Que sais-je ?

LA CYBERSÉCURITÉ

Nicolas Arpagian

puf

QUE SAIS-JE ?

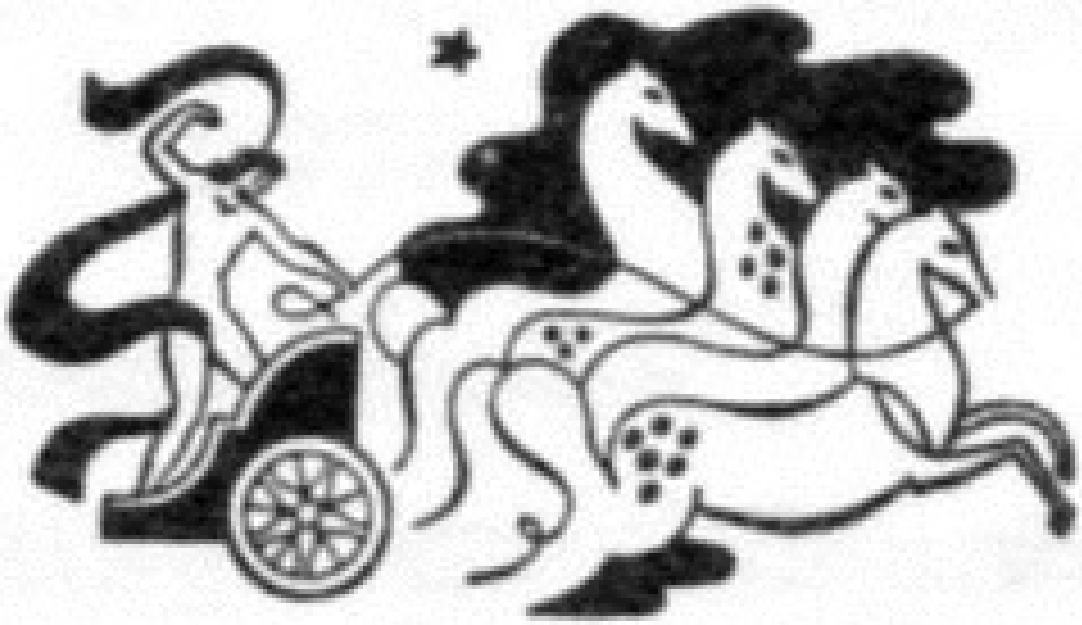
La cybersécurité

NICOLAS ARPAGIAN

Rédacteur en chef de la revue *Prospective stratégique*

Coordinateur d'enseignements à l'Institut national

des hautes études de la sécurité et de la justice (INHESJ)



Introduction

Le 21 avril 2010 a été la date choisie par Google pour lancer son nouveau service[1] *Government requests,* littéralement « requêtes gouvernementales ». Ce dispositif illustre de manière emblématique la question de la cybersécurité. En effet, il recense pour la première fois, pays par pays, les demandes d'accès aux données privées des internautes faites à Google[2] par les gouvernements du monde entier ainsi que le nombre des demandes de suppressions de contenus émanant de ces mêmes autorités politiques. Une sorte de palmarès permanent de la censure sur la Toile ? Pas si simple. Puisque certains pays sont exclus d'office de cette recension, telle la Chine qui estime que ces informations relèvent du secret d'État.

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.

Informations sur la vie privée, surveillance des contenus et éventuelle suppression de certains d'entre eux, enregistrement des sites visités sur la Toile… Voici donc résumés les grands enjeux de la sécurité numérique. Qui ne feront que progresser au fur et à mesure que se déploieront les usages mobiles d'Internet et que la population des internautes augmentera. De l'enfant qui fait ses premiers pas sur le Net, au chef d'entreprise qui utilise des serveurs informatiques pour faire fonctionner son activité en passant par les forces armées, chacun est dorénavant concerné par cette activité cybernétique. Qui suscite des attaques, des ripostes et des tentatives de protection technologiques. Ce nouveau champ de bataille est par essence planétaire et voit s'affronter des intérêts de puissance protéiformes. Pouvoirs politiques, acteurs économiques ou militaires sont tour à tour dans la posture

de l'agresseur et de l'agressé. Avec – fait nouveau – la possible participation d'individus isolés ou de militants désireux de faire triompher leur cause sur le forum mondial que représente désormais Internet.

Dans ce monde-là, les industriels du numérique détiennent des capacités d'action, notamment financières, comparables à celles d'un État souverain. La cybersécurité devient alors la condition nécessaire du développement de nos sociétés modernes. Au détriment, souvent, du droit individuel à la vie privée.

Notes

[1] www.google.com/governmentrequests/
[2] Les demandes de suppression de contenus concernent le site de partage de vidéos YouTube, de stockage de photos Picasa ou la plateforme de blogs « Blogger ».

Chapitre I

Définition et historique de la cybersécurité

I. Cybersécurité : de quoi parle-t-on ?

La création du mot « cybernétique » revient à un professeur au Massachusetts Institute of Technology (mit), Norbert Wiener, qui, dans un ouvrage [1] publié en 1948, désigna par ce vocable le « champ entier de la théorie de la commande et de la communication, tant dans la machine que dans l'animal ». Il l'a construit à partir du grec *kuberneïn,* qui signifie « diriger ». C'est plusieurs décennies plus tard, en 1984, que l'auteur de science-fiction William Gibson utilise le terme de cyberespace dans

son roman *Le Neuromancien*. Il s'agit d'une trilogie qui a pour personnage central un voleur de données. Celui-ci est en mesure d'établir des connexions entre son esprit et un réseau mondial reliant entre eux des ordinateurs.

Peu à peu, le préfixe *cyber* va participer ainsi à la construction de nouveaux substantifs relatifs à cette société de l'information qui a vu le jour à compter de la fin du xx^{e} siècle. La cybersécurité va donc concerner les usages défensifs et offensifs de ces systèmes d'information qui irriguent désormais nos organisations modernes. Elle prend en compte les contenants, c'est-à-dire les moyens techniques (réseaux informatiques, téléphoniques, satellitaires…) utilisés pour l'échange de données, qui peuvent faire l'objet d'opérations d'infiltration, d'altération, de suspension voire d'interruption, comme les contenus, c'est-à-dire l'ensemble des informations qui circulent ou sont stockées sur des supports numériques (sites Internet, bases de données, messageries et communications électroniques, transactions dématérialisées…).

La cybersécurité porte aussi bien sur la protection et l'attaque d'équipements informatiques (la guerre pour ou

contre l'information), afin de les surveiller ou d'en prendre le contrôle, que sur les renseignements disponibles sur la Toile (la guerre par l'information), avec de possibles atteintes à la réputation, le vol de données sensibles, des actions de piratage numérique et autres campagnes de dénigrement.

Ce nouveau théâtre d'ombres consacre le principe de la guerre asymétrique, où les parties prenantes n'ont plus nécessairement la même nature juridique ni *a priori* la même puissance : des États peuvent êtres attaqués par des militants isolés, des sociétés commerciales être visées par des services de renseignements gouvernementaux ou la cible de compétiteurs indélicats, des particuliers mis en cause par d'autres personnes privées. Sur ce terrain numérique, la taille des budgets de communication et de sécurité informatique ne garantit pas l'avantage.

L'imagination, la créativité et la maîtrise technique des pirates informatiques sont capables de contourner bien des systèmes de sécurité établis. La logique de guérilla joue à plein : des activistes parviennent à harceler – et finalement à mettre en difficulté – des adversaires disposant de moyens substantiels (entreprises, administrations, forces

armées…). Et le champ des menaces possibles est aussi vaste que la présence grandissante des technologies de l'information et de la communication dans les structures administratives, économiques, commerciales, financières, industrielles, médicales ou militaires. Auxquelles s'ajoutent nos usages personnels qui sont de plus en plus numérisés (blogs, messageries instantanées, télédéclarations fiscales, réseaux sociaux…).

L'actuel réseau Internet puise son origine dans le souhait exprimé dès 1962 par les autorités états-uniennes, notamment l'Advanced Research Project Agency (arpa), l'agence gouvernementale spécialisée en R&D (Recherche &Développement) technologique, de disposer d'un système de communication qui résisterait à une attaque nucléaire massive émanant de l'Union soviétique. C'est l'Université de Californie-Los Angeles (ucla) qui élabore ainsi à partir de 1969 le réseau Arpanet, dont l'Internet contemporain n'est qu'un prolongement. Sur ce terrain de l'innovation, la France n'est pas en reste puisqu'en 1971, l'ingénieur en informatique Louis Pouzin pilote le projet Cyclades, qui relie alors 25 ordinateurs installés en France, en Italie et au Royaume-Uni afin de permettre à des chercheurs de collaborer à distance. Pour ce faire, il met au

point le premier réseau mondial dit « à commutation de paquets », fondé sur la technique du datagramme, encore employée sur le Net. Intéressés par ce savoir-faire, les universitaires Vinton Cerf de l'ucla et Robert Kahn de l'arpa s'en servent largement pour bâtir, à la fin 1973, leur premier protocole de communication (tcp/ip).

Cyclades fonctionne jusqu'en 1979, mais ce programme n'est pas jugé prioritaire par le gouvernement français. Et faute de moyens financiers suffisants, il est finalement abandonné, laissant aux États-Unis la possibilité d'investir pleinement ce secteur d'avenir… Avec une constante depuis cette époque : sa construction sous la forme d'une toile (en anglais, *web*) d'araignée. Soit un maillage qui ne connaît pas de point central et qui permet à l'information de circuler même si le réseau est partiellement détruit.

Comme les générations d'outils de communication qui l'ont précédé, Internet a suscité et suscite encore des comportements ambivalents : d'une part, des détournements variés de la part de surdoués de l'informatique pour passer outre les sécurités ou monter des escroqueries, et d'autre part, une surveillance attentive des autorités gouvernementales qui interviennent très tôt

dans l'histoire du réseau des réseaux. Rappelons ici pour mémoire que la France s'est dotée dès 1915 d'une Section de contrôle télégraphique afin d'inspecter les correspondances postales et télégraphiques en provenance, à destination ou transitant par son territoire. Quant aux pirates du téléphone, ils commencent à sévir dès les années 1960. Tel ce John Draper qui s'aperçoit que le sifflet offert avec les céréales Capt'ain Crunch émettait opportunément une tonalité de 2 600 mégahertz. Or, les centraux téléphoniques d'alors l'interprétaient comme une consigne de ne pas facturer l'appel. De même, les *blue boxes* – ces boîtiers électroniques permettant de stopper la facturation des télécommunications à l'insu des opérateurs ont longtemps été le cauchemar des compagnies de téléphone états-uniennes.

Avec sa diffusion croissante parmi la population et dans la vie en général, Internet ne pouvait certainement pas faire exception. Ainsi, les États ont chacun opté pour des dispositifs de contrôle ou de filtrage des communications numériques. Tant pour anticiper de possibles agressions que pour porter des coups à leurs adversaires. Fait nouveau sur cette nouvelle scène géopolitique : les entreprises y jouent un rôle comparable à celui dévolu

jusqu'alors à des pays. Ainsi, la société Google a-t-elle été amenée à négocier presque d'égal à égal avec le gouvernement de Pékin, fin 2009, lors d'un contentieux sur la censure de l'information pour les internautes chinois. Il en est allé de même des géants mondiaux comme l'éditeur de logiciels Microsoft ou le portail Internet Yahoo. Leur puissance financière, la masse de leurs utilisateurs, et leur savoir-faire technologique en font des acteurs politiques à part entière.

II. Pas de moyens de communication sans contrôle des États

Selon l'institut Forrester Research, le monde devrait compter en 2013 quelque 2,2 milliards d'internautes. Ce qui représenterait une progression de 45 % en cinq ans, puisque l'évaluation 2008 recensait 1,5 milliard d'utilisateurs du Net. Et cela, indépendamment de la crise économique ambiante. La connexion au réseau devenant une priorité, les familles préfèrent rogner sur d'autres dépenses.

Cet accès à la technologie bouleverse l'équilibre des forces en présence sur la Toile. Par exemple, l'Amérique du Nord, qui représentait 17 % de la population mondiale connectée en 2008, tombera à 13 % en 2013. L'Europe passera également de 26 % à 22 %. Tandis qu'à l'inverse, la zone Asie-Océanie grimpera de 38 % à 43 %. Autant de données factuelles que la réalité géopolitique ne pourra longtemps ignorer. Notamment en ce qui concerne la gouvernance future de l'Internet.

