la guerre dans le cyberespace : *Inside cyber warfare*, Jeffrey Carr O'Reilly 2011.

acceptable pour les utilisateurs. Ainsi les systèmes, par leurs logiciels, sont vulnérables aux erreurs. D'où les multiples mises à jour de Microsoft, quasi quotidiennes.

La raison de cette vulnérabilité est la fragilité des codes face à des attaques volontaires qui cherchent les failles d'un logiciel. Celles ne seraient pas forcément mises à jour dans une utilisation normale par les utilisateurs. Une faille mise à jour et inconnue est ce qu'on appelle un « zéro day exploit ». Une telle faille permet de pénétrer dans un ordinateur et de prendre son contrôle, à l'insu de l'utilisateur, jusqu'à ce que cette faille soit publiée sur Internet et corrigée par l'éditeur du logiciel ou par les antivirus. Elle peut être utilisée impunément tant qu'elle n'est pas trouvée par un autre informaticien.

Microsoft propose une récompense de 250000 dollars à celui qui met une faille à jour et la communique à Microsoft. Cette somme est très faible comparée à ce que l'on peut obtenir comme avantages financiers de la possession secrète d'une telle faille dans le monde de la cyberdélinquance.

Une propriété paradoxale des réseaux des ordinateurs rend ces failles particulièrement efficaces.

Un réseau ne se développe que si ses protocoles sont standards. Il est utile si tous les utilisateurs peuvent disposer des mêmes programmes d'accès et de traitement. Le revers de cette universalité est qu'une faille dans les programmes peut être utilisée contre des milliers ou des millions d'utilisateurs. Plus un système est standard, plus il vulnérable et plus il est rentable de chercher les failles de ce système. C'est ce qui s'est passé avec Windows qui domine le marché et qui est particulièrement attaqué. Linux est tout aussi vulnérable mais il est souvent moins rentable d'exploiter ses failles.

Cette vulnérabilité sui generis des systèmes, n'est pas sans rappeler les maladies du monde vivant. La terminologie employée révèle l'analogie qui est plus qu'une séduisante métaphore. On parle de virus informatiques et d'antivirus. Pour s'introduire dans une cellule vivante le virus doit tromper les défenses immunologiques. Si la cellule ne possède pas d'anticorps le virus pénètre dans les cellules et infecte l'être vivant sans que celui-ci puisse réagir**.**

Si la cellule possède la signature du virus, l'a déjà rencontrée et identifiée, par exemple lors d'une vaccination, alors elle peut produire des anticorps adaptés et détruire le virus. Les antivirus informatiques fonctionnent suivant le même principe. Ils possèdent des bibliothèques de signatures de virus qui permettent en principe de les identifier. Les meilleurs virus utilisent ces mécanismes d'identifications pour les tromper et pénétrer malgré tout dans les systèmes. La médecine des ordinateurs, la sécurité informatique qui lutte contre les infections virales est sans fin. A chaque nouveau virus on crée un antivirus qui a son tour est contourné.

L'initiative est à l'attaquant. Le défenseur construit des lignes Maginot qui sont toujours contournées. Les virus informatiques sont beaucoup plus petits que les systèmes (de même en biologie). Ils n'utilisent qu'une petite partie du code des systèmes. Ils sont beaucoup moins chers que les systèmes. Ainsi l'initiative est à l'attaquant qui est dans une position fondamentalement asymétrique. Celui qui

trouve un « zero day exploit » dans Windows est seul devant une des plus grandes multinationales avec des dizaines de milliers de salariés et pourtant il est capable de la mettre en défaut[32].

Ici encore le coût marginal quasi nul de l'économie numérique change radicalement la donne.

L'asymétrie est politique et économique.

[32] Voir le Cybergenome project de la Darpa sur son site http://www.darpa.mil et le projet classifié Plan X.

XIV. La nouvelle asymétrie

Dans une société complètement numérisée tous les systèmes industriels sont pilotés et régulés par des systèmes informatiques. Beaucoup, sinon tous, sont ou sont destinés à être reliés à Internet. Et ceux qui ne sont pas connectés en temps réel, le sont épisodiquement via des clefs USB ou des portables par les utilisateurs.

Ainsi la société civile numérisée, devient ou deviendra à terme, comme les réseaux informatiques, vulnérables aux attaques informatiques.

Aujourd'hui les attaques informatiques sur des systèmes industriels, circulation aérienne, des trains, hôpitaux, distribution de l'électricité et de l'eau, régulation du trafic urbain, peuvent provoquer des dysfonctionnements et des destructions analogues dans leurs conséquences à des attaques militaires.

Le domaine « cyber » devient ainsi un enjeu sécuritaire et militaire.

La frontière entre la guerre et la paix s'estompe. Mais à l'inverse des interventions militaires classiques elles peuvent ne pas faire de victimes. Elles s'inscrivent donc dans le concept d'une guerre à « zéro mort » étendu aux deux parties. Jusqu'ici le « zéro mort » ne concernait que la partie qui menait l'intervention. Avec le cyber le « zéro mort » peut aussi s'appliquer à la partie qui subit une cyberattaque.

Le coût marginal quasi nul, qui est la caractéristique du monde numérique, est à la racine de l'asymétrie de la cyber guerre. La capacité de nuisance d'une lutte informatique offensive n'est pas reliée directement à l'investissement engagé par la construction d'une cyber-arme. Une fois conçue une cyber-arme peut être reproduite, autant de fois qu'on le désire, sans coût supplémentaire.

Ce n'est pas le cas d'une arme classique. Le coût de fabrication matérielle ne disparaît pas devant le coût de la conception.

L'asymétrie entre l'attaque et la défense est portée à son maximum dans l'univers du numérique.

La possibilité de ne pas faire de victimes humaines donne à la cyber-guerre un statut particulier, différent de la guerre classique. Celle-ci permet de porter la cyber-guerre à distance dans un pays sans intervenir physiquement avec tous les problèmes de coût et de logistique qu'une intervention extérieure suppose. Cet aspect joue aujourd'hui un rôle déterminant chez les militaires et les politiques américains dans leurs réflexions stratégiques.

Si la cyber-guerre peut ne pas faire de victimes, surtout si elle reste localisée, elle peut aussi faire des victimes dans les sociétés numériques très industrialisées, comme une guerre classique.

Les Etats Unis ont compris après 2001 qu'ils pouvaient s'approprier cette forme technologique d'asymétrie; que l'asymétrie n'était pas réservée aux terroristes. Ils n'avaient à se restreindre à une utilisation passive et défensive de la technologie avec la NSA. Cet intérêt stratégique pour le cyberespace comme nouveau champ d'exercice du pouvoir et de la domination a conduit à une

réorganisation du rôle de la NSA et à la création d'un haut commandement du cyberespace autonome, quasiment comme une nouvelle arme à coté de trois armes traditionnelles la terre, la mer et l'air.

Le Strategic Air Command, en charge de la gestion de l'arme nucléaire, a mis sur pied une équipe de cyberguerre pour développer des armes de lutte informatique offensive. La démarche était la suite logique de la création d'Arpanet et d'Internet qui avaient été inventés pour relier l'ensemble des sites nucléaires du Strategic Air command et résister à une attaque nucléaire. Mais l'expertise de la NSA et son caractère secret, en particulier aux Etats-Unis ont fait que les deux institutions ont créé le US Cyber Command, composé de quelques milliers d'hommes installés dans les bâtiments de la NSA à Fort Meade sous le commandement du général Alexander qui est le patron de la NSA et du Cyber Command.

L'étude de la vulnérabilité des réseaux, pour les défendre et pour les attaquer, a fait depuis quelques années l'objet d'une réalisation concrète pilotée par la Darpa, le « Cyber range ». Ce Cyber range est un réseau réel, non simulé, constitués de quelques milliers de serveurs sur le modèle réel des serveurs utilisés chez les militaires et dans la société civile. Des jeux de rôle avec des attaquants et des défenseurs sont menés sur ce vrai réseau afin d'en étudier toutes les possibilités. La simulation d'un tel objet est trop complexe, le nombre des états possibles est trop grand, pour faire l'économie de la construction d'un vrai réseau, véritable champ d'expérimentions des défenses et des attaques menées au sein des nouvelles sociétés numériques.

Parallèlement à cette réorganisation qui a acté la naissance d'un nouveau concept de défense[33], la cyberguerre, le numérique a introduit à l'autre bout de la chaînes les drones armés. Un homme, un assassinat, un drone. Les drones utilisent eux aussi l'asymétrie, mais à front renversé, dans une pyramide qui repose sur la pointe. L'emploi d'un drone réclame une chaîne complexe de transmission qui mobilise un satellite. Le coût du système de transmission est beaucoup plus élevé que le drone lui-même et limite le nombre de drones.

[33] Ce concept de cyberguerre, cyberwar a été développé en particulier par Richard A.Clarke conseiller de plusieurs présidents à la Maison Blanche, le dernier étant Bill Clinton dans un livre : *Cyberwar; the next threat to national security and what to do about it*, Harper Collins 2010

XV. La première rupture de la cyberguerre : l'opération Olympic Games

L'opération Olympic Games s'est déroulée de 2006 à aujourd'hui. Elle a été organisée par les Etats-Unis et Israël, dans une étroite collaboration qui est restée ultra secrète, jusqu'à ce qu'elle soit révélée par différents laboratoires d'analyse de la sécurité du Web.

Les américains ont révélé une part essentielle de l'opération. Les Israéliens n'ont fait aucune déclaration sur cette opération.

Elle a été menée depuis la « situation room » de la Maison Blanche en présence du président Obama qui s'est directement impliqué dans cette opération.

Le but d'Olympic Games a été le sabotage, à l'aide d'un programme informatique, des centrifugeuses de l'usine iranienne d'enrichissement d'uranium de Natanz.

L'opération a été lancée par le président G.W.Bush en 2006, qui a sommé ses services de trouver une solution alternative à deux propositions de tout ou rien, l'inaction ou la guerre, à propos de l'usine d'enrichissement iranienne qui est un des points essentiels de divergence entre les Etats-Unis et Israël.

C'est devant l'ultimatum de G.W. Bush que la solution de la mise au point d'une cyberarme a été décidée dans le plus grand secret. Les fuites involontaires ou volontaires, on ne peut l'affirmer aujourd'hui, ont révélé l'opération dans un assez grand détail. Le journaliste David Sanger a raconté une grande partie de l'opération, à commencer par son nom de code Olympic Games dans une série d'articles du New York Times et dans un livre[34]. Cette opération a été conduite par la NSA et son équivalent israélien appelé l'unité 8200. Elle a consisté à la fabrication d'un virus fonctionnel adapté au processus de pilotage informatique des centrifugeuses de l'usine de Natanz. L'usine n'est pas reliée directement à un réseau extérieur, Internet ou autre. Pour être menée à bien elle supposait la possibilité d'introduire matériellement le virus, à l'aide probablement d'une clé USB dans le système de contrôle de l'usine.

Elle supposait donc l'existence d'une taupe à laquelle on pouvait confier cette tâche. Le programme pouvait, à partir de cette intrusion physique, réaliser le sabotage et la destruction des centrifugeuses, ou du moins d'une partie de celles-ci. En un sens Olympic Games est une opération classique de sabotage qui utilise in fine, au lieu d'explosifs, un programme informatique.

Le président Obama était très inquiet des conséquences de la révélation éventuelle de l'opération. Les Etats-Unis ne sont pas en guerre contre l'Iran et cette opération de sabotage pouvait être considérée comme une opération d'agression et un acte de guerre. Le statut juridique de l'opération est incertain aux Etats-Unis. Pour illustrer la gravité politique du geste, la conduite de l'opération a été soustraite au

[34] *Confront and consceal : Obama's secret war and surprising use of american power*, David E. Sanger, Crown publisher, 2012

commandement militaire et donné à la NSA car ainsi chaque étape de l'opération demandait l'autorisation explicite du président. Le caractère ultra secret de l'opération et l'implication de la Maison Blanche ont conduit les différents informateurs de l'enquêteur à comparer le projet Olympic Games, non par son coût mais par son caractère secret et sa nouveauté au projet Manhattan de construction de la première bombe atomique à Los Alamos. Comme le dit l'ancien chef de la CIA, Michael Hayden : « les précédentes cyberattaques avaient des effets limités sur d'autres ordinateurs… C'est la première attaque majeure dans laquelle une cyberattaque était utilisée pour provoquer des destructions physiques. Quelqu'un a traversé le Rubicon »[35].

L'attaque a commencé effectivement en 2008. Il a fallut auparavant, en utilisant des méthodes classiques, se procurer des exemplaires des centrifugeuses utilisées par les iraniens auprès de Kadhafi qui en avait hérité quelques unes d'un programme nucléaire interrompu volontairement par lui-même. Il a fallu aussi se procurer le code des logiciels qui pilotent ces centrifugeuses, fabriqué par Siemens, et construire une copie de l'usine d'enrichissement de l'uranium, avec quelques centrifugeuses, dans un laboratoire secret, sans que des fuites interviennent pour mettre au point et tester l'efficacité du virus. Ce qui fut fait et le résultat dépassa toutes les espérances. Le programme de destruction des centrifugeuses marchait parfaitement.

Contre toute attente, en 2010, le programme est sorti de l'usine iranienne pour se répandre sur le web à la suite semble-t-il d'une manœuvre d'un opérateur qui a connecté son portable au système de l'usine. Le virus a infecté en silence son ordinateur. Rentré chez lui, il a branché son portable sur Internet et le virus est sorti parti infecter d'autres ordinateurs du réseau. Les américains, affirment, off the record, que ce sont les israéliens qui ont modifié le programme car il devait être conçu, en principe, pour n'infecter que les systèmes qui géraient des centrifugeuses. Mais c'était trop tard la boite de Pandore avait été ouverte. Le virus a été analysé et le lien a été fait avec d'autres virus analogues. On peut consulter Wikipedia aux noms de « Duqu », « Stuxnet », « Flame » pour trouver les détails. D'une certaine façon ce virus est classique. Il pénètre dans les ordinateurs en exploitant trois « zéro day exploits de Windows » et vise le système SCADA « win CC sz Siemens ». D'un autre point de vue il très inhabituel par sa taille, un demi mégaoctet, et sa complexité. Il utilise ainsi de faux certificats de sécurité utilisés dans les procédures de mises à jour du logiciel Windows. En fait c'est un véritable logiciel professionnel, une boite à outil, qui permet de construire une infinité de virus pour différentes fonctions, de destruction, de vol de fichiers et de rapatriement de ces fichiers, codés, vers une destination extérieure à des fins d'espionnage. Il comporte aussi une fonction d'espionnage des activités d'un opérateur sur un ordinateur qui enregistre toutes les opérations au clavier et effectue toutes les copies d'écrans. Il possède aussi une fonction d'autodestruction qui le fait disparaître d'un ordinateur une fois son travail terminé. Bref c'est un virus qui réuni toutes les astuces et les

[35] cf *Confront and consceal* page 200

fonctionnalités des malwares des hackers découverts au cours de ces dix dernières années, mais poussées à leur maximum d'efficacité par des professionnels. Un nouveau virus, Flame, probablement dérivé de Stuxnet, vient d'être identifié et renforce ces analyses.[36]

[36] En fait, il vient de redéfinir complètement la notion de cyber-guerre et de cyber-espionnage », déclarait le 28 mai Aleks expert chez Kaspersky http:// www.dreuz.info%2F2012%2F05%2Fflame-le-nouveau-et-etrange-virus-de-la-cyber-guerre-contre-liran%2F&ei=1A5WUN7SJeKu0QWYpoDgCQ&usg=AFQjCNHQ6UsA762yC93nb1oX0IDp48J7uw

XVI. Le catalogue des attaques, Wikileaks, Anonymous, Lulz etc…

Les groupes de hackers, Wikileaks, les Anonymous, Lulz, etc… démontrent chaque jour que la sécurité des systèmes étatiques ou des grandes entreprises sont vulnérables malgré les précautions prises. Des failles dans les programmes et des erreurs humaines permettent de multiples pénétrations des systèmes et des vols de données.

Les attaques antérieures en Estonie et en Géorgie attribuées aux Russes, sans que la preuve soit certaine, comme les attaques contre les Tibétains, identifiées comme des attaques provenant de la Chine, montrent la fragilité des systèmes informatiques et la quasi impossibilité de les protéger, malgré les multiples sécurités mises en place contre les attaques, vol de données et dénis de service.

La dernière attaque documentée de septembre 2012 contre les installations pétrolières de l'Arabie saoudite, Saudi Aramco, attaque menée avec succès contre les PC de la compagnie, dénommée « Shamoon », le démontre encore une fois[37]. La revendication de cette attaque par la « Cutting Sword of Justice » rend encore plus complexe les attributions réelles de ces attaques.

Une compilation de différentes attaques subies par les institutions américaines a été publiée par Mac Affee[38].

[37] cf Shamoon wikipedia

[38] cf *Revealed: Operation Shady Rat, An investigation of targeted intrusions into more than 70 global companies, governments, and non-profit organizations during the last five years.* Mac Affee 2011

XVII. Les leçons d'Olympic Games

On peut analyser les conséquences de l'opération d'Olympic Games de deux points de vue différents.

On peut ne voir dans cette opération que la continuation d'une opération de renseignement et d'espionnage dans laquelle l'intervention d'un virus informatique, in fine, ne change pas radicalement la nature des opérations classiques de sabotage. D'ailleurs des opérations classiques de sabotage, sans intervention de l'informatique, ont été utilisées auparavant dans l'usine de Natanz. Sans grand résultat en ne faisant que ralentir le développement de l'enrichissement de l'uranium. Et les partisans de cette analyse, à l'appui de leurs dires, affirment que même avec Olympic Games, l'enrichissement n'a été que ralenti et non interrompu. Tout cela est vrai.

Mais on peut faire une autre analyse de l'opération Olympic Games.

Que la révélation de l'opération soit volontaire ou involontaire, l'essentiel est qu'elle a été maintenue secrète pendant cinq ans avant d'être révélée dans toute son ampleur par la presse, même si des rumeurs laissaient supposer l'existence d'une guerre informatique secrète. D'autres infections, d'autres réseaux d'ordinateurs infectés ont pu être construits, sans qu'on les détecte. Ainsi la vulnérabilité des systèmes informatiques apparaît dans toute son ampleur.

La révélation récente d'un nouveau virus, Gauss, spécialisé dans l'espionnage des banques, particulièrement de celles du Moyen Orient vient conforter ce point de vue.

Ainsi la construction de lignes Maginot qui protègeraient Windows ou Linux semblent illusoires, aussi sophistiquées soient-telles, surtout si on utilise les mises à jour de Windows qui permettent une intervention sur tous les fichiers des ordinateurs.

On voit que les conséquences de la révélation d'Olympic Games nous obligent à reconsidérer la sécurité, dans son ensemble et remet en cause les architectures logicielles les plus répandues, Windows, Linux et équivalents.

XVIII. Une leçon paradoxale du cyberespace

Le troisième enseignement paradoxal de la société numérique est que les propriétés du cyberespace renforcent l'importance du renseignement traditionnel. L'information ne pèse pas, on peut stocker cinq millions de livres ou des centaines de milliers de plans sur un disque de la taille d'un paquet de cigarette ou une clef USB. L'espionnage moderne, avec la pénétration des réseaux, permet de soustraire des quantités énormes d'informations, pertinentes ou non. L'intérêt d'une pénétration à distance s'en trouve augmenté.

Ainsi le « air gap », la pénétration d'un réseau non connecté à l'extérieur et à Internet par la présence d'une « taupe », devient extrêmement intéressant. Les gains d'informations envisagés sont de plusieurs ordres de grandeurs supérieurs à ce qu'ils étaient il y a seulement quelques dizaines d'années. Aussi les efforts de pénétrations humaines deviennent de plus en plus efficaces quand on les compare aux gains que l'on peut en espérer. Donc naturellement la maîtrise des cyberarmes et leur utilisation humaine devient un enjeu majeur de tous les services de renseignement et en particulier de la France qui est bien placée dans la maîtrise et l'invention des logiciels.

XIX. Une nouvelle arme dans le cyberespace, une nouvelle dissuasion ?

Nos sociétés industrielles et post industrielles vont devenir à terme, à un horizon d'une décennie, complètement numérisées et il faudra les caractériser comme des sociétés essentiellement numériques.

A ce titre de nouvelles vulnérabilités propres à l'utilisation universelle de logiciels vont survenir. La sécurité de ces sociétés et leurs défenses ne pourront plus être assurées seulement par les solutions d'aujourd'hui.

Il semble qu'il sera très difficile, voire impossible, de supprimer ces vulnérabilités étroitement associées à l'univers numérique. Pour faire face à cet état de fait très probable un courant de réflexion s'est donné pour tâche d'établir un parallèle entre une situation antérieure que nous avons connu avec l'apparition de l'arme nucléaire et les cyberattaques. Et donc armé de cette analogie, certains analystes proposent de traiter les cyberarmes comme on a traité les armes nucléaires.

Les analyses qui précèdent montrent d'une part le caractère incontournable de la numérisation de la société et la nouvelle sociabilité qui l'accompagne et, d'autre part, la très grande difficulté à supprimer les nuisances qui sont associées au développement de cette nouvelle technologie structurante.

La suppression des frontières dans le cyberespace, la disparition de la possibilité de contrôler les frontières géographiques d'un pays par des dispositifs de défense numérique rappellent son équivalent nucléaire avec les missiles intercontinentaux qui se jouent des frontières.

Le caractère massif d'une cyberattaque générale, capable de paralyser une société numérique, rappelle aussi le caractère massif d'une attaque nucléaire et son immense pouvoir de destruction.

La défense contre une attaque nucléaire étatique s'avère quasi impossible dans l'état actuel de la technologie actuelle et doit jouer d'une manière très défavorable contre les lois de la physique.

Les défenses antimissiles américaines ont surtout joué jusqu'ici un rôle politique, du SDI aux propositions de défenses antimissiles actuelles.

De la même manière il semble que la défense contre une cyberarme moderne soit en pratique quasi-impossible. Mais les analogies s'arrêtent là.

La réalisation d'un système d'armes nucléaires est du domaine d'un Etat. Ou d'un quasi-Etat. Elle se compte en milliards d'euros.

La réalisation d'une cyberarme mobilise quelques excellents informaticiens. Elle peut être quasi artisanale ou étatique comme les Anonymous et Wikileaks d'une part et les Etats Unis avec Olympic Games d'autre part le montrent.

La « livraison » d'une arme nucléaire nécessite une technologie coûteuse, un avion ou une fusée spatiale. L'attaque, à cause de son origine et à cause de l'ampleur de ses dommages et de la physique nucléaire elle-même, est signée.

Au contraire il est très difficile, sinon impossible d'attribuer avec une certitude raisonnable, une attaque par une cyberarme, à une place géographique, à un groupe d'individus, à un Etat.

Enfin les cyberarmes ouvrent un nouvel espace stratégique. Elles permettent des attaques d'un pays d'une nouvelle espèce. Jusqu'à aujourd'hui la violence de la guerre est toujours liée à la destruction et à la mort des adversaires, militaires et civils. Les armes modernes permettent de limiter en principes les dommages collatéraux civils ou militaires en augmentant la précision des attaques.

Les sociétés modernes recherchent pour leurs citoyens le « zéro mort ». Les cyberarmes opèrent un tournant stratégique en introduisant dans l'utilisation de la violence le « zéro mort » non seulement pour elles –mêmes mais aussi pour les adversaires. Les cyberarmes peuvent moduler leurs effets, dans des effets locaux ou globaux, du « zéro mort » aux dysfonctionnements globaux d'une société civile pouvant provoquer des morts « collatéraux » accidentels ou volontaires.

La cyberguerre ouvre ainsi un nouveau champ de conflits de nature très différente des conflits anciens et actuels, symétrique ou asymétriques.

Ces nouveaux conflits, qui peuvent être globaux, sans défense évidente possible, comme les conflits nucléaires, sont d'une nature radicalement différente.

Les cyberarmes sont ainsi des armes d'une espèce nouvelle d'autant plus efficaces qu'elles agissent sur des sociétés complètement numériques dans lesquelles tous les systèmes, les relations entre les personnes et entre les choses sont régies par des dispositifs informatiques communicants, dans lesquels le cyberespace joue un rôle central.

Ainsi on voit que les similitudes entre l'arme nucléaire et les cyberarmes sont partielles. Les différences sont grandes. Ces similitudes et ces différences permettent-elles la construction d'une politique de dissuasion ? Les différences sont trop grandes pour qu'on puisse plaquer des solutions élaborées avec la régulation de l'arme nucléaire[39].

[39] Une discussion approfondie des similitudes et des différences entre les armes nucléaire et les cyberarmes et une possible conceptualisation d'une cyber-dissuasion est celle de Martin Libicki de la Rand Corporation avec : *Cyberdeterrrence and cyberawar Rand Corporation 2009* http://www.rand.org

Table