INSTITUT DIDEROT

Les Carnets des Dialogues du Matin

NICOLAS ARPAGIAN

L'avenir de la cybersécurité

www.institutdiderot.fr

Les Carnets des Dialogues du Matin

NICOLAS ARPAGIAN

L'avenir de la cybersécurité

Retranscription de la conférence du 14 décembre 2009

Sommaire

Avant-propos

Une mutation de nos civilisations est en train de se produire sous nos yeux, sans que nous réalisions que son ampleur sera comparable à celle à laquelle la maitrise de l'énergie a donné naissance, mais dans un laps de temps beaucoup plus court : la généralisation des TIC (technologies de l'information et de la communication).

Internet est un moyen de communication très performant, mais c'est aussi la possibilité d'intégrer potentiellement, dans un seul système global, la totalité des informations numérisées existant dans le monde. Les capacités de traitement et d'acheminement de ces données étant illimitées, la combinaison des deux offre des perspectives infinies, d'autant que le champ des informations numérisées lui-même ne cesse de s'accroître au point que, demain, ce qui ne sera pas numérisé sera condamné à l'oubli : le moindre achat d'un consommateur signe sa localisation, son emploi du temps et, combiné à d'autres informations de nature aussi banale, ses goûts, ses revenus, ses fréquentations.

Comme toujours, la technologie est moralement ambiguë : cette fantastique puissance en train de naître facilite la recherche scientifique, peut favoriser le suivi de malades, permet de rompre la solitude de personnes isolées, élargit l'accès à la culture, abaisse le coût de distribution de nombre de produits de consommation, mais se présente en même temps comme un ensemble utile à la guerre et au crime : espionnage des organisations et des hommes, opérations de brouillage, d'intoxication et de subversion, attaque des réseaux d'intelligence et

de communication des adversaires (états entre eux, états face aux terroristes et aux opposants politiques, crime organisé face aux systèmes de protections et à leurs victimes potentielles, etc.).

Telles sont les perspectives décrites par Nicolas Arpagian. L'homme est certainement capable de s'adapter, mais à quelle vitesse, à quel prix et pour quel nouveau visage de la civilisation ?

Jean-Claude Seys
Président de l'Institut Diderot

L'avenir de la cybersécurité

La définition est connue depuis Carl von Clausewitz[1]. La guerre est donc un acte de violence destiné à contraindre l'adversaire à se soumettre à notre volonté. Pour ce faire, les technologies de l'information constituent sans doute une arme à part entière. Tant dans le rôle que jouent les réseaux de communication pour permettre le maintien en contact et le contrôle des troupes et des systèmes d'armes. Mais également en matière de guerre de l'information et d'opérations d'influence pour rallier à sa cause les opinions publiques. Par ce biais, les outils technologiques modernes tels qu'Internet ou les téléphones portables se sont désormais imposés au cœur des compétitions idéologiques contemporaines. Leur facilité d'accès et d'emploi, leur rapidité de diffusion et leur présence au sein des populations étaient autant de qualités attendues par les personnes désireuses de produire et de faire circuler des idées. Surtout qu'en l'espèce le rapport coût/efficacité en fait un arsenal à la portée de chaque militant ou activiste. Sur ce terrain, ce n'est plus seulement l'importance d'un budget publicitaire ou militaire qui permet de faire la différence, et de faire entendre sa voix, mais bien une connaissance fine des mœurs et usages du réseau des réseaux.

Le couple technologie/pouvoir des idées ne date évidemment pas de l'ère Internet. Dès sa création en 1915

1. Carl von Clausewitz, *De la guerre* (1832), Editions Payot-Rivages, 2006.

dans notre pays, la Section de Contrôle Télégraphique dispose par exemple d'un service chargé de la surveillance de la correspondance[2]. Cette notion est comprise au sens large puisqu'elle inclut les correspondances privées internationales, en provenance, à destination ou transitant par la France, les correspondances des prisonniers de guerre, la télégraphie privée nationale et la radiotélégraphie. C'est à dire tous les canaux de communications modernes d'alors. Pendant près d'un siècle, ce qu'Ulrich Beck[3] a appelé la « colonisation étatique » n'a fait que progresser ; les états revendiquaient le droit de contrôler les informations ainsi mises en circulation, un monopole qu'ils n'exercent plus seuls désormais puisque les grands réseaux de communication sont pour l'essentiel détenus et contrôlés par des firmes multinationales. De ce fait, la nature des données –et leur éventuelle surveillance– est d'abord envisagée au nom de la science *marketing*. En pistant les contenus, on est à même de proposer une publicité contextuelle vendue au meilleur prix à des sociétés commerciales désireuses de coller au plus près des attentes et envies de leurs prospects ou clients. Seule la sécurité nationale semble être l'autre justification acceptable aux yeux de l'opinion pour effectuer cette immixtion dans l'intimité des correspondances électroniques et des navigations des individus sur la Toile, à l'instar des dispositifs de contrôle mis en place à l'initiative des Etats-Unis dans les semaines qui ont suivi les attentats du 11 Septembre 2001.

Internet, présenté alors comme étant aussi la technologie permettant à des militants terroristes répartis sur le globe de communiquer entre eux et légitimant par la même toutes les formes de surveillance du réseau, est à l'inverse désigné comme symbole de liberté lors de la crise politique

2. Lire à ce propos, Hervé Kirsch (dir.), *La France en guerre économique*, IERSE/Vuibert, 2008.
3. Ulrich Beck, *Pouvoir et Contre-pouvoir à l'heure de la mondialisation*, Flammarion pour l'édition française, 2003.

qu'a traversé l'Iran au printemps 2009. Puisque le Département d'Etat a officiellement demandé au fournisseur du service réseau de la plateforme de *microblogging Twitter* (NTT America) de reporter des opérations de maintenance planifiées pour permettre une continuité de service optimale à un moment clé de l'actualité. En clair, il s'agissait de permettre aux opposants iraniens qui contestaient les résultats des élections présidentielles de disposer d'un moyen de communication entre eux, et à destination du reste de la planète. Car dans la foulée de la réélection de Mahmoud Ahmadinejad, les autorités de Téhéran ont choisi de fermer certains sites Internet et de bloquer l'envoi de SMS par téléphones mobiles. Seul *Twitter* restait alors en état de fonctionnement. Dans la guerre des idées, la maîtrise des vecteurs de communication devient un atout décisif. Quand il s'agit de prendre en main les rebondissements de l'actualité. Mais également en ce qui concerne les pages du passé.

George Orwell[4] nous avait prévenus : « Qui contrôle le présent contrôle le passé, qui contrôle le passé contrôle l'avenir ». A l'ère numérique, la notion de patrimoine culturel doit s'envisager de paire avec la digitalisation des contenus. Quand Internet, et surtout les moteurs de recherche, devient un peu plus chaque jour la porte d'entrée[5] sur toutes les formes de savoir (historique, politique, culturel…), il apparaît de plus en plus que le format numérique constituera la norme. Et en l'espèce *Google* exerce une domination sans partage : 67,5 % des recherches sur Internet seraient passées par son intermédiaire en 2009, selon le cabinet *ComScore*. Le deuxième opérateur mondial, *Yahoo*, ne serait sollicité par

4. George Orwell, *1984* (1948), Folio pour la traduction française, 1972.
5. Selon le cabinet ComScore, les internautes du monde entier ont réalisé en juillet 2009 plus de 113 milliards de requêtes via leur moteur de recherche, soit 41% de plus que l'année précédente.

les internautes que pour 7,8 % des requêtes. S'il elle n'est pas numérisée et correctement indexée, une information sera donc invisible aux yeux des moteurs de recherche. Et par voie de conséquence de moins en moins accessible au grand public. Puis à terme aux spécialistes qui auront pris le pli de ne s'appuyer que sur des recherches par voies électroniques. C'est ce qui donne toute sa saveur et son importance à la démarche précisément entreprise par *Google* de numériser les contenus de bibliothèques entières. Cette société dont la devise de ses deux fondateurs, Larry Page et Sergey Brin, est « Ne faites pas le mal » (« *Don't be evil* ») s'est donc auto-désignée pour établir une part conséquente du patrimoine culturel numérique de demain. En effet, forte de ses moyens budgétaires considérables, elle est largement en mesure de pallier le manque d'argent des bibliothèques publiques, qui ne sont aucunement capables de rivaliser avec de telles dotations dédiées à la numérisation de leurs contenus. Les atermoiements européens sur un projet d'envergure en la matière en sont la meilleure illustration,

Même le géant *Microsoft* a renoncé en 2008 à son programme de numérisation de livres, dont la rentabilité n'a pas été jugée suffisante à court terme. En France, par exemple, la Bibliothèque municipale de Lyon a autorisé *Google* depuis juillet 2008 à numériser gratuitement quelque cinq cent mille documents libres de droit d'auteur sur les 3,7 millions que possède l'établissement. En échange, la firme californienne s'autorise à exploiter ce fonds à des fins commerciales. *A priori* son mode opératoire est déjà connu : *Google* mise sur le trafic suscité par les internautes à la recherche de ces contenus pour vendre des espaces publicitaires et des liens sponsorisés. Un modèle économique qui peut rapidement transformer cet acteur de l'Internet en première bibliothèque du monde, et ainsi une privatisation *de facto* de la mémoire collective et des principales références culturelles disponibles. Avec, à la clé, la possibilité de rendre inaccessibles certains documents jugés indésirables. La mise au ban passera aisément

inaperçue aux yeux d'un internaute peu au fait du sujet qu'il recherche. En maîtrisant le contenu éditorial, on prend la main sur les informations qui permettront à l'internaute de se forger une opinion. Une position idéale quand il s'agit de former des esprits « bien faits ».

Pas sûr donc que la culture européenne, et *a fortiori* française puisse évoluer à armes égales dans un tel environnement. Selon les mots-clés, les modalités de référencement et les mises en page éditoriales retenues émergeront différents types de documents à l'issue de la requête de l'internaute. Cette sélection n'est pas neutre car elle menace de faire tomber dans l'oubli numérique des séquences entières de savoir et de création. Un péril qui ne semble pas si théorique que cela, d'autant plus si les exigences politiques venaient à être prises en compte.

Internet est certes un lieu formidable d'échanges, de dialogues et de mise à disposition d'informations, mais il reste profondément ancré dans la réalité politique du monde réel. Peut-être encore davantage que dans d'autres domaines d'activité, la convergence de la sécurité nationale et de l'Internet est importante. Ainsi, par exemple, le Président Barack Obama, à peine élu, planche sur un corpus législatif des plus innovants. En effet, selon les termes du *Cybersecurity Act of 2009* déposé devant le Sénat au printemps 2009, le président des Etats-Unis s'autorise à restreindre voire à couper l'accès aux réseaux privés de communication, au nom de la sécurité nationale. Soit des circonstances que l'Administration Obama évite soigneusement de préciser. A l'instar des législations étatsuniennes protégeant les actifs stratégiques du pays, est considérée comme « stratégique » toute activité que le président aura qualifié comme tel. Ce qui permet de réagir au cas par cas au fur et à mesure que l'actualité évolue. Cette formule a le double mérite d'assurer une réelle souplesse aux autorités de Washington et de laisser ses concurrents dans l'incertitude permanente, puisqu'ils encourent à tout instant le risque que leur domaine

d'activité soit considéré comme relevant de la priorité nationale ; avec toutes les exceptions au droit commun qui peuvent en découler.

Pour défendre ses intérêts, la France a par exemple choisi la méthode contraire. Ainsi, le décret 2005-1739 du 30 décembre 2005 réglementant les relations financières avec l'étranger a établi de manière limitative la liste des onze secteurs jugés stratégiques[6], pour lesquels des investissements hors Union européenne exigent l'accord du ministre de l'Economie. Tant pis pour les activités qui, à l'avenir, pourraient émerger. Sans un autre texte ministériel, elles ne bénéficieront d'aucun cadre spécifique.

Le pouvoir politique ne peut donc ignorer l'extraordinaire caisse de résonance que constitue le réseau, qui s'apparente désormais à une menace sérieuse dans les états autoritaires. Ainsi, la Chine a opté pour une solution radicale en limitant à deux le nombre d'opérateurs Internet et télécoms pour l'ensemble du pays. En 2009, Pékin a souhaité pousser plus avant sa surveillance en annonçant l'installation obligatoire dans les ordinateurs fabriqués en Chine, à partir du 1er janvier 2010, d'un logiciel de contrôle des images violentes et pornographiques. Au nom du respect des bonnes mœurs, voici que l'usine du monde envisage donc d'inclure un dispositif aussi intrusif. Evidemment, la pornographie est apparue ici comme un prétexte à l'installation d'outil

6. La liste précise est la suivante : les jeux d'argent, la sécurité privée, la Recherche & Développement des produits toxiques, les matériels d'interception & détection à distance des conversations, les technologies d'évaluation et de certification en matière de sécurité des systèmes d'information, les interventions en sécurité informatique chez certains opérateurs de service, les activités duales, les activités relatives à la cryptologie, les activités auprès des entreprises dépositaires de secrets de la Défense nationale, la recherche, production d'armes, explosifs & munitions. Et les activités auprès d'entreprises ayant signé des contrats d'études ou de fournitures d'équipement au ministère de la Défense.

de censure. Et il aura fallu attendre les réponses hostiles des clients de la Chine pour que les autorités du pays renoncent provisoirement à leur projet. Ce n'est pas l'argument démocratique qui l'a emporté mais bien la crainte de perdre des parts de marché en cas de boycottage des ordinateurs *made in China*. Quelques semaines plus tard, au début du mois de septembre 2009, c'est cette fois au nom de la lutte contre le piratage des œuvres musicales et audiovisuelles que Pékin a annoncé une surveillance accrue des communications électroniques sur son territoire. Les sites musicaux, comme par exemple ceux détenus par *Google* ou son concurrent chinois *Baidu* devront désormais obtenir un accord préalable des censeurs avant de distribuer des titres étrangers.

D'un point de vue organique, les services rendus par les technologies de l'information (TIC) ont une spécificité. Cette activité ne connaît pas dans nos sociétés occidentales d'équivalent en termes de « service public ». Alors que l'eau, les transports, la santé ou l'éducation existent dans une forme régie par l'Etat, les TIC sont généralement proposées dans une logique de marché. Seule exception héritée du temps des monopoles, la règle dit du « service universel » qui établit notamment que les citoyens doivent pouvoir accéder au téléphone partout sur le territoire, avec par exemple, le réseau de cabines téléphoniques. En matière d'Internet, l'offre alternative à celle du marché dépend de la stratégie menée par des acteurs institutionnels. Tels les restaurants *McDonald's* qui offrent l'Internet gratuit à leurs clients ou la Mairie de Paris qui le rend librement accessible aux personnes qui fréquentent les bibliothèques municipales ou les squares de la capitale.

Nous assistons donc à ce qu'Eric Delbecque[7] a qualifié de « métamorphose du pouvoir », où après les épreuves

7. Eric Delbecque, *La métamorphose du pouvoir – La chance des civilisations*, Vuibert, 2009.

de force du *hard power*, les opérations de *soft power* qui jouent davantage sur le registre de l'influence, de la séduction et des idées trouvent leur plein épanouissement dans nos sociétés hautement numérisées. Où les informations nous parviennent d'un clic, avec le sentiment que l'abondance de données nous met à l'abri de toute manipulation. Nous n'avons jamais eu autant d'informations disponibles, comment pourrions-nous donc être victimes d'ignorance ? Gare à cet aveuglement informationnel qui ne peut que fragiliser l'établissement de doctrines ou d'opinions qui nous sont propres, et non pas le fruit d'un syncrétisme diffus qui serait né de l'amalgame mal digéré de la masse de points de vue glanés sans discernement sur la Toile. L'excès de confiance suscité par une apparente accumulation de savoirs peut se révéler être une menace fatale à nos démocraties, le tout dans le confort ouaté de notre salon, face à un ordinateur toujours prêt à nous abreuver d'informations maîtrisées par d'autres.

« Les Rafales de l'Aéronavale ont été cloués au sol par une attaque informatique ». Cette information qui a circulé[8] fin janvier 2009 sur la Toile illustrait à nouveau la capacité du cyberespace à devenir un champ de bataille. De quoi s'agissait-il ? D'un réseau informatique de la Marine nationale qui a effectivement été contaminé, vraisemblablement à la fin de l'année 2008, par le virus *Conficker*. Mais pas au point de paralyser les aéronefs ; des dispositifs de secours, qui permettent de supplanter des installations provisoirement défaillantes ou suspectes d'abriter des logiciels malveillants, ayant pu être activés. La phase la plus longue était désormais de repérer dans les méandres de ces réseaux la trace du virus afin de veiller à son nettoyage en bonne et due forme. Car *Conficker* a la particularité de neutraliser les solutions de sécurité qui lui sont destinées, en faisant croire au gestionnaire des

8. Comment le virus *Conficker* a paralysé les armées, *Lettre Intelligence On Line* n°587 du 5 au 18 février 2009.

infrastructures que les réparations ont été correctement effectuées. Pas question donc d'installer les « patchs » de sécurité proposés par l'éditeur, en l'espèce Microsoft, tant que les informaticiens de la Défense n'ont pas la certitude d'avoir expurger leurs serveurs de toute présence de ce logiciel malveillant.

Quelles leçons peut-on d'ores et déjà tirer de cet événement ?

1) La cyberguerre est d'abord une guerre des technologies de l'information et de la communication.
   Celles-ci sont un actif stratégique qu'il convient de maîtriser et de protéger, car elles permettent dans une organisation de plus en plus numérisée de donner corps à la chaîne de commandement, et font en sorte que, de l'état-major aux personnels engagés sur un théâtre d'opérations les ordres soient connus et transmis en toute intégrité. Sans un système d'informations opérant, il devient périlleux –voire hasardeux– de mener aujourd'hui une entreprise d'envergure. Sans parler forcément de « dépendance numérique », on doit être conscient de la nécessité de disposer en permanence d'outils pleinement opérationnels. Or, ces équipements ont un coût : d'acquisition, d'entretien et de développement, avec, en outre, la nécessaire formation des équipes chargées de les exploiter au quotidien. En période de disette économique et budgétaire, il ne faudrait pas voir là qu'un poste de dépenses, mais bien des investissements stratégiques pour le maintien d'une souveraineté nationale à part entière.

   C'est le maillon indispensable à toute organisation moderne. Leur fiabilité doit être une préoccupation de tous les instants. Ainsi, au mois de mai 2008, plusieurs institutions de la défense des Etats-Unis (l'École Navale, le Centre de guerre aéronavale, la principale base aérienne US en Allemagne qui se trouve à Spangdahlem…), et aussi la firme Raytheon, qui fabrique notamment le missile *Patriot* rendu

célèbre pour son efficacité contre les *Scuds* irakiens pendant la première Guerre du Golfe, ont été alertées par le FBI du fait de fortes présomptions[9] quant à d'éventuelles contrefaçons d'origine chinoise sur les serveurs Cisco Systems et autres équipements informatiques achetés dernièrement par ces honorables entités. Et, plus grave, ces équipements *high tech* contiendraient des logiciels facilitant l'entrée et la circulation dans les réseaux informatiques auxquels ils sont reliés, soit une porte d'entrée hors pair dans les coulisses de la Défense des États-Unis. Une manière de faire qui, si elle était confirmée, relativiserait évidemment les procédures de protection pouvant être mises en place par le plus appliqué des responsables de la sécurité informatique.

2) La cyberguerre est également une guerre par l'information

Pas question de verser dans une quelconque théorie du complot. Toutefois, on ne doit pas sous-estimer l'impact de tels assauts informationnels. En effet, communiquer sur des avions de combat incapables de décoller à cause d'une clé USB contaminée fichée dans un réseau informatique peut se révéler dévastateur pour l'image de marque et la crédibilité d'une armée. Donc, d'une nation et de ses technologies. Ceci d'autant plus que la matière est suffisamment complexe d'un point de vue technique pour que les présentations qui en seront faites soient simplifiées à l'extrême, notamment par les relais que constituent les médias. Autant d'occasion de diffuser des informations erronées. Dans ce cas là, tout est possible : de l'imprécision véhiculée de bonne foi par des interlocuteurs peu au fait des technologies, à des relais structurés et bien décidés à nuire par l'amplification de nouvelles négatives. Pour résumer,

9. FBI : China may use counterfeit Cisco routers to penetrate US networks, 15 mai 2008, www.worldtribune.com

cela va de l'intervention des « idiots utiles » à celle de professionnels de la désinformation et de la manipulation. La rumeur constitue une arme à part entière : dénigrements, diffusion de fausses nouvelles… tout est bon pour fragiliser sa cible. Déjà en conflit avec son partenaire local Wahaha, Danone doit par exemple faire face depuis la mi-février 2009 à une campagne de mobilisation sur la Toile visant sa filiale chinoise, Dumex. Des forums sur Internet et des échos dans la presse relaient alors l'information, non vérifiée, selon laquelle 48 bébés auraient été contaminés en Chine, avec des maladies rénales à la clé, après avoir consommer du lait en poudre fabriqué par Dumex. Quelques mois après le scandale du lait chinois contenant de la mélamine, au point d'en faire une boisson mortelle, c'est donc une attaque en règle contre les positions commerciales du producteur tricolore. Sans qu'aucun coup de feu ne soit tiré ou aucun éclat de voix ne soit entendu, c'est bien un nouvel acte de guerre économique dans laquelle le cyberespace serait transformé en gigantesque terrain d'affrontements.

La conduite de telles opérations de cyberattaques suppose de disposer de profils qui allient la maîtrise des technologies de l'information à un véritable savoir-faire dans le domaine de l'influence. Soit, des compétences que l'on n'enseigne pas forcément dans les cursus classiques des écoles d'ingénieurs, de commerce, voire à l'École Nationale d'Administration, à l'instar d'un Premier ministre de la France de la fin du XX^{ème} siècle, dont le biographe –et pourtant ancien conseiller– écrivait : « L'ordinateur qui trône sur son bureau est plus un presse-papiers qu'un outil de travail ». Au-delà de la formule, il serait souhaitable que les enjeux technologiques soient davantage intégrés parmi les composantes des politiques publiques : réforme de l'Etat, politiques d'intelligence économique, aménagement effectif du territoire…

La cyberguerre possède en outre une caractéristique importante : la victoire n'est non seulement jamais acquise,

mais elle s'établit avec difficulté. La conquête d'un territoire physique peut se comprendre en termes matériels, avec l'occupation d'une région et le contrôle de sa population, ce qui n'est assurément pas le cas dans l'univers cybernétique, où toute position est forcément précaire, et dépendante de la créativité et de l'imagination de ceux qui cherchent à l'attaquer. Pleinement conscients de cette menace, les Chinois ont opté pour un contrôle intégral du Net sur leur territoire, en surveillant étroitement les points d'accès. En effet, l'Internet chinois est géographiquement coupé en deux. La société China *Netcom*[10] gère le nord du pays, tandis que *China Telecom*[11] alimente le sud. Ces deux sociétés sont concurrentes, et les interconnexions entre leurs deux réseaux restent encore de piètre qualité, par exemple, dans le cas d'un internaute installé dans le sud qui souhaiterait se connecter à un site basé dans le nord. Ou *vice versa*. Pékin pourrait même profiter de la masse largement critique que représente sa population pour se doter de son propre réseau. Totalement isolé du reste du monde, il fonctionnerait en vase clos. Même si les précédentes expériences techniques allant dans ce sens ont toutes été des échecs, cela reste un scénario envisageable.

Si les campagnes de cyberguerres se multiplient, il s'agira pour les autorités politiques de veiller à la manière dont elles communiqueront à leur propos auprès de leurs opinions publiques. D'abord, en ayant conscience que celles-ci pourront déjà être informées par leurs propres moyens. Ensuite, en établissant un moyen d'expression crédible aux yeux des populations pour que la prise de parole des gouvernants, en période de crise, reste audible. En clair, comment assurer à ses concitoyens que les informations présentées sur les sites gouvernementaux sont sincères et véridiques quand des informaticiens

10. http://www.china-netcom.com/eng/global/home.htm
11. http://www.chinatelecom-h.com/eng/global/home.htm

chevronnés sont capables de placer sous leur contrôle ces vitrines en ligne ? À l'instar des sites gouvernement aux géorgiens qui, au cours de l'été 2008 ont vu les portraits de leurs ministres remplacés systématiquement par des photographies d'Adolf Hitler… Une opération de déstabilisation attribuée aux Russes qui conduisaient alors d'importantes opérations militaires dans cette région.

Loin de se cantonner à une compétition technologique, la cyberguerre exige donc une réponse globale de la part des décideurs gouvernementaux et de la haute administration. En prenant en compte les aspects managériaux, stratégiques, politiques, médiatiques, économiques… et techniques. C'est donc une composante essentielle d'une nouvelle stratégie globale de sécurité nationale à laquelle les pouvoirs publics sont appelés à donner corps.

Enfin, les particuliers sont assurément une composante de l'avenir de cette cybersécurité. Pas seulement parce qu'ils détiennent de plus en plus à leur domicile des équipements informatiques plus performants que ceux qui sont mis à leur disposition sur leur lieu de travail, mais bien parce que l'activité Internet au sens large (navigation sur la Toile, courriers électroniques, messageries instantanées, jeux vidéos en ligne, *e-formalités* administratives…) occupe et occupera une place grandissante dans leurs vies quotidiennes. Il est désormais entré dans les mœurs, à tort ou à raison, pour des millions de nos compatriotes de présenter leur famille par le menu sur le réseau, de détailler les moindres étapes de leur parcours professionnel (avec les plateformes d'échanges *Viadeo, Linkedin*…) ou sentimental (*Meetic*…). Et les fonctionnalités nouvelles révélées chaque semaine par les opérateurs de ces services Internet ne vont faire, dès lors que les utilisateurs s'en saisissent, qu'accentuer cette mise à nue numérique, à l'instar de ces téléphones portables qui vous proposent de signaler à tout instant votre présence, grâce à la

géolocalisation via le GPS intégré, à vos « amis » afin que vous puissiez le cas échéant rencontrer celui ou celle qui se trouve à proximité. Présenté sous le prétexte de passer du temps avec des proches, un tel dispositif représente par ailleurs un formidable outil de suivi des individus ; certains parleraient de « flicage ».

De même, sur le réseau cette fois, quand votre moteur de recherche favori enregistre consciencieusement chacune de vos requêtes. L'objectif affiché est de mieux vous connaître afin de vous apporter chaque jour les réponses les plus adaptées à vos attentes. L'enfer est pavé de bonnes intentions, disait-on à l'ère pré-Internet… Blague à part, cette fréquentation assidue du Net et des accessoires numériques qui l'accompagnent (cartes bancaires, cartes de fidélité de commerçants, lecteurs numériques de musique, lecteurs de films…) conduisent inévitablement à une série de renoncements successifs à des pans entiers de notre sphère privée. A chaque inscription, acte d'achat ou séance de « surf » sur la Toile, nous nous délestons ainsi de bribes de notre intimité. Rien de si grave, certes, même si ces pertes, au final, sont conséquentes. D'autant plus qu'il n'existe pas de retour en arrière possible : contrairement aux discours ambiants de certains prestataires en *e-réputation*. En effet, l'information disponible sur Internet ne peut être supprimée par votre seule volonté. Au mieux, elle peut être « enfouie » dans les tréfonds des classements de réponse des moteurs de recherche, et donc être rendue moins facilement accessible pour l'internaute *lambda* qui ne maîtrise pas les techniques d'investigation numérique.

Le tour de force réalisé par le journal indépendant *Le Tigre*[12] à la fin de l'année 2008 constitue peut être la démonstration la plus flagrante de cette société de la transparence qui s'annonce. En effet, un journaliste

12. *Le Tigre*, n°28, novembre-décembre 2008 : www.le-tigre.net

s'est saisi au hasard de l'existence d'un jeune Bordelais trouvée par hasard sur un forum Internet. En prenant le temps de ratisser les sources ouvertes, c'est-à-dire les sites et supports accessibles gratuitement et en toute légalité par n'importe quel internaute, la rédaction est parvenue à reconstituer avec un luxe de détails chacun des événements de la vie personnelle, scolaire, professionnelle et même sentimentale de cet individu, de ses lieux et activités de vacances, en passant par son téléphone portable. Pour appuyer sa démonstration, la version papier du journal mentionnait l'identité précise du jeune homme, tandis que celle disponible sur Internet était anonymisée. La preuve était ainsi faite que ce ne sont pas tant les données dispersées qui sont intéressantes, voire utiles, mais bien leur agglomération, leur synthèse et leur recoupement. Ce qui est faisable pour un étudiant en architecture à qui l'on ne souhaite aucun mal, est évidemment tout aussi accessible quand on vise une personne que l'on souhaite déstabiliser, ou avec laquelle on souhaite entrer en contact. On parle alors de *social engineering* ou ingénierie sociale. Une activité autrefois réservée au petit monde de l'espionnage qui souhaitait cerner le profil de sa cible avant de l'approcher. Ces techniques sont aujourd'hui à la portée d'un clic pour la très grande majorité de nos contemporains.

Et pour ce qui reste encore du domaine de l'inatteignable, *Google* a ouvert en avril 2010 un site[13] fort instructif. Il recense les demandes qui lui ont été faites ces derniers mois par les gouvernements étrangers. Qui réclamaient soit la suppression de certains contenus. Soit les données personnelles de certains internautes.

13. www.google.com/governmentrequests

Demandes des gouvernements faites à Google
Juin 2009 à décembre 2009

Demandes de suppression de contenus		Demandes de suppression de contenus	
Brésil	291	Brésil	3 663
Allemagne	188	Etats-Unis	3 580
Inde	142	Grande-Bretagne	1 166
Etats-Unis	123	Inde	1 061
Corée du Sud	64	France	846
Grande-Bretagne	59	Italie	550
Italie	57	Allemagne	458

Source : Google, 2010.

Pour le deuxième semestre 2009, on note ainsi que si la France occupe la cinquième place des nations qui réclament le plus souvent des données personnelles (846 requêtes) à Google, elle a sollicité moins de dix fois le retrait d'un contenu. Et a obtenu satisfaction dans 66 % des cas. De nombreux internautes ont appris à cette occasion que le célèbre moteur de recherche détenait une quantité impressionnante de données concernant ses utilisateurs : le contenu de leurs recherches sur le Net, leurs courriers électroniques, l'historique de leurs navigations sur la Toile, leurs lieux de connexion ainsi que la configuration de leurs ordinateurs… Le tout sur une période de neuf mois.

Même si les demandes de suppression de contenus ne concernent que les sociétés appartenant à la sphère de *Google Inc.* (notamment les sites de partage de vidéos *YouTube*, de stockage de photographies *Picasa* ou la plateforme de blogs *Blogger*), cette publication rappelle que les états souhaitent exercer leurs droits sur le Net. Et que pour y arriver, ils doivent solliciter des prestataires privés qui sont de dimension mondiale.

Sans verser dans la paranoïa ni dans un optimisme béat, il convient donc de prendre toute la mesure de ce monde numérique qui se construit autour de nous. Et à qui nous confions de plus en plus de nous-mêmes. Ceci exige une prise de conscience par le plus grand nombre, puisque chacun devient un consommateur assidu des enjeux stratégiques de cette Toile, qui ne doivent pas rester l'apanage d'une catégorie spécifique (informaticiens, équipes marketing, militaires…) mais bien faire l'objet de débats publics dépassionnés.

C'est cela, aussi, la société de l'information qui s'annonce.

Retrouvez l'intégralité du débat sur www.institutdiderot.fr

Dans la même collection

L'avenir de l'automobile
Louis Schweitzer

Les nanotechnologies
& l'avenir de l'homme
Etienne Klein

L'avenir de la croissance
Bernard Stiegler

L'avenir de la régénération cérébrale
Alain Prochiantz

L'avenir de l'Europe
Franck Debié

Les Notes de l'Institut Diderot

L'euthanasie, à travers le cas
de Vincent Humbert
Emmanuel Halais

Les Dîners de l'Institut Diderot

La Prospective, de demain à aujourd'hui
Nathalie Kosciusko-Morizet,
Secrétaire d'Etat à la Prospective
et au Développement de l'économie numérique.

L'avenir de la cybersécurité

Entré en moins d'une décennie au cœur des foyers, des entreprises, des administrations et des états-majors, Internet constitue un outil de contrôle hors normes mais porte en lui des menaces majeures en raison de la dépendance numérique dans laquelle se trouvent des pans entiers de nos systèmes politiques et économiques.

Les cyberattaques et leurs possibles conséquences dramatiques justifient-elles l'établissement d'une société de surveillance ? En quoi la cyberguerre peut-elle caractériser les nouvelles formes de conflit ? Quelles sont les réponses des démocraties face à de tels enjeux ? Cette sécurité mérite-t-elle que nous lui sacrifiions l'essentiel de notre vie privée ?

Nicolas Arpagian

Rédacteur en chef de la revue *Prospective Stratégique*, Nicolas Arpagian est coordonnateur d'enseignements à l'Institut National des Hautes Etudes de la Sécurité et de la Justice (INHESJ). Egalement Chargé de cours à l'IRIS & à l'Université Paris Ouest, il est notamment l'auteur de *La Cybersécurité* (Que Sais Je ?) à paraître en 2010.

INSTITUT DIDEROT

FONDS DE DOTATION POUR LE DEVELOPPEMENT DE L'ECONOMIE SOCIALE REGI PAR LA LOI N°2008-776 DU 4 AOUT 2008 – SIRET N° 513 746 651 00019
11, place des 5 martyrs du lycée Buffon 75014 Paris / T. +33 (0)1 53 10 65 60 / F. +33 (0)1 53 10 65 36
contact@institutdiderot.fr / www.institutdiderot.fr