L'apparition de moyens modernes de communication a systématiquement été accompagnée par la mise en place d'organes étatiques de surveillance. Ainsi, les États-Unis et la Grande-Bretagne ont-ils signé, dès 1943, un accord de coopération destiné à venir à bout des mécanismes de cryptographie utilisés par les Allemands avec leur machine *Enigma*. Leur réussite en la matière les incite, quatre ans plus tard, à élaborer un pacte baptisé ukusa (United Kingdom-usa) qui donne par la suite naissance au réseau *Échelon*. Son rôle ? Surveiller les communications téléphoniques, les télécopies et désormais les courriers électroniques. Pour couvrir l'ensemble de ces moyens de correspondance, les États membres dudit réseau (parmi lesquels, outre les deux fondateurs, se trouvent le Canada,

l'Australie, la Nouvelle-Zélande, l'Allemagne ou la Turquie) emploient une large gamme d'outils technologiques : un maillage de stations satellitaires, des bretelles placées sur des câbles sous-marins de télécommunications…

Une fois ces capteurs installés, des outils *ad hoc* sont utilisés en fonction de chaque type de support : logiciels de reconnaissance vocale, lecteurs optiques, dispositifs d'extractions de données et d'évaluation de contenus. La règle appliquée ici est simple : on écoute tous les échanges et on tâche d'y repérer les messages intéressants. Bien évidemment, la marque d'intérêt évolue en fonction du contrôleur. Certains privilégient les informations politiques, d'autres se montrent surtout attentifs aux renseignements économiques ou commerciaux.

Qui contrôle les critères de recherche détient donc un pouvoir considérable. Dans le cas d'*Échelon,* des pays comme la Turquie ou la République fédérale d'Allemagne ne peuvent que formuler des requêtes auprès des États à l'origine du réseau. Ces derniers sont donc informés des sujets de préoccupation de Berlin et Ankara, et peuvent même sélectionner l'information qui leur est adressée –

avantage stratégique tout à fait conséquent.

Étant donné le nombre croissant d'informations que les entreprises, les individus et les administrations placent au quotidien dans des bases de données et échangent sur la Toile, on comprend aisément que les États ne peuvent renoncer à exercer leur autorité sur ces territoires numériques. Ils doivent d'autant plus donner de la voix et se placer sur le terrain de la sécurité nationale qu'ils sont souvent des joueurs de poids moyen, voire léger, en ce qui concerne leur capacité d'intervention financière. Au 31 mars 2010, Google annonce disposer d'une réserve financière de 26,5 milliards de dollars. Une cagnotte qui, selon les chiffres transmis par Google, a donc progressé de deux milliards par rapport à fin décembre 2009.

Pour rester un interlocuteur crédible, les États démocratiques doivent par conséquent jouer la carte de la collaboration avec leurs champions nationaux.

C'est ce qu'a annoncé très clairement Barack Obama dans un discours [2] prononcé à la Maison Blanche le 29 mai 2009, dans lequel il indique que l'infrastructure numérique du pays doit être traitée pour ce qu'elle est, c'est-à-dire un « bien stratégique national » *(a strategic national asset),* sa

défense devant être considérée comme une priorité de sécurité nationale. Pour ce faire, sans doute davantage encore que dans les autres activités économiques, le Président Obama annonce une montée en puissance des collaborations à conduire entre acteurs publics et privés. Et donc une association de plus en plus étroite entre les sphères politiques, économiques et militaires.

En Russie, on trouve une autre illustration de cette implication de l'appareil d'État dans la sécurisation, en l'espèce la surveillance des réseaux de communication. En février 2008, Leonid Reiman, alors ministre chargé des Télécommunications, signe un décret qui oblige les fournisseurs d'accès à Internet et tous les opérateurs privés de téléphonie installés dans la Fédération de Russie ainsi que dans plusieurs pays de la Communauté des États indépendants (cei) de connecter leurs serveurs sur la base Sorm. La gestion de celle-ci relève directement de l'organe policier héritier du kgb, le fsb. Ainsi, le service de renseignements intérieur dispose en temps réel des moyens de contrôler les communications téléphoniques et Internet qui circulent dans sa zone d'influence.

Là encore, c'est au nom de la sécurité qu'une telle

surveillance est imposée aux opérateurs commerciaux… et accessoirement à leurs clients.

III. Des pirates désintéressés aux mafias du Net

Les premiers pirates technologiques qui, à partir des années 1980, affrontèrent les équipes de R&D des plus grands conglomérats industriels, comme l'américain at&t, cherchaient avant tout la performance, la satisfaction morale d'être parvenu, seul ou avec des moyens limités, à traverser les protections établies par des ingénieurs chevronnés – voire des militaires surentraînés à défendre la nation. Un sens du défi nourri par des ego souvent très développés et par cette particularité du monde numérique qui veut que l'expertise ne soit pas nécessairement liée à l'âge, à un diplôme ou à l'ampleur de l'expérience professionnelle.

Le Californien Kevin D. Mitnick, né en 1963, est considéré comme l'un des premiers pirates informatiques à avoir

déployé ses « talents » à grande échelle. Son activité favorite ? Entrer dans les systèmes informatiques d'institutions comme la compagnie de téléphone de Los Angeles Pacific Bell, les ordinateurs du Pentagone et de l'arpa, ou le service des cartes grises *(Department of Motor Vehicles)* de Sacramento. À chaque fois, il finit par se faire prendre et séjourne quelques mois en prison.

Les principaux chefs d'accusation concernent les intrusions et non un vol d'argent, sa démarche étant essentiellement fondée sur la prouesse technologique. Persistant à mener ses effractions numériques à travers les États-Unis, il est condamné, en 1995, à une peine de cinq ans de prison. Il détient même, un temps, le « privilège » d'être sur la liste des criminels les plus recherchés *(most wanted criminals)* établie par le fbi. Ces années de cavale, son désintéressement et son statut de pionnier du piratage ont conduit à le transformer en personnage mythique de la communauté d'Internet. Au point d'en faire aujourd'hui un auteur à succès [3] et un consultant recherché. Comme pour parfaire la légende, c'est grâce à la collaboration active d'un pirate repenti, Tsutomu Shimomura, que la police fédérale parvient à l'interpeller. Sorte de duel au sommet par écrans interposés.

Les années 2000 marquent la fin de ces as de l'informatique agissant pour la seule beauté du geste. Les pirates (ou *hackers*) visent désormais des buts militants ou des objectifs nettement mercantiles. Les réseaux numériques leur servent dès lors à conduire des opérations d'influence pour diffuser leurs idées et mener des campagnes de mobilisation de l'opinion publique, voire à capter les richesses d'autrui (argent, données…).

IV. – Vers une internationale de la cybercriminalité

La fluidité des systèmes d'information a aboli les frontières physiques et permet de mener des opérations criminelles sur le Net. Les fournisseurs de ces outils informatiques proposent leurs services sur l'ensemble du globe. Et se jouent de la territorialité des règles de droit. Par exemple, le 16 octobre 2008, le fbi[4] a procédé à la fermeture d'une plate-forme de recel de données informatiques volées. Baptisé « Dark Market », ce forum mettait à la disposition de ses 2 500 clients répartis sur

toute la planète des informations bancaires (numéros de cartes de crédit, codes d'accès à des comptes bancaires de particuliers…) captées frauduleusement *via* le Net. Cette place de marché à vocation mondiale misait sur la numérisation des échanges financiers qui permet à un délinquant de siphonner tranquillement et sans violence les liquidités placées dans une banque située à des milliers de kilomètres de chez lui.

Arrêté au cours de l'été 2009 aux États-Unis, Albert Gonzalez détient à ce jour le record de la fraude à la carte bancaire. Il est parvenu entre 2006 et 2008 à pénétrer les architectures informatiques de plusieurs systèmes de paiement en ligne et à détourner les coordonnées bancaires de leurs utilisateurs. Au total, il a ainsi piraté quelque 130 millions de comptes dont les références étaient commercialisées par la suite sur des serveurs informatiques installés aux États-Unis, en Lettonie, aux Pays-Bas et en Ukraine. Avec une poignée de complices, il avait réussi à industrialiser son commerce illicite et à en faire une activité réellement internationale.

Le monde devient donc une échelle naturelle pour appréhender la cybermenace. Ainsi, le 17 février 2010, la

société de sécurité informatique Netwitness a-t-elle annoncé qu'une campagne de piratage avait permis la prise de contrôle de 74 000 ordinateurs dans quelque 200 pays, notamment les États-Unis, le Mexique, l'Arabie Saoudite, l'Égypte et la Turquie. Avec des volumes si conséquents, on peut considérer que les assauts ne visent plus nécessairement telle ou telle catégorie d'organisation. Mais que toutes les entités connectées au réseau (particuliers, entreprises, institutions étatiques ou forces armées…) constituent potentiellement des cibles dignes d'intérêt. L'ampleur des moyens déployés démontre sans peine que tout ce qui est accessible en passant par les réseaux peut faire l'objet d'une intrusion, d'une captation et ultérieurement d'une utilisation malintentionnée. Un état de fait qui doit faire prendre conscience aux internautes, que ce soit durant leur temps libre ou à leur travail, qu'ils sont autant de cibles en puissance. Sans verser dans une paranoïa paralysante et finalement peu utile, il convient néanmoins de promouvoir une mise en garde et des réflexes de précaution qui permettent une circulation paisible sur la Toile.

Sur Internet, que l'on soit étudiant sans le sou ou cadre prospère, habitant en pleine ville ou dans la plus reculée

des campagnes, notre patrimoine informationnel est également exposé. C'est aussi le cas des entreprises, où les pme-pmi sont des victimes potentielles au même titre que les multinationales les plus renommées. L'éloignement géographique ou la langue ne sont pas sur la Toile des protections efficaces ni des immunités durables.

L'éditeur de solutions de sécurité Symantec publie un état des lieux des cyberattaques en fonction de leur origine géographique.

Tableau 2. – **Les activités malveillantes sur Internet**

Rang 2009	*Rang 2008*	*Pays d'origine*	*% du nombre total de cyberattaques*	
			2008	2009
1	1	États-Unis	23 %	19 %
2	2	Chine	9 %	8 %
3	5	Brésil	4 %	6 %
4	3	Allemagne	6 %	5 %
5	11	Inde	3 %	4 %
6	4	Royaume-	5 %	3 %

		Uni		
7	12	Russie	2 %	3 %
8	10	Pologne	3 %	3 %
9	7	Italie	3 %	3 %
10	6	Espagne	4 %	3 %

Source : *Symantec, Internet Security Threat,* avril 2010.

La France ne fait pas partie du peloton de tête des nations d'où émanent des attaques sur Internet, puisqu'elle occupe la 8e place en 2008, et la 13e en 2009. Au fur et à mesure que le « savoir-faire numérique criminel » se propage et que les équipements informatiques sont de plus en plus accessibles, les pays émergents s'en saisissent. La perspective de gains importants et le relatif sentiment d'impunité lié à la faiblesse de la coopération judiciaire internationale en la matière sont autant d'encouragements pour de futurs cyberdélinquants.

V. Quel droit international pour la cybersécurité ?

C’est au Conseil de l’Europe que l’on doit le principal texte de dimension réellement internationale en matière de criminalité numérique. En effet, la convention [5] de Budapest du 23 novembre 2001 sur la cybercriminalité a été signée par les 43 États membres de cette organisation. Toutefois, nombre d’entre eux comme l’Autriche, la Belgique, l’Espagne, la Grèce, l’Irlande, la Pologne, le Royaume-Uni, la Suède ou la Suisse ne l’ont toujours pas ratifié en 2010. Ce qui en relativise évidemment l’impact. Les rédacteurs de ce texte insistent notamment dans le préambule sur « le risque que les réseaux informatiques et l’information électronique soient utilisés pour commettre des infractions pénales et que les preuves de ces infractions soient stockées et transmises par le biais de ces réseaux ». Ainsi, le Conseil de l’Europe considère-t-il que la cybercriminalité constitue une menace pour la démocratie et les États de droit. La France et les États-Unis l’ont ratifié et intégré dans leur droit national dès 2006. Tandis que la Russie n’a toujours pas jugé utile d’y apposer sa signature.

Pourtant, dès 1982, l’Organisation pour la coopération et le développement économiques (ocde) avait pressenti la nécessité prochaine pour les États de prévoir dans leurs

corpus juridiques nationaux des incriminations relatives aux infractions commises en mettant à contribution l'informatique. Et dans les années qui suivirent, les juristes ont commencé à réfléchir aux conséquences des délits informatiques [6]. En septembre 1995, le Conseil de l'Europe a ainsi recommandé une harmonisation des dispositifs de collecte de preuves entre ses membres. En effet, le principe même d'un traitement judiciaire de telles attaques suppose que magistrats et services de police puissent s'appuyer sur des éléments indiscutables. Or, dans un monde numérique où les supports sont copiables et modifiables à l'envi, la question de l'intégrité des documents (textes, images, films ou sons) sort de la seule technique informatique pour devenir un enjeu du respect des règles démocratiques et judiciaires.

Le caractère éminemment international des communications électroniques amènera l'Europe à instaurer une coopération pénale contre la cybercriminalité. Notamment en permettant que, sur ces thèmes, les policiers des États membres puissent saisir directement Europol par le biais de commissions rogatoires pour des affaires se déroulant sur le territoire de l'Union. Ce qui reste plus rapide que le processus classique qui emprunte

les voies diplomatiques ou judiciaires.

Hors de cette « exception » européenne, la lutte contre la cybercriminalité pâtit encore trop souvent de la lenteur des procédures de coopération internationale. Là où quelques minutes suffisent à un internaute pour déplacer d'un continent à l'autre l'hébergement de son site crapuleux, il faut des semaines et une maîtrise fine des arcanes administratifs à un magistrat ou un policier désireux de solliciter ses homologues à l'étranger. Là encore, le temps judiciaire est loin de correspondre au temps technologique… On constate ainsi que des délinquants ont dès lors un intérêt manifeste à mener leurs escroqueries sur plusieurs pays, en prenant soin de voler peu d'argent, par exemple, à chacune de leurs victimes. Isolément, cela apparaîtra aux yeux du magistrat comme de petits préjudices et il est vraisemblable qu'il ne traitera pas en priorité ce dossier venant de l'étranger. Au total, en accumulant ainsi les petits détournements, le voleur disposera d'un vrai pactole tout en limitant le risque d'être poursuivi.

En février 2010, lors du Forum économique mondial de Davos, en Suisse, le secrétaire général de l'Union

internationale des télécommunications (uit), Hamadou Touré, a suggéré l'établissement d'un traité international sur la cybersécurité. Celui-ci reposerait sur trois principes. D'une part, les États devraient se doter des moyens de prémunir leurs concitoyens contre les cyberattaques. Ensuite, ils s'interdiraient d'abriter ou de protéger des cyberterroristes sur leur territoire. Enfin, ils renonceraient à lancer des attaques à destination d'un autre pays. Si on ne peut que partager *a priori* l'esprit généreux de cette proposition du responsable de l'agence des Nations unies en charge des télécommunications, ses aspects opérationnels semblent beaucoup plus aléatoires. D'autant qu'elle reprend pour l'essentiel les termes de la Déclaration faite le 10 décembre 1997 par les ministres de l'Intérieur et de la Justice des pays du G 8. Elle portait déjà en principe fondateur la règle selon laquelle « il n'y aurait aucun refuge pour ceux qui fraudent grâce aux technologies de l'information ». Presque quinze années se sont écoulées, et on constate aisément que ce discours solennel doit se heurter à la réalité du quotidien.

En effet, il n'existe pas de réel consensus international sur la cybersécurité et, *in fine,* nombre de gouvernements regardent avec intérêt ces technologies qui permettent de

porter des coups à leurs adversaires, sans que leur responsabilité juridique puisse être engagée avec certitude. Si on peut démontrer l'origine d'une attaque militaire classique, avec interventions de soldats et d'équipements lourds, il en va autrement de ces campagnes d'assauts informatiques qui paralysent les systèmes d'information d'un pays ou prennent la forme de mobilisation médiatique de grande ampleur sur les forums de discussion à travers le Web planétaire.

VI. Cyberguerre et cyberterrorisme

Internet employé comme une arme incarne parfaitement le principe des conflits dits « asymétriques ». Les parties prenantes n'y sont pas nécessairement de même nature juridique – il peut s'agir d'un État, d'une entreprise, d'un collectif de militants ou d'un individu isolé – ni de même taille. Ainsi une personne peut mener des cyberattaques à l'encontre de son ex-employeur ou d'une société dont elle désapprouve le comportement ou les produits. Tout comme un gouvernement est en mesure de conduire des

cyberagressions au détriment d'entreprises qui agissent à l'encontre de ses intérêts. Ainsi, le 12 janvier 2010, un communiqué officiel[7] intitulé « A new approach to China », émanant de Google, révélait que le célèbre moteur de recherche avait fait l'objet, le mois précédent, de tentatives massives de pénétration de ses infrastructures informatiques. Dans ce cas, une société commerciale désigne donc clairement le gouvernement d'un État souverain comme étant à l'origine des attaques dont elle a été la cible.

Dans un autre genre, les mouvements terroristes sont également devenus des utilisateurs naturels des techniques de cyberattaques. De la même manière que des activités criminelles « traditionnelles » comme le racket, le vol de voitures ou de stupéfiants peuvent servir au financement de groupuscules terroristes, ces derniers ont spontanément investi le champ de la fraude numérique. Elle permet de récolter des fonds pour mener leurs actions tout en ménageant les zones dans lesquelles ils ont trouvé refuge, puisque les victimes peuvent se trouver n'importe où sur le globe. Elle se pratique en toute discrétion, permettant de contourner services de police. Les sommes ainsi réunies peuvent être élevées et le cloisonnement des réseaux en est

facilité puisque chaque entité dispose à son échelle de son mode de financement.

Peu à peu, les États s'organisent et se dotent les uns après les autres de doctrine de cybersécurité et d'équipes *ad hoc* pour les traduire dans les faits. En 2008, le *Livre blanc sur la Défense et la Sécurité nationale* [8], qui pose les bases de la stratégie militaire française pour les quinze prochaines années, a établi un « palmarès » des risques et menaces visant le pays. Les attaques informatiques arrivent en deuxième place derrière les attentats terroristes. Aux États-Unis, en janvier 2009, le fbi a annoncé au Président Obama que le *Cybergeddon* ou *Armageddon cybernétique* constituait, après les armes de destruction massive et les offensives nucléaires, la plus grande menace pesant désormais sur l'Amérique et indiqué qu'un tel péril pouvait causer « le même type de dégâts que le 11 septembre 2001 ». Une analogie lourde de sens vue de Washington.

Les événements du printemps 2007 en Estonie semblent illustrer cette forme annoncée de cyberguerre en l'occurrence, lorsque les technologies de l'information et de la communication sont mises à contribution pour appuyer

un jeu diplomatique et géopolitique bien réel. Dans ce cas précis, les tensions locales entre la population et la forte communauté russophone du pays avaient culminé lorsque les pouvoirs publics ont pris la décision de transférer dans un cimetière militaire sis en périphérie de Tallinn un monument célébrant la « libération » du pays par l'Armée rouge.

Considéré comme un affront à la fierté russe – et perçu comme une prise de distance supplémentaire vis-à-vis de Moscou –, ce déplacement a suscité de violentes émeutes dans ce petit État où la minorité russe représente près d'un tiers de la population. Comme pour amplifier ces mouvements de rue, les principaux sites Internet gouvernementaux de cet État balte ont fait notamment l'objet, de fin avril à la mi-mai 2007, d'opérations de déni de service : ils devenaient inaccessibles sous le coup d'un trop grand nombre de connexions simultanées, ou de détournement. Par exemple, les pages d'accueil des sites ministériels estoniens se trouvaient ornées d'un portrait d'Adolf Hitler. Ces assauts cybernétiques ont créé d'autant plus de désordres dans l'opinion que l'Estonie a pris très tôt le virage du tout-numérique. Avec une dématérialisation des échanges financiers et une e-

administration que l'on peut comparer à ce qui existe en Corée du Sud.

Bis repetita ? Un an plus tard, les 19 et 20 juillet 2008, le site Internet de la présidence de la République de Géorgie est la cible d'attaques informatiques émanant d'un réseau de plusieurs centaines d'ordinateurs piratés à distance. On les désigne fort à propos sous le nom d'ordinateurs zombis. Coïncidence ou non, au même moment, Moscou et Tbilissi sont à couteaux tirés au sujet de l'Ossétie du Sud. Quelques jours plus tard, le 12 août 2008, la vague informatique prend de l'ampleur et vise désormais les sites des principaux médias, ministères et organismes publics géorgiens qui sont tous inaccessibles en raison de l'afflux concomitant des connexions. Là encore, des visuels truqués représentant les leaders géorgiens parés de l'uniforme nazi achèvent de démontrer la puissance technologique des assaillants.

Le message délivré était clair : nous pouvons entrer dans vos systèmes informatiques et les modifier à loisir. Quant à savoir à qui l'on pouvait imputer ces attaques, la prudence s'impose. Évidemment le pouvoir russe semblait le responsable tout désigné. Reste encore à le prouver. C'est

toute la spécificité de cette arme numérique : elle assène des coups sans que l'on puisse avec certitude en déterminer l'auteur. Une véritable aubaine pour mener des actions offensives…

Dans le cas géorgien, les piratages numériques ont tout de même obligé l'aviation militaire – une flotte de dix-huit appareils – à rester au sol. En effet, des raids informatiques ciblés ont opportunément infecté les réseaux locaux de commandement et de conduite des opérations aériennes. En d'autres temps, ces appareils auraient été abattus en vol. Aujourd'hui, on les empêche tout simplement de décoller. Les mêmes menaces guettent les infrastructures qui pilotent nos grands systèmes industriels : barrages hydroélectriques, centrales électriques ou nucléaires, stations de traitement des eaux, coordination des circulations aériennes ou ferroviaires… Autant de cibles possibles pour contribuer à la déstabilisation d'un pays, de son économie et de sa population. Les pirates à la manœuvre peuvent être aussi bien des États que des mouvements terroristes résolus à conduire des opérations meurtrières et médiatiques de grande ampleur.

En janvier 2010, le Centre pour la protection des

infrastructures nationales du mi 5 (le contre-espionnage britannique) a publié un rapport d'une quinzaine de pages qui recense les tentatives conduites par Pékin pour pénétrer les systèmes d'information des entreprises qui l'intéressent. Des cartes mémoires ou des appareils photos numériques sont ainsi offerts lors de salons professionnels à des collaborateurs de la firme que l'on souhaite infiltrer. Ces supports sont contaminés par un programme (on parle de cheval de Troie puisqu'il agit à l'insu de son destinataire) qui permettra le contrôle à distance ou la surveillance de l'ordinateur auquel le salarié insouciant l'aura branché.

Autrefois réservées aux aventures de James Bond ou aux meilleures pages de la littérature de science-fiction, ces pratiques sont désormais monnaie courante. De même, le vol d'équipements électroniques (ordinateurs portables, assistants personnels…) s'est généralisé. Outre les informations qu'ils contiennent, ces appareils permettent souvent d'accéder au réseau informatique de l'entreprise ou de l'organisation de leur légitime propriétaire. En 2008, par exemple, un conseiller du Premier ministre Gordon Brown s'est fait dérober son ordinateur de poche alors qu'il avait été invité à danser par une hôtesse dans une

discothèque de Shanghai. Rien n'empêche aujourd'hui une organisation terroriste d'utiliser ces mêmes techniques pour capter des données ou des richesses nécessaires au financement de sa cause.

Cette capacité à recueillir facilement des fonds de manière illicite contribue à lier de plus en plus les activités cybercriminelles et les mouvements terroristes.

Les supports choisis peuvent apparaître sous les visages les plus angéliques. Souvent, l'actualité permet aux pirates de renouveler leur inspiration. Ainsi après le tsunami qui a dévasté l'Asie en décembre 2004 ou à la suite du tremblement de terre qui a frappé Haïti en janvier 2010, des campagnes d'appel au don ont foisonné sur la Toile. Misant sur la compassion générale, des escrocs ont collecté des fonds au nom d'organismes humanitaires qu'ils avaient créés juste pour l'occasion. L'envoi de dizaines de milliers de courriers électroniques appelant à la générosité était rapidement amorti par les premiers donateurs généreux, mais naïfs.

Les entreprises ne sont pas en reste. Au cours du mois de février 2010, plus de 2 000 sociétés allemandes ont été sollicitées afin d'ouvrir un nouveau compte auprès de la

Deutsche Emissionshandelstelle (dehst), l'organisme fédéral chargé de la gestion et des échanges des quotas d'émissions de co^2. Le message désignait en réalité un site pirate. Chaque fois qu'une firme lui fournissait ses coordonnées d'identification auprès de la dehst, les quotas de co^2 ainsi détournés étaient immédiatement revendus. Dans la presse allemande[9], les autorités parlent d'au moins 3 millions d'euros de préjudice pour une dizaine d'entreprises victimes.

Les cyberattaques peuvent enfin être exploitées par des mouvements terroristes en complément d'attentats réels pour les amplifier. Par exemple, l'explosion d'une bombe dans un métro en plein centre-ville peut être suivie d'une pénétration ciblée des réseaux informatiques des services de police de la municipalité. Notamment pour prendre le contrôle ou neutraliser le système de gestion des feux de signalisation. En créant des embouteillages monstres alors que les ambulances ont au contraire besoin de circuler au plus vite pour acheminer les blessés vers les hôpitaux, les terroristes peuvent amplifier le bilan de leur attentat. Et susciter par voie de conséquence un traumatisme majeur au sein de l'opinion publique, qui prend ainsi conscience de l'incapacité de ses autorités à assurer la sécurité de la

collectivité. Avec un impact certain auprès de ceux qui se trouvent à l'autre bout du pays et réalisent que leur État est démuni face à des agressions de cette nature. En plus, la pagaille routière ainsi créée constitue autant d'images chocs pour les chaînes de radio et de télévision d'information continue. Qui sont toujours désireuses d'illustrer leurs programmes spéciaux avec des situations que l'on peut montrer à l'écran.

Car si la cyberguerre est le fruit de solutions technologiques de pointe, elle se nourrit néanmoins d'émotions fortes. Avec des vidéos et des témoignages qui circulent, société de l'information oblige, à la vitesse de la lumière. Et façonnent tout aussi vite le débat public.

Notes

[1] Norbert Wiener , *Cybernetics*, Paris, Hermann, 1948.
[2] Remarks by the President on securing our nation's cyberinfrastructure, 29 mai 2009, www.whitehouse.gov
[3] Kevin D. Mitnick et William L. Simon , *The Art of Deception*, Indianapolis, Wiley, 2002, *The Art of Intrusion*,

Indianapolis, Wiley, 2005.
[4] Description de l'opération sur le site Internet du fbi : http://www.fbi.gov/pressrel/pressrel08/darkmarket101608.
[5] Son texte intégral et le suivi de sa ratification par les États signataires sont disponibles sur le site du Conseil : http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm
[6] *La Fraude liée à l'informatique : analyse des politiques juridiques*, Paris, ocde, 1986.
[7] Disponible sur le site institutionnel de Google : http://googleblog.blogspot.com/2010/01/new-approach-to-china.html
[8] *Livre Blanc sur la Défense et la Sécurité nationale*, Paris, Éditions Odile Jacob-La Documentation française, 2008.
[9] Michael Kröger et Frank Patalong, « Millionenschaden durch phishing », *Der Spiegel,* 3 février 2010.

Chapitre II

Les attaques sur les réseaux informatiques et téléphoniques

I. L'espionnage et les interceptions

« Alerte sur la sécurité d'Internet ! » Une fois n'est pas coutume, ce titre a fait la une des médias du monde entier lorsque la nouvelle fut connue le 28 juillet 2008. De quoi s'agissait-il ? De la révélation faite par un jeune informaticien de talent, Dan Kaminsky, d'une faille majeure dans l'architecture du réseau Internet. Sept mois auparavant, ce spécialiste en sécurité numérique a identifié

une brèche qui aurait permis à des pirates de leurrer les machines qui connectent chaque internaute au nom de domaine qu'il inscrit sur son navigateur Web. En utilisant cette fonctionnalité, un *hacker* aurait été en mesure de vous faire croire que vous vous étiez bel et bien connecté au site de votre banque. Le temps de récupérer vos codes d'accès et le voilà à même, sans effraction, de disposer de vos comptes bancaires. Et cela pouvait fonctionner avec tous les autres sites auxquels on confie des données en principe confidentielles. Le point faible ? Le dispositif d'adressage qui faisait coïncider l'adresse numérique des sites et leur intitulé utilisé par tout un chacun. Conscient de l'ampleur du péril qui guettait la planète informatique, Dan Kaminsky a veillé dans un premier temps à conserver la confidentialité de sa découverte. Le temps que les opérateurs Internet, dûment avertis, pallient la situation. Ce qui explique que l'information n'ait été finalement divulguée que sept mois plus tard, au cours de l'été 2008. Cette catastrophe évitée a suscité la coalition des cinq plus grands industriels du secteur informatique et des réseaux : Cisco Systems, ibm, Intel, Juniper Networks et Microsoft. Ils ont en effet créé, cette même année, l'Industry Consortium for Advancement of Security on the Internet [1] (icasi), une association à but non lucratif

destinée à traiter les menaces de sécurité pouvant affecter les processeurs, les cartes mères, les systèmes d'exploitation, les logiciels ou le réseau. L'idée étant que ces sociétés, qui, à l'occasion, peuvent être concurrentes, se mettent à collaborer afin de participer à la correction des défaillances techniques de l'internet. À nouveau, on assiste à une riposte concertée d'acteurs privés à des fins de sécurité, sans que, par ailleurs, les services gouvernementaux concernés, malgré l'importance des conséquences possibles, y soient directement associés. Il n'y a guère de situations équivalentes dans d'autres domaines d'activité.

Dans une économie de la connaissance, l'information constitue un actif très convoité. Le cabinet d'audit kpmg International estime [2] qu'au cours du premier semestre 2009, 110 millions de personnes dans le monde ont été directement ou indirectement affectées par de telles « pertes » de données. Dans 10 % des cas, ces vols ont été commis par des collaborateurs de la société, le plus souvent à l'occasion de leur transfert chez un concurrent ou lors de la création de leur propre structure. Tous les moyens sont employés : envoi par messagerie électronique, copie des documents imprimés, cd, dvd, clés

usb, disques durs externes…

En juillet 2009, le fbi a arrêté Sergey Aleynikov pour avoir volé les codes sources des logiciels utilisés par la banque Goldman Sachs pour traiter en temps réel les échanges entre institutions financières. Ce programmeur avait quitté son poste au sein de la compagnie états-unienne quelques semaines auparavant. Doté de cette plate- forme informatique, un utilisateur malveillant aurait été en mesure de manipuler frauduleusement les marchés financiers, et générer ainsi des gains substantiels.

Moins technique mais tout aussi lucratif, l'envoi de messages imitant une enseigne réputée ou une administration officielle permet aux pirates de récupérer des données personnelles sans violence ni intrusion informatique. On désigne ce procédé sous le terme de *phishing,* ou hameçonnage.

Par exemple, pendant l'automne 2009, des milliers d'internautes français ont reçu dans leur courrier électronique une demande aux couleurs de la Caisse d'allocations familiales (caf) leur annonçant leur droit à toucher une prime de 325 euros. Pour obtenir la somme, il suffisait de cliquer sur un lien placé dans le texte. Arrivé

sur le site de l'escroc, on vous demandait vos coordonnées bancaires complètes afin d'effectuer au plus vite le virement. Évidemment, le naïf qui transmettait ces informations avait surtout toutes les chances de se voir délesté de quelques milliers d'euros dans les heures suivantes. Dans ce cas, le site était hébergé en Hongrie. Mais à peine fermé, une fois repéré, il est réapparu à partir d'autres pays d'Europe centrale.

Des versions similaires de telles escroqueries existent également sous les couleurs de la Direction générale des impôts qui se propose de vous rembourser un trop-perçu fiscal.

Le but étant toujours de récupérer un maximum des données personnelles de l'internaute, les pirates collent au plus près de l'actualité. Afin de répondre à la curiosité du plus grand nombre et donc assurer le meilleur taux de transformation : entre le nombre de pourriels (spams ou courriers indésirables) envoyés et l'activation par le destinataire du lien qu'il contient. Dans les heures qui ont suivi l'annonce du décès du *King of pop* en juin 2009, des pourriels intitulés « Who killed Michael Jackson? » (qui a tué Michael Jackson ?) circulaient en grand nombre sur le

Net. Un autre assurait disposer des images montrant que l'on venait de tirer sur le Président Obama élu en novembre 2008.

L'éditeur Symantec, spécialisé en sécurité informatique, estime à 60 000 le nombre de sites de *phishing* dans le monde en 2010. Un chiffre en progression de 7 % par rapport à l'année précédente.

L'attaque dite « à la nigériane » reste un grand classique. Une jeune Africaine – veuve ou orpheline selon les cas – vous appelle à l'aide dans un message de détresse. Il se trouve que son père ou défunt mari était ministre ou gouverneur de la banque centrale de son pays. Et qu'elle vous a opportunément choisi pour l'aider à faire sortir du pays – en échange d'un pourcentage – les millions de dollars de son héritage. Naturellement, il vous revient d'abord de payer des frais administratifs divers en attendant de recevoir votre pactole. Celui-ci ne parviendra pas et l'argent envoyé ne sera jamais remboursé.

L'ensemble de ces spams représente désormais la très grande majorité des courriers électroniques qui circulent quotidiennement sur la Toile. Les éditeurs de solutions de sécurité estiment même qu'il avoisine les 90 % de la

correspondance numérique planétaire. Cette abondance s'explique par le fait que de tels envois en grand nombre deviennent rentables pour leurs auteurs dès lors que 0,1 % des destinataires répondent. Ils misent donc sur l'effet de levier que permet la modicité des prix pour élaborer et diffuser en ligne ces arnaques financières et autres moyens de collecter des données monnayables par ailleurs.

À titre indicatif, en 2010, il fallait débourser à peine 800 dollars pour pouvoir disposer des services d'un parc de 10 000 ordinateurs infectés. Qualifiées de zombies, ces machines se trouvent aussi bien chez des particuliers que dans des entreprises. Elles ont été contaminées préalablement par un virus à l'insu de leur légitime propriétaire. Sans que celui-ci en soit informé, et *a fortiori* ait donné son accord, leur puissance de calcul et leur connexion à Internet peuvent être mises à contribution à distance par le pirate. Par exemple, afin de participer à une campagne d'assaut numérique de grande ampleur pour rendre inaccessible un site Internet déterminé. Si une enquête est menée, elle désignera alors l'ordinateur d'un individu ou d'une institution qui ignorera tout de l'attaque en question.

Cet espionnage numérique peut également revêtir des formes inattendues. Ainsi, le 17 décembre 2009, le *Wall Street Journal* [3] expliquait par le menu comment des insurgés irakiens étaient parvenus à pirater les flux d'images prises par les drones *Predator* et transmis aux opérateurs installés aux États-Unis. Avec un logiciel disponible dans le public pour une trentaine de dollars, les rebelles disposaient en temps réel des mêmes images que l'opérateur chargé de les surveiller ou de procéder à des tirs à distance. Un atout décisif pour connaître les zones observées par l'ennemi et échapper ainsi à ses assauts. Comment était-ce possible ? L'us Army n'avait pas songé à crypter les messages émis par ses drones. Washington a officiellement suspecté Téhéran d'avoir transmis la marche à suivre aux combattants irakiens. En retour, le gouvernement iranien a aussitôt nié toute responsabilité dans cette affaire.

En octobre 2009, la lettre d'information spécialisée *Intelligence on Line* [4] raconte comment les pirates somaliens détournent les systèmes de localisation utilisés par les armateurs pour surveiller le bon cheminement de leurs navires. Là encore, le cryptage est quasi inexistant. Or le dispositif permet à tous ses utilisateurs de suivre en

temps réel le parcours de ces bateaux sur le Net. Afin de limiter les risques, le commandement européen chargé de la sécurisation de la zone (eu Navfor Somalia) recommande donc aux équipages de désactiver leurs équipements de suivi le temps du passage du périmètre à risques. Une réponse basique à cette flibuste high-tech.

Autre illustration de ces piratages à grande échelle un peu plus tôt dans l'année : le 21 avril 2009, le porte-parole du ministère de la Défense des États-Unis confirme l'infiltration par des pirates informatiques des programmes de construction du chasseur le plus sophistiqué du monde, le futur F-35 Lightning II. Le matin même, le *Wall Street Journal* [5] avait révélé que des espions s'étaient emparés de données concernant sa conception et ses systèmes électroniques. Et cela « de manière répétée depuis au moins 2007 ». Une performance au goût plutôt saumâtre pour l'état-major, où l'on sait pertinemment que ledit programme est doté d'un budget de 230 milliards d'euros. Dans la foulée, Robert Gates, le secrétaire d'État à la Défense, annonçait lui-même le renforcement des équipes de cybersécurité de son ministère, passant de 80 à 250 personnes.

Mais aucun secteur n'est épargné. En mars 2007, le spécialiste mondial de la gestion de bases de données, Oracle, traîne son concurrent sap en justice, au motif qu'il aurait pillé son centre de support clients afin de télécharger des milliers de copies de son code logiciel propriétaire. En France, l'état-major d'edf a été perquisitionné en février 2009 dans le cadre d'une plainte déposée par l'association de défense de l'environnement Greenpeace qui s'inquiétait d'opérations de piratage de son réseau informatique.

Nous avons parlé à chaque fois d'attaques menées à l'encontre de réseaux informatiques. L'offre, en la matière, évolue naturellement avec les usages du marché et les technologies disponibles. Ainsi, le succès commercial des assistants personnels, avec les formules d'abonnement à l'Internet mobile, a déplacé – et étendu – le champ d'action potentiel des pirates. Ces appareils qui tiennent dans la poche sont désormais les dépositaires de nombre de nos informations confidentielles (contacts, codes d'accès à nos comptes bancaires, photographies de nos proches, historiques de nos sms…).

En 2010, on estime à 525 millions le nombre de ces smartphones commercialisés dans le monde. À tel point

que les éditeurs de logiciels incluent désormais le téléphone dans la gamme des outils numériques devant disposer d'un antivirus. Avec des options supplémentaires qui donnent une idée de l'importance prise par ces boîtiers high-tech dans nos vies modernes : en cas de perte ou de vol, blocage à distance de l'appareil ou destruction des données qu'il contient par l'envoi d'un sms, identification automatique du numéro de la personne qui souhaiterait changer la carte sim à votre insu, localisation à tout instant du combiné…

Autre piste d'insécurité numérique : la sous-traitance. Notamment avec une formule de prime abord séduisante pour la comptabilité des entreprises : le *cloud computing,* ou informatique des nuages. Derrière cet intitulé poétique se dessine une offre d'externalisation du traitement des données. La société utilisatrice n'acquiert plus des serveurs informatiques mais loue des puissances de calcul à des prestataires qui hébergent et gèrent les informations qu'elle leur a confiées. L'idée est simple : plutôt que d'investir dans des infrastructures informatiques dont vous n'êtes pas sûr d'avoir l'usage, ou qui risquent de se révéler rapidement insuffisantes, préférez la solution de la location à la demande. Les informations ne sont plus stockées chez vous mais dans des équipements proportionnés pour les

traiter et les exploiter dans les meilleures conditions.

L'attrait financier vient du fait que seul l'usage réel est finalement facturé. Si cela peut éventuellement constituer une bonne affaire, il en va tout autrement de la confidentialité des données ainsi transférées. Puisqu'à chaque fois que vous les utilisez, l'informatique interne va aller les chercher dans ces serveurs situés hors de la sphère de l'entreprise. Guidées par la volonté de réduire les coûts, les sociétés optent de plus en plus pour ce type d'organisation.

Selon le cabinet Markess International, le marché français du *cloud computing* s'élevait à 1,5 milliard d'euros en 2009, pour atteindre 1,85 milliard d'euros en 2010, et 2,29 milliards d'euros en 2011. Soit un taux de croissance annuel moyen de 23,6 %. La tendance est la même à l'échelle de la planète. Un tel transfert exige la mise en place d'une politique de sécurité informatique très rigoureuse. Et un suivi étroit du fournisseur retenu. On assiste à ce propos à la constitution rampante, à l'échelle des grands pays, de groupes industriels spécialisés dans cette activité. Souvent encouragée par les pouvoirs publics, cette dynamique a vocation à faire émerger des acteurs nationaux du *cloud*

computing fiables, afin d'encadrer au plus près cette externalisation massive d'informations possiblement stratégiques.

En France, l'engagement étatique en la matière se traduit par la mise à disposition de fonds publics. En effet, sur les 2,5 milliards d'euros du grand emprunt annoncé par le président Nicolas Sarkozy qui iront aux services numériques, environ 700 millions devraient être alloués à cette informatique *distribuée,* la participation de ces équipements informatiques à la souveraineté et à la sécurité nationales ne faisant plus aucun doute. Reste néanmoins à ce que les projets proposés au financement tiennent la route. En matière de calendrier, les premiers versements devraient intervenir fin 2011, puis au cours de l'année 2012.

II. L'altération de données

Le pirate qui s'introduit dans les systèmes d'information de sa cible peut souhaiter modifier les informations détenues par celle-ci. Les motifs qui justifient une telle démarche sont multiples.

En juin 2009, Jesse McGraw a été arrêté au Texas par le fbi pour avoir contaminé les ordinateurs d'une clinique de Dallas avec un logiciel qui lui permettait à distance de réécrire les dossiers personnels des patients ainsi que leurs examens médicaux. À la tête d'un groupe de *hackers* baptisé l'*Electronik Tribulation Army,* il était également parvenu à prendre le contrôle des systèmes de climatisation des blocs opératoires. De quoi générer des infections en cas de variations de température durant une intervention chirurgicale. Le jeune homme avait prévu de déclencher son attaque le jour de la Fête nationale, le 4 juillet. Mais sa vanité l'a perdu : quelques jours avant d'ouvrir les hostilités numériques à l'encontre de l'hôpital, il a posté sur le site de partage de vidéos YouTube le film de sa prouesse technique. Cette poussée d'orgueil aura au moins permis son arrestation avant qu'il ne passe effectivement à l'acte.

Toujours dans l'univers médical, un magistrat du tribunal de grande instance de Nanterre (Hauts-de-Seine) a lancé, fin janvier 2010, un mandat d'arrêt national à l'encontre de l'éphémère vainqueur du Tour de France 2006, Floyd Landis. Reconnu coupable de dopage à la testostérone, il est suspecté d'avoir mené des intrusions informatiques

dans les ordinateurs de l'Agence française de lutte contre le dopage (afld) installés à Châtenay-Malabry, près de Paris, afin de corriger à son avantage les résultats obtenus lors de ses tests de dépistage. Vraisemblablement pour se disculper et ensuite mettre en cause la responsabilité de l'afld. Les investigations des enquêteurs avaient permis de remonter jusqu'à l'adresse Internet de son médecin et entraîneur.

De telles attaques ne sont pas l'apanage des adultes et des cabinets d'investigation. En effet, le 5 octobre 2009, un collégien d'Arras (Pas-de-Calais) a été placé en garde à vue. Il est soupçonné, en effet, d'avoir piloté une intrusion informatique dans le système de son école. L'adolescent de quinze ans voulait tout simplement retoucher à distance son bulletin scolaire en intervenant sur les fichiers numériques de l'administration. N'étant pas parvenu à ses fins, il a paralysé le serveur de l'école en procédant à l'envoi simultané de 40 000 courriels à partir des ordinateurs de l'établissement. Bilan : quatre jours d'interruption de l'informatique de ce collège Saint-Joseph. Au-delà du récit qui peut prêter à sourire, cet épisode témoigne de la grande démocratisation des techniques de piratage et de *spamming*. Et de la banalisation annoncée du

recours à ces pratiques pour régler un différend ou tenter de changer en sa faveur le cours de certains événements.

Des opérations classiques de chantage sont également en train de se développer. Le pirate contamine le réseau de sa cible, généralement une entreprise, et l'avertit de son forfait. Les termes du « marché » sont clairs : soit la société visée paie une rançon, soit ses données seront instantanément détruites ou rendues inaccessibles par un codage particulièrement robuste. Si le dirigeant de l'entité concernée n'est pas certain de son niveau de protection numérique, il ne prendra généralement pas le risque. Et préférera verser la somme demandée.

L'ingéniosité des *pirates rançonneurs* est alors de fixer un montant suffisamment élevé pour être crédible. Mais pas trop cependant pour permettre de sortir discrètement l'argent de la comptabilité maison. À titre indicatif, à la mi-2008, une filiale de l'allemand basf a déboursé 80 000 dollars pour recouvrer des données préalablement chiffrées par un interlocuteur malveillant. Renouvelé régulièrement auprès de différentes sociétés, le procédé peut se révéler éminemment lucratif. Et finalement peu risqué au plan judiciaire tant que les victimes préfèrent rester discrètes

quant à la piètre qualité de leur sécurité informatique.

III. La prise de contrôle totale à distance

C'est sans doute l'idée que chacun se fait de la cyberattaque : la capacité à prendre les commandes des systèmes d'information de sa cible comme si on en était le légitime propriétaire. Dès lors que l'intrusion est possible, une telle mainmise ne relève évidemment plus de la science-fiction. Mais un tel scénario concerne avant tout les infrastructures les plus stratégiques. Pour les autres, le vol ponctuel d'argent ou de données représente la principale menace.

L'ampleur du péril numérique est ici à la hauteur de l'informatisation des processus de production industrielle. Dès lors qu'une action est pilotée par un ordinateur, cet échange peut être détourné de son but initial. Or, la quête constante menée par les entreprises, ces dernières années, d'une réduction systématique des coûts de fabrication a conduit à la suppression progressive de l'intervention humaine dans le contrôle et le suivi des opérations

techniques.

Les sociétés chargées de la gestion des équipements d'importance vitale (tels les réseaux de transport, d'électricité ou d'eau…) ont très fréquemment recours à des solutions informatiques achetées sur étagère dans le commerce pour surveiller et intervenir à partir d'un poste de commandement central sur des zones entières de notre territoire. Les professionnels emploient pour les désigner l'acronyme anglophone scada : *Supervisory, Control and Data Acquisition.* Ces dispositifs permettent aux gestionnaires des sites (centre de traitement des eaux, pompes, flux de transport, production et distribution électriques…) de surveiller à distance ces activités.

Le magazine américain *Forbes* [6] a recensé quelques-unes des cyberattaques menées récemment contre les systèmes scada. Un *hacker* explique dans quelles conditions il est parvenu – sans jamais mettre les pieds dans le site en question – à prendre le contrôle d'une centrale nucléaire aux États-Unis. L'impact mortel potentiel de ces actions et le caractère hautement symbolique de ces cibles en font des objectifs éminemment stratégiques. De quoi susciter l'appétit d'un pirate réellement malintentionné ou

simplement tenté par le défi personnel que représente la préservation de ces lieux sensibles.

À ce jeu, les *hackers* disposent souvent d'un avantage de taille : les dispositifs de suivi du bon fonctionnement de ces équipements industriels communiquent, dans la très grande majorité des cas, entre les différents sites *via* le réseau Internet classique. Et non par un réseau sécurisé dédié (recherche d'économies oblige). Des circonstances qui les rendent d'autant plus vulnérables face à des pirates informatiques.

Tableau 3. – **Solutions de sécurité déployées dans les entreprises françaises (novembre 2009)** [7]

Antivirus	97 %
Gestion des identités et des accès	84 %
Détection/Prévention d'intrusion	70 %
Accès distants sécurisés (vpn)	67 %

Contrôle d'accès physique	60 %
Outils de sécurité des réseaux sans fil	52 %
Chiffrement	32 %
Authentification forte (biométrie ou carte à puce par exemple)	19 %
Sans opinion	1 %

Source : tns-Sofres-Logica, *L'Insécurité numérique des entreprises,* novembre 2009.

Le péril vient donc non seulement des dégâts causés par une cyberattaque, mais également des conséquences qui peuvent en découler en cascade. Globalement, on est en mesure de répartir en cinq catégories les effets de ces assauts numériques :

- les conséquences physiques pour la population (avec la paralysie des services médicaux et de secours, des transports air, fer et mer, les risques accrus d'accidents de la route faute de

signalisations en état de marche…) Sans parler d'éventuels traumatismes psychologiques pour les habitants ainsi jetés dans la crise ;

- les conséquences pour l'environnement (interruption de l'alimentation en eau, en électricité…, dysfonctionnement des égouts, effets sur la maintenance des sites nucléaires et chimiques) ;

- les conséquences économiques : les pertes industrielles, financières et sociales liées aux dérangements informatiques ;

- les conséquences politiques, qui peuvent susciter tensions, désordres publics, voire émeutes ;

- les conséquences liées au cumul et à la combinaison des circonstances ci-dessus.

Dans l'analyse de leur vision du monde en 2025 [8], le National Intelligence Council et le Director of National Intelligence des États-Unis citent parmi les premières menaces pour la sécurité les agressions menées à l'encontre de leurs systèmes d'information stratégiques. Et insistent

sur les risques de sabotages électroniques qui pourraient affecter leurs installations critiques. Ce qui constituerait également un moyen performant de fragiliser les troupes américaines présentes sur les champs de bataille à l'étranger. Autrement dit, des cyberattaques ayant un impact matériel direct sur le sol d'une nation peuvent fragiliser la puissance de celle-ci hors de ses frontières.

À l'intérieur même d'un pays, on peut se demander combien de temps la population d'un État démocratique serait prête à vivre sans eau, électricité ou moyens modernes de communication. De telles privations, si elles devaient durer dans le temps, constitueraient à n'en point douter un élément de déstabilisation d'un gouvernement et d'une économie. Le tout sans avoir à conduire la moindre opération militaire, ni sans voir sa responsabilité juridique – si, par exemple, un gouvernement étranger était à la manœuvre – engagée dans de tels dysfonctionnements. Se découvre ainsi une autre manière de conduire des conquêtes qui remet partiellement en cause l'analyse de Carl von Clausewitz selon laquelle la guerre revenait à contraindre son ennemi par la force.

Notes

[1] www.icasi.org

[2] kpmg International, Data Loss Barometer, décembre 2009.

[3] Siobhan Gorman, Yochi J. Dreazen et August Cole, « Insurgent hack us drones », *The Wall Street Journal,* 17 décembre 2009.

[4] *Intelligence on Line* n° 603, 15-28 octobre 2009.

[5] Siobhan Gorman, Yochi J. Dreazen et August Cole, « Computer spies breach Fighter-Jet Project », *The Wall Street Journal,* 21 avril 2009.

[6] Andy Greenberg, « America's Hackable Backbone », *Forbes,* 22 août 2007.

[7] Le total des pourcentages est supérieur à 100, les personnes interrogées ayant pu donner plusieurs réponses.

[8] *Global Trends 2025: a Transformed World,* novembre 2008, www.dni.gov/nic/nic_2025_project.html

Chapitre III

Les attaques informationnelles

I. Attenter à l'e-réputation

La renommée est assurément un patrimoine stratégique pour une entreprise. Le crédit que l'on porte à sa marque et à sa signature lui permet d'attirer des candidats de valeur, d'aborder plus facilement ses prospects et de fidéliser ses clients. Il en va de même pour les investisseurs, qui, outre les résultats financiers, peuvent rechercher cette forme de valorisation sociale. Les sociétés traduisent même sous une forme comptable la valeur de leurs marques comme un étant un actif à part entière. Selon les classements annuels établis par des cabinets de référence comme Interbrand ou Millardbrown, l'estimation

des plus grands noms d'entreprise se chiffre en dizaines de millions de dollars. C'est le cas pour des sociétés comme Google, Intel, Coca-Cola, Disney, McDonald's, General Electric ou Louis Vuitton. Dans ce contexte, les atteintes à la réputation – qu'elles soient fondées ou non sur le fond – peuvent causer des dégâts financiers considérables. Au point de forcer la structure à changer de nom. Ainsi, pour rompre avec une période de turbulences judiciaires associées à sa raison sociale, le Crédit Lyonnais laissa la place au plus discret lcl.

Dans ce domaine encore, Internet « démocratise » la menace. Ces mises en cause informationnelles ne sont désormais plus l'apanage des firmes emblématiques. Et des pme, voire des individus, peuvent ainsi faire l'objet de campagnes de dénigrement, au risque de voir leur patronyme durablement entaché. En avril 2009, la chaîne de vente de pizzas, Domino's Pizza, a vu circuler sur certains sites de partage de vidéos en ligne comme YouTube un clip filmé par deux de ses salariés de Caroline du Nord. On les voyait maculer consciencieusement les plats qu'ils s'apprêtaient à livrer à leurs clients. En quelques jours à peine, un demi-million d'internautes l'avaient visionné et relayé sur les réseaux sociaux.

À cause de pannes à répétition sur son réseau, en décembre 2009, la compagnie ferroviaire Eurostar a dû faire face jusqu'à la fin de cette même année à des vagues de mise en cause sur les forums de discussion et le site de microblogging Twitter [1]. En effet, les clients mécontents adressaient leur message en direct des quais de gare ou à partir des wagons immobilisés pour dénoncer la mauvaise gestion de ces incidents. La Société Générale a connu pareille mésaventure quand les frasques de son trader Jérôme Kerviel lui ont fait perdre quelque 5 milliards d'euros. Réalisées par des internautes, les parodies moqueuses soulignant l'incompétence des dirigeants de la banque ont fait partie des films les plus demandés sur YouTube.

Pour tenter de reconquérir leur crédibilité, et d'endiguer le flot de cette communication hostile et non maîtrisée, les sociétés ont peu à peu appris à s'organiser. Ainsi, la sncf dispose de sa propre enceinte numérique d'échanges avec les internautes : « Opinions &Débats ». L'inscription est libre mais permet à la compagnie nationale de jouer sur son terrain. Elle compte en 2010 environ 20 000 membres.

Tenter d'égratigner la réputation d'une entreprise n'est pas

seulement le fait de clients insatisfaits. Cela peut faire partie d'une stratégie délibérée. Notamment dans le domaine financier quand la rapidité des transactions limite la capacité des investisseurs institutionnels ou personnes privées à recouper rapidement l'information qui circule. Selon une enquête[2] publiée en mars 2009 par la Rice University de Houston (Texas), les firmes états-uniennes sont de plus en plus nombreuses à être victimes de manipulations de cours par la diffusion de fausses nouvelles. Les cibles sont généralement des entreprises de taille moyenne, qui font l'objet de faibles volumes de transactions, qui se montrent plutôt discrètes en matière de communication, et qui ne sont pas cotés sur les grands marchés organisés comme le Nasdaq ou le New York Stock Exchange (nyse). Même si les effets de ces informations mensongères ne sont pas durables sur les marchés, ils laissent suffisamment de temps à celui qui se trouve en embuscade pour procéder à des ventes ou des achats de titres dans des conditions optimales.

Preuve supplémentaire du rôle d'Internet comme source d'informations pour les investisseurs, les travaux[3] de l'Université de Notre Dame publiés en mars 2009 démontrent la corrélation existant entre les recherches

qu'effectuent les internautes sur Google à propos de sociétés commerciales et les performances boursières à court terme de celles-ci. Notamment, au moment de leur introduction en Bourse. Pour résumer : plus une valeur fera l'objet de recherches sur Internet, plus le niveau de son cours aura tendance à grimper à brève échéance. Un phénomène passager mais qui affecte bel et bien les petites ou moyennes sociétés, notamment. Selon ces universitaires, les actions qui suscitent le plus grand nombre de recherches enregistrent des gains supérieurs de 5,7 % par an par rapport aux titres qui connaissent une chute des requêtes les concernant.

Pour tenter de maîtriser l'information à leur sujet, les entreprises se sont donc mises peu à peu à investir le champ des réseaux sociaux. Contrairement à la communication par l'intermédiaire des médias traditionnels où elles sont dépendantes de l'intérêt rencontré par les rédactions, qui en outre peuvent relativiser leur prise de parole, ces nouveaux supports sont à leur entière disposition.

Ainsi, selon le cabinet de conseil en communication Burston-Marsteller, en janvier 2010, la majorité des cent

premières firmes mondiales (le *Fortune 100*) étaient inscrites auprès de ces médias sociaux.

L'attaque informationnelle peut se combiner avec des infractions classiques telles que l'extorsion ou le chantage. Au printemps 2010, un logiciel malveillant nommé Kenzero contaminait les amateurs de *hentai,* ces dessins animés pornographiques. Ces internautes les téléchargeaient notamment *via* des plates-formes illégales de partage de fichiers. Le pirate rançonnait alors lesdits internautes en les menaçant de rendre publics sur la Toile leur identité et leur historique de navigation. En avril 2010, près de 6 000 Japonais ont ainsi reconnu que leur ordinateur avait été infecté de cette manière.

Tableau 4. – **Présence des principaux groupes multinationaux sur les réseaux sociaux**

	% des sociétés du Fortune 100	*Volume de leur production moyenne sur ces médias*
Disposant d'un compte Twitter	65	27 messages/semaine

Disposant d'une page Facebook	54	3,6 messages/semaine
Disposant d'une chaîne sur YouTube	50	10 vidéos/mois
Disposant d'un blog d'entreprise	33	7 messages/mois

Source : Burston-Marsteller, novembre 2009-janvier 2010.

Fin novembre 2009, la justice des États-Unis a condamné Alan M. Ralsky à cinquante et un mois de prison ferme pour avoir expédié avec ses complices 4 millions de pourriels. Il avait rédigé des courriers contenant de fausses informations relatives à des entreprises cotées, mais faisant l'objet de peu d'échanges sur les marchés boursiers. La lecture de son courrier électronique devait inciter les internautes candides à acheter des titres des compagnies en question, histoire de faire monter leurs cours et de permettre ainsi à ce sexagénaire de Detroit de réaliser une plus-value. Le texte de la condamnation évoque des opérations portant sur plusieurs millions de dollars entre les mois de janvier 2004 et septembre 2005.

Plus simple encore : l'usurpation d'identité est facilitée sur la Toile. On peut ainsi aisément s'inscrire sur les forums, réseaux sociaux et autres sites d'anciens élèves sous une fausse identité, qu'elle corresponde ou nom à quelqu'un de réel. À titre symbolique, on peut citer le cas de cet ingénieur marocain de vingt-huit ans qui, en 2008, a ouvert un compte Facebook en se faisant passer pour le frère du roi Mohammed VI. La Federal Trade Commission (ftc [4]) – l'organisme fédéral des États-Unis chargé de la protection des consommateurs – comptabilise à des centaines de milliers les infractions commises chaque année sur le Net grâce à de telles fraudes à l'identité.

II. Stratégies d'influence à l'ère du Net

Si la Toile est une vitrine où chacun peut vanter ses mérites ou présenter ses opinions, c'est également une caisse de résonance fort utile pour mener des opérations d'influence. Qu'il s'agisse d'atteindre des prospects, des décideurs politiques ou des clients. Partant du principe que le Net constitue la première source d'information de nos

contemporains, on peut comprendre l'avantage qu'il y a ainsi à orienter les messages que l'on y trouve afin de défendre telle cause ou assurer la protection de tels intérêts. Le tout à des prix abordables et dans un certain anonymat.

Tout commence par le moteur de recherche. En mai 2009, le tribunal de commerce de Paris [5] a condamné Google à la demande de la société Direct Energie. Notamment en raison de la fonction « suggest », qui permet à l'internaute de se voir proposer des intitulés de mots dès qu'il commence à composer les premières lettres d'un nom dans le champ de recherche dudit moteur. En l'espèce, à peine aviez-vous inscrit les premières lettres de Direct Energie que Google y associait prioritairement le mot « arnaque ». Les magistrats ont considéré que cela constituait un trouble manifestement illicite et participait à une campagne, même involontaire, de dénigrement de la société en question.

Internet va désormais être mis à contribution pour orchestrer des opérations d'information – ou d'influence – de l'opinion publique. Qu'il s'agisse des gens de la rue ou des classes dirigeantes. Sur ce terrain, la différence ne se fait pas avant tout sur le montant des budgets publicitaires

mais bien sur la maîtrise de la pédagogie et la capacité des acteurs à faire passer leur message. Au final, plus le sujet est ardu, plus le caractère multimédia de la Toile est exploité : textes, archives, images, vidéos, enregistrements sonores… Si cette agora numérique permet aux militants sincères et souvent désargentés de prendre la parole, c'est aussi un terrain d'exercice pour les agences de communication de crise et autres stratèges de l'influence tarifée.

L'actualité donne chaque jour l'occasion d'observer les avancées de cette guerre de l'information.

Ainsi, trois jours avant la sortie en librairie en 2007 de l'ouvrage *Pesticides, révélations sur un scandale français* [6], un site Internet intitulé www.alerte-environnement.org se proposait « spontanément » de démonter les arguments présentés dans cet ouvrage qui dénonçait l'usage abusif des pesticides. Sous l'apparence d'un média indépendant, les tenants des groupes chimiques tentaient donc d'élaborer un contre-feu médiatique [7] en envoyant sur le réseau des articles décrivant les deux auteurs comme des « militants s'adonnant à la théorie du complot ». L'objectif visé était clair : affaiblir les critiques

en contestant par avance la fiabilité de leurs auteurs.

Il faut reconnaître que la thématique médicale se prête particulièrement à ce type de campagne. Ce sont des sujets techniques mais aussi sensibles car portant sur la santé – il faut donc chercher des informations pour se faire une idée plus précise – qui recouvrent généralement des enjeux financiers importants.

Début mars 2010, en diffusant sur la Toile un clip stigmatisant les industriels de l'agroalimentaire qui intègrent de l'huile de palme dans leurs recettes, Greenpeace a lancé un débat international sur cette composante contestée. La vidéo parodiait un film publicitaire pour Kit-Kat, une des barres chocolatées phares de Nestlé. Motifs ? Cette huile végétale n'est pas bonne pour la santé humaine et la culture de la palme conduit à des vagues de déforestation en Indonésie qui mettent en danger la survie même des orangs-outans. Face à la polémique, Nestlé s'est engagé, fin mars 2010, à n'utiliser d'ici 2015 que de l'huile certifiée « durable ».

Pour tenter d'infléchir les positions des uns et des autres, l'information est injectée dans les réseaux numériques afin de la mettre au contact du plus grand nombre.

Et cela peut quelquefois porter ses fruits sans qu'il y ait besoin de manipuler le message. Rendre publiques des informations qui n'étaient pas destinées à l'être suffit parfois à faire basculer une situation. À ce sujet, le « Climategate[8] » survenu en novembre 2009, à quelques jours du sommet mondial de Copenhague sur le climat est exemplaire. La publication sur le Net d'une série de courriers électroniques échangés entre universitaires britanniques participant aux travaux du giec (Groupe intergouvernemental d'experts sur l'évolution du climat) et évoquant une possible dramatisation exagérée des changements climatiques à venir, servait opportunément la cause des pays et industriels peu enclins à revoir la politique énergétique mondiale.

À aucun moment dans l'Histoire, les activistes de tous bords n'ont eu accès à une telle capacité de production et de diffusion de leur vérité. Sans filtre éditorial préalable ni barrière financière à l'entrée.

En septembre 2005, l'Association internationale de défense des droits de la presse Reporters sans Frontières (rsf), publiait un *Guide du blogueur et du cyberdissident.* Outre les développements expliquant tout l'intérêt de ce

type de support de communication, trois rubriques veillaient à inculquer à celles et ceux qui désiraient prendre la plume numérique des règles essentielles de cybersécurité. Leurs intitulés étaient très prometteurs : comment bloguer de manière anonyme ? Comment choisir sa technique pour contourner la censure ? Comment assurer la confidentialité de ses e-mails ? En 2010, le site Internet de l'association, www.rsf.org , met à la disposition des blogueurs français un simple résumé des dispositions légales auxquelles ils doivent se soumettre. En cinq ans, la connaissance des arcanes du Net a progressé. Les militants ont donc cessé de dévoiler au grand jour leurs techniques de dissimulation. Plus que jamais, c'est la guerre entre les partisans de la libre parole et les tenants des pouvoirs autoritaires, qu'ils soient financiers ou politiques.

Sur ce terrain, tous les coups sont permis. Même et surtout quand ils mêlent habilement l'art de l'intoxication médiatique à un vrai savoir-faire informatique. Par exemple en instillant auprès de la masse des internautes la peur d'une contamination virale. Très actif pour dénoncer la tenue des jeux Olympiques à Pékin en 2008, rsf a ainsi été l'objet d'une attaque cybernétique de grande envergure la

veille d'une cybermanifestation que ses militants comptaient organiser le 7 août, veille de la cérémonie d'ouverture des jo. Réagissant à cette infiltration, le porte-parole de l'ong est catégorique : « Des pirates ont réussi à s'introduire au sein de l'administration de notre site Internet pour mettre un virus à retardement qui peut contaminer les ordinateurs qui s'y connectent. » Et de préciser : « On sait que ce fichier se fait passer pour un virus mais on ne sait pas s'il s'agit d'un vrai virus. »

Dans ce cas, le virus et les dégâts qu'il pourrait causer deviennent une arme politique, brandie à la face de la communauté des internautes afin de les dissuader de fréquenter dorénavant le site Internet de cette association. En diffusant l'idée que l'infection d'un ordinateur peut se produire par simple connexion au site du mouvement de défense des journalistes, les pirates atteignent leur objectif : faire chuter la fréquentation de ce média militant. Ce qui, dans le brouhaha informationnel du Net, revient quasiment à le rendre muet. Et donc politiquement inopérant.

III. Maîtriser la mémoire collective

Les moteurs de recherche constituent désormais la porte d'entrée sur Internet. Une majorité d'internautes ne se préoccupe plus de retenir les adresses url des sites qu'ils souhaitent visiter. Leur moteur préféré (en France, c'est Google dans plus de 90 % des cas) leur sert de page d'accueil. Ils inscrivent le nom de la société ou du service qui les intéresse, et généralement la réponse souhaitée apparaît dans la première page de résultats que leur soumet ledit moteur. De telles pratiques consolident le caractère incontournable des Baidu, Yahoo, Google et autres Bing (Microsoft).

Tableau 5. – **Les recherches sur Internet (en milliard de recherches)** [9] Marché mondial en décembre 2009**Marché mondial en décembre 2009**

	Décembre 2008	*Décembre 2009*	*Évolution*
Total mondial	**89 708**	**131 354**	**+ 46 %**
Google	55 638	87 809	+ 58 %
Yahoo !	8 389	9 444	+ 13 %
Baidu.com Inc.	7 963	8 534	+ 7 %

Microsoft/Bing	2 403	4 094	+ 70 %
eBay	1 327	2 102	+ 58 %
nhn Corporation	1 892	2 069	+ 9 %
Yandex	992	1 892	+ 91 %
Facebook.com	1 023	1 572	+ 54 %
Ask Network	1 053	1 507	+ 43 %
Alibaba.com Corporation	1 118	1 102	– 1 %

Source : *ComScore,* janvier 2010.

En mémorisant et analysant les requêtes de leurs utilisateurs, les moteurs savent donc en temps réel ce qui intéresse ces derniers.

À tel point que Google, en 2010, a proposé ses services à l'Organisation mondiale de la santé (oms) avec son programme « FlueTrends »[10]. Le moteur de recherche s'estimait en mesure de suivre la progression de la pandémie grippale qui terrorisait alors la planète. La firme considérait en effet que les internautes, inquiets de ressentir certains symptômes, se renseignaient en ayant recours à Internet. En repérant ces mots-clés, et grâce au

panel très fourni que représente la masse des personnes qui utilisent Google, le croisement avec les données géographiques des utilisateurs permettait à la société de Mountain View de disposer d'un observatoire incomparable pour pister l'évolution de cette maladie. La firme annonçant même être en mesure de déceler deux semaines avant les services médicaux l'émergence d'une vague grippale. L'histoire ne dit pas si la surévaluation de ce phénomène pandémique par l'oms est due à ce mode de surveillance ; toutefois, ces événements ont démontré que l'on pouvait trier et lire rapidement le détail des sollicitations du célèbre moteur.

Cette maîtrise de l'information instantanée se trouve complétée par la stratégie de numérisation à grande échelle de contenus que le même Google a adoptée. En effet, sa capacité de calcul – avec son algorithme fétiche – et donc de sélection des données disponibles sur la Toile exige la mise à disposition d'une masse croissante d'informations de toutes sortes. L'idée maîtresse est que chacun y trouve ce qui peut l'intéresser. Et dans le monde de l'Internet, ce qui n'est pas numérisé n'existe tout simplement pas.

Un principe qui explique en partie la décision annoncée par

Google, le 14 décembre 2004, d'initier sur quatre ans un programme de numérisation de quelque 1,5 million d'ouvrages tombés dans le domaine public, notamment la littérature du xix^{e} siècle. Ces volumes émanaient pour l'essentiel des bibliothèques des universités du Michigan, de Harvard et de Stanford aux États-Unis. Prochaine étape annoncée : 15 millions de titres d'ici 2015. Cet objectif sera largement atteint à cette date puisque, en février 2010, Google revendiquait déjà la numérisation de 12 millions de livres – tombés dans le domaine public ou non –, dont 50 % étaient des titres non anglophones.

Selon un rapport sénatorial [11] de 2010, avec les moyens dont dispose l'État français, il faudrait environ 750 millions d'euros et 375 ans pour numériser l'ensemble des ouvrages de la Bibliothèque nationale de France (bnf). Une perspective qui impose presque obligatoirement le partenariat avec des prestataires privés. En restant extrêmement vigilant sur les conditions posées par ceux-ci, afin que ce ne soit pas l'occasion d'une sélection des titres et des contenus qui écarterait tel auteur ou tronquerait tel pan de bibliographie.

Le patrimoine numérique disponible sur la Toile ne se

limite certainement pas aux œuvres littéraires ou artistiques. Ce sont désormais des tranches de vie entière que chacun d'entre nous confie aux serveurs informatiques qui composent le réseau des réseaux. Avec une capacité d'accumulation et d'archivage sans équivalent dans le monde physique auquel nous étions habitués. Des sites de compilations de photographies, aux réseaux sociaux en passant par les blogs ou les commentaires que nous laissons sur la Toile, nous semons ainsi des bribes de notre existence. Disséminés, ces éléments disparates ne sont rien. Mais assemblés, ils deviennent plus pertinents que les fichiers de police les plus élaborés.

Pour incarner cet état de fait, il faut lire le portrait qu'un journaliste d'une revue française indépendante, *Le Tigre* [12], a consacré, fin 2008, à Marc L., un presque trentenaire vivant près de Bordeaux. En cherchant sur Internet, uniquement à partir de sites libres d'accès, le reporter a pu reconstituer la vie sentimentale, professionnelle, familiale, scolaire et amicale de cet ancien étudiant en architecture. Ou comment, avec un peu de patience et d'astuce, la vie de nos contemporains peut faire l'objet de toutes les surveillances. Sans jamais enfreindre aucune loi ni violer d'une quelconque manière l'intimité de

sa cible. Uniquement par une exploitation fine des données disponibles sur le Net.

Pour tenter de pallier cette situation et essayer de reconstituer une sphère privée, voire de faire oublier quelques errements de jeunesse (photos prises sous l'emprise de l'alcool, engagement militant passé…), des sociétés commerciales proposent déjà leurs services pour prendre en charge votre e-réputation. Certaines revendiquent la promesse affichée de faire « disparaître » de la Toile des informations vous concernant jugées indésirables. Or, il y a loin du discours à la pratique.

Si un texte ou une image présents sur un seul site vous pose problème, vous pouvez toujours tenter d'obtenir son retrait par l'animateur dudit site. Il en va tout autrement quand la nouvelle a déjà été indexée par des moteurs de recherche, et qu'elle se trouve donc stockée dans la mémoire de leurs serveurs informatiques. Et que d'autres sites l'ont dupliqué, automatiquement ou délibérément. Chacun de ces supports devient donc un média à qui il convient de demander de retirer le message en question. Face à la difficulté de la tâche, il est alors souvent conseillé de « noyer » l'information litigieuse sous un flot de

nouvelles anodines. Afin de la rendre moins accessible à la majorité des internautes, qui se contenteront pour l'essentiel des premières pages de réponse présentées par leur moteur de recherche favori. L'enfouissement semble donc fréquemment la tactique à privilégier.

Pour certaines personnes ou entreprises mises en cause sur le Net, ne rien faire peut se révéler également être la meilleure des stratégies. En effet, les algorithmes des différents moteurs de recherche ont nettement tendance à mettre en avant les sujets qui suscitent un grand nombre de réactions. En faisant en sorte que la polémique ne s'envenime pas, le sujet a de fortes chances de sombrer à son tour dans les tréfonds des résultats fournis lors d'une requête sur un moteur.

IV. Le piratage numérique comme arme économique

Le domaine artistique représente une incarnation extrême des effets dévastateurs du piratage numérique sur un secteur économique. En 2008 en Europe, les industries créatives (films, musiques, programmes télévisuels,

logiciels) affichaient un chiffre d'affaires de 860 milliards d'euros, soit 6,9 % du pib de l'Union européenne (ue). Côté emplois, elles faisaient travailler 14 millions de personnes, soit 6,5 % de la main-d'œuvre totale de l'ue. En mars 2010, la chambre de commerce internationale (www.icwbo.org) a publié une étude sur les pertes liées à ces piratages en Europe si la consommation de copies illégales continue sur sa lancée actuelle.

Tableau 6. – **Les pertes liées au piratage en Europe**

Année	*Perte de chiffre d'affaires en Md€*	*Perte d'emplois cumulée*
2008	10	186 600
2009	12	227 500
2010	15	276 900
2011	19	351 500
2012	22	422 400
2013	26	491 800
2014	30	555 700
2015	32	611 300

Source : Chambre de commerce internationale-Tera Consultants, *Enjeu de l'emploi dans les industries créatives,* mars 2010.

Ces scores plaident résolument pour une surveillance de la Toile afin de poursuivre les contrefacteurs. Toutefois, l'ampleur de la révolution technologique, et donc économique, intervenue dans ce secteur justifie peut-être davantage encore une refonte du modèle artistique et commercial qui s'applique à ces métiers. Ils ne pourront durablement assurer leur salut et leur avenir en se fondant sur des techniques de contrôle des internautes. La barrière technologique est si fragile qu'elle ne saurait sérieusement constituer un rempart protecteur pérenne pour les futures marges bénéficiaires des professionnels de ces industries créatives.

Le piratage numérique peut ensuite trouver sa place au sein d'activités elles-mêmes illicites telles que les paris et autres casinos en ligne. Dans un rapport [13] remis au ministre français du Budget en 2009, le criminologue Alain Bauer décrit l'implication de la mafia italo-américaine dans le cyberespace comme étant essentiellement liée à l'industrie

des jeux et des paris en ligne (mais également à la pornographie). Outre les sommes éventuellement blanchies lors de ces opérations, les auteurs de vols ou de détournements des données personnelles voire bancaires confiées par les parieurs ont la conviction que leurs victimes ne chercheront pas à porter plainte.

Le support numérique peut enfin servir à diffuser et commercialiser des prestations ou des productions illégales. Faux médicaments, faux diplômes et certificats, pièces détachées contrefaites, appareils électroniques de contrebande… seule l'imagination semble pouvoir limiter la liste des biens piratés que l'on peut acquérir sur le Net.

Le piratage est donc bel et bien une pratique qui fragilise nos économies développées. Et pas seulement un phénomène marginal qui se limiterait à la copie de dvd ou de succès musicaux. La faculté d'entrer dans un système et de dupliquer ses contenus est un facteur de déstabilisation sans précédent de nos sociétés modernes.

Puisque les organisations criminelles internationales persistent à ne pas publier leurs comptes annuels, il est évidemment difficile de cerner le périmètre de leurs actions et de les traduire en termes financiers, ou en tout cas

chiffrés. Pour contourner cet état de fait, l'éditeur de solutions informatiques Symantec[14] a observé durant une année entière (de juillet 2007 à juin 2008) les publicités qui vantaient les mérites de « biens et services frauduleux » sur des réseaux de discussion instantanée (irc).

Même si on se doute de la motivation commerciale de ce fournisseur de technologies de sécurité à démontrer que la Toile est un territoire où les dangers sont permanents, l'originalité et la durée de son enquête méritent que l'on s'y intéresse. Symantec déclare ainsi avoir surveillé au cours de ces douze mois, quelque 69 000 cybercriminels qui auraient publié 44,3 millions de messages publicitaires sur ces forums. Best-seller incontesté : les numéros de cartes de crédit, vendus en moyenne 8 centimes d'euros l'unité, qui représenteraient 59 % de la valeur totale du marché des produits et services cybercriminels étudié par l'éditeur.

Viennent ensuite les coordonnées bancaires, dont le prix de vente grimpe selon la localisation géographique de son détenteur légal et le montant de liquidités disponible sur ledit compte. Il faudrait alors débourser de 8 à 780 dollars l'unité. On peut également trouver des pourriels (spams)

ou des messages d'hameçonnage *(phishing)* prérédigés ou encore des annuaires d'adresses e-mails. Les offres, très complètes, permettent d'envisager de la sous-traitance : on peut en effet acquérir pour moins d'un millier d'euros la description d'une faille informatique constatée dans l'architecture d'un site Internet financier. Fort de cette information, son acheteur pourra faire chanter le gestionnaire du site ou exploiter à son profit la brèche technique.

Symantec formule des estimations sonnantes et trébuchantes, en affirmant que le montant des échanges de services cybercriminels que ses équipes ont étudié de juillet 2007 au mois de juin 2008 s'élèverait à 276 millions de dollars. L'éditeur établit à 7 milliards de dollars le chiffre d'affaires qu'ils auraient permis de générer. Soit respectivement 5,3 milliards de dollars pour les seuls numéros de cartes de crédit piratés et 1,7 milliard pour l'exploitation des coordonnées volées de comptes bancaires.

Ces évaluations donnent une idée des sommes en jeu, même si la question de la sanction encourue ne peut manquer de venir à l'esprit. La question se pose également

de savoir comment un opérateur marchand peut-il être en mesure d'effectuer une telle surveillance de réseaux criminels qui ont pignon sur rue, sans disposer de pouvoirs judiciaires et de police… En tout cas, force est de constater qu'ils disposent de vitrines aisément accessibles sur le Net. Une situation qui s'explique notamment par le décalage croissant entre la mondialisation effectivement rendue abordable par ces technologies de l'information qui se jouent des frontières et les rigidités des procédures administratives, judiciaires et policières qui peinent à sortir de leur cadre national ou régional, malgré les accords formels de coopération et de partenariat qui ont pu être signés par les différentes autorités politiques.

À l'instar de ces pêcheurs nonchalants qui laissent filer une ligne à l'arrière de leur bateau durant une promenade en mer, le pirate mise parfois sur la chance, ou, au contraire, la malchance des internautes. Notamment lorsqu'il a pris soin d'acheter les noms de domaines proches d'intitulés célèbres ou d'adresses Internet très fréquentées. Son but ? Accueillir les internautes pressés qui rédigent l'url de leur site de destination avec des fautes de frappe ou d'orthographe. On appelle cela le *cybersquatting*. Par exemple, entre le 30 mars et le 11 avril 2010, 738 noms de

domaines de ce genre en.fr ont été enregistrés. On y trouve pêle-mêle : www.ailymotion.fr , www.vingtminutes.fr , www.googele.fr , www.onforama.fr , www.interieurgouv.fr , etc. L'idée est de capter l'audience de ces sites leaders et de leur proposer une page avec des liens sponsorisés. À chaque clic, c'est un peu d'argent qui rentre. L'opération s'avère fort lucrative dès lors que le nombre de ces versions pirates est élevé. Si le titulaire de la marque ainsi parasité le souhaite, il peut obtenir la suppression de cette adresse illégitime. Ou même la récupérer à son profit en quelques semaines. Mais s'il en ignore l'existence ou s'il n'effectue pas les démarches *ad hoc,* elle reste active. En ce qui concerne le.fr, après les excès qui ont suivi la libre acquisition de ces adresses, les cas litigieux représenteraient aujourd'hui seulement 1 % des noms déposés.

La création de fausses pages Web présentant des adresses proches de celles de sociétés dotées d'une bonne réputation peut aussi constituer un leurre efficace afin d'obtenir les données personnelles ou bancaires de l'internaute trop pressé pour vérifier qu'il est arrivé à bon port.

En 2009, l'Organisation mondiale de la propriété intellectuelle (ompi) a enregistré 2 107 plaintes déposées par des détenteurs de marques contre un cybersquattage. Un bel exemple de mondialisation réussie : elles impliquaient 114 pays !

Tableau 7. – **Nombre annuel de litiges relatifs à des noms de domaine administrés par l'Organisation mondiale de la propriété intellectuelle (ompi)**

Année	*Nombre de litiges*	*Nombre de noms de domaine*
2000	1 857	3 760
2001	1 557	2 465
2002	1 207	2 042
2003	1 100	1 774
2004	1 176	2 559
2005	1 456	3 312
2006	1 824	2 806
2007	2 156	3 545
2008	2 329	3 958
2009	2 107	4 688

Source : ompi, www.wipo.int , 2010.

En 2009, le groupe hôtelier InterContinental a déposé la plainte la plus importante puisqu'elle portait à elle seule sur 1 545 noms de domaine.

La lutte contre le piratage a conduit une quarantaine d'États (dont l'Union européenne) à entamer, en 2008, la négociation d'un traité[15] désigné sous le nom d'acta (Anti-Counterfeiting Trade Agreement). Alors qu'il s'agit d'enjeux essentiellement commerciaux, les États-Unis ont demandé et obtenu que l'ensemble des discussions relatives à ce texte soit classé secret Défense. Ce qui interdit leur diffusion hors des enceintes de la négociation. L'idée est de mettre en place des contrôles supplémentaires sur la Toile afin de vérifier le respect de la propriété intellectuelle des biens numériques disponibles sur le réseau : films, jeux vidéo, logiciels, musique… Largement poussé par les industriels, ce processus d'élaboration de la norme, mené à l'écart de tout débat public, va à l'encontre de la logique collaborative de l'internet. Et suscite de vives interrogations quant à l'impact de telles mesures de contrôle sur la confidentialité

des échanges sur le Net. Le texte final est attendu pour la fin de l'année 2010.

V. Le commerce illégal

Quel internaute n'a pas vu sa messagerie électronique déjà envahie de propositions commerciales pour recevoir une célèbre pilule bleue destinée à lutter contre les problèmes d'érection, ou pour des anabolisants et autres granules prétendument amincissantes ? La diffusion à très grande échelle de telles offres paramédicales témoigne de l'importance de ce marché parallèle qui se nourrit essentiellement de contrefaçons. La généralisation du Net a participé à la remise en cause des structures établies de longue date au service de la sécurité des échanges. Ainsi, le choix français de confier, par le passé, l'exclusivité de la commercialisation des médicaments à des pharmaciens a certainement contribué à la garantie de salubrité de la très grande majorité desdits médicaments mis en circulation dans notre pays.

Pourtant, la jurisprudence européenne est formelle : frapper d'une interdiction nationale des médicaments

vendus par correspondance, ayant reçu une autorisation de mise sur le marché d'un État de l'Union européenne et non soumis à une prescription médicale, est contraire au droit communautaire. L'arrêt DocMorris [16] rendu par la Cour de justice des Communautés européennes le 11 décembre 2003 l'a confirmé. Et de nombreux États européens ont ainsi légalisé ce marché de la vente de médicaments *via* le Net : comme la Belgique, l'Allemagne, les Pays-Bas, le Royaume-Uni ou la Suisse. Certains ont opté pour un formalisme de façade. À l'instar de l'Australie et de la Nouvelle-Zélande, où les sites peuvent commercialiser des médicaments dès lors qu'ils salarient un médecin et que celui-ci procède à une rapide discussion avec le patient avant de conclure la vente. Première brèche en France : dans une décision [17] du 8 mars 2007, le Conseil de la concurrence a admis la capacité des distributeurs de produits cosmétiques de les vendre et d'en faire la publicité sur Internet. En l'espèce, l'autorité administrative indépendante désignait notamment les produits « dermocosmétiques » commercialisés exclusivement sur « conseil pharmaceutique » dans un réseau de distribution sélective.

Paris envisage désormais de remettre en cause sa doctrine

historique en autorisant par un prochain texte de loi la vente des produits non remboursables et disponibles sans prescription médicale.

Là encore, la cybersécurité de ces échanges marchands devra passer par un contrôle accru de la qualité des produits ainsi diffusés pour éviter que ce canal de distribution ne soit l'occasion d'un commerce de molécules contrefaites ou dangereuses pour la santé. Une enquête conduite en juin 2008 pour le compte de l'Alliance européenne pour l'accès à des médicaments sûrs (eaasm [18]) affirmait que « 62 % des médicaments achetés en ligne sont des contrefaçons ou des produits de qualité inférieure ». Même si cette Alliance défend ouvertement les intérêts de l'industrie pharmaceutique (elle compte parmi ses membres les groupes Bayer, Pfizer ou Johnson &Johnson), la présence en grand nombre de contrefaçons sur le réseau est difficilement contestable.

Il en va ainsi très souvent des domaines d'activité lucratifs où les autorités exerçaient jusqu'alors une tutelle manifeste et où l'apparition d'Internet vient bousculer la donne. C'est notamment le cas pour les jeux et paris en ligne, qui constituent des enjeux de cybersécurité de la première

importance. En effet, ils concentrent potentiellement toutes les composantes d'une activité criminogène. Blanchiment d'argent sale, escroquerie, enchères truquées, corruption… sont autant de délits bien connus susceptibles de surgir parallèlement à ces jeux numériques. Avec en ligne de mire, si l'on est pris, des sanctions finalement moindres que pour la plupart des autres activités crapuleuses (trafic de stupéfiants…). Il est donc loin le temps des casinos de bord de mer où les effectifs de la Brigade des courses &jeux des Renseignements généraux suffisaient à surveiller ce petit monde des tapis verts et des hippodromes.

Ce souci d'encadrer ces jeux d'argent répond au moins autant à une préoccupation de santé publique que de la volonté de l'État de préserver ses rentrées financières. Une motivation qui n'est peut-être pas glorieuse mais qui explique en partie la prudence gouvernementale en matière de libéralisation de ce secteur au profit de nouveaux entrants. La règle en vigueur jusqu'alors était le monopole de La Française des Jeux et du Pari mutuel urbain pmu). Mais, construction européenne oblige, Bruxelles a exigé la fin des situations monopolistiques et forcé la France à créer les conditions d'une concurrence accrue. Depuis le 12

mai 2010, une loi[19] *ad hoc* fixe un cadre juridique spécialement adapté à cet univers numérique.

Paris compte bien assurer par ailleurs le respect de ses législations nationales. Même sur l'Internet mondial. En effet, l'article 113-2 de notre Code pénal établit expressément que la loi française s'applique non seulement aux infractions commises sur le territoire de la République, mais également à celles qui sont réputées commises dès lors qu'un des faits constitutifs de l'infraction a eu lieu sur ce territoire.

Ainsi le fait de pouvoir se connecter à partir de la France à un site situé à l'étranger, et qui propose des jeux d'argent non autorisés sur notre sol, est constitutif d'une infraction pénale selon les termes de la législation tricolore.

L'article 46 du Code de procédure civile établit en outre que le demandeur peut notamment saisir la juridiction du lieu où le dommage a été subi. Ainsi, un tribunal situé dans l'Hexagone sera compétent pour juger de l'action d'un site installé hors de notre territoire national. Par extension, un site Internet qui assurerait la publicité et la promotion de jeux de hasard en ligne non autorisés en France serait aussi en infraction avec les lois françaises. Cette interdiction

relève d'une loi sur les loteries prohibées du 21 mai… 1836. Soit bien avant l'ère Internet.

Autre « vice » mais même principe, en ce qui concerne la commercialisation du tabac dont le monopole est attribué aux débits de tabac par l'article 568 du Code général des impôts. Dans la majorité des cas, c'est la direction générale des Douanes qui poursuit les cybermarchands contrevenants. Par exemple, en mars 2007, elle a obtenu la condamnation du site www.e-tabac.com qui proposait des cartouches de cigarettes issues de différents trafics internationaux. Mais, à peine repérés, ces commerçants fraudeurs réapparaissent sous un autre intitulé.

Leurs compétiteurs directs ? Les réseaux de vendeurs à la sauvette installés dans les grandes villes, qui viennent, chaque jour un peu plus, concurrencer à leur tour les canaux légaux. La cigarette étant peut-être l'un des rares produits où la vente dans la rue « résiste » bien face aux offres disponibles sur le Net. L'inquiétude du client à l'idée de se faire identifier lors de l'envoi par courrier et le fait de disposer immédiatement de ses paquets seraient autant d'incitations à se fournir en bas de chez soi.

Naturellement, les éventuelles escroqueries ou

détournements de coordonnées bancaires qui interviendraient sur ces sites illégaux ne font généralement l'objet d'aucune plainte de la part de leurs victimes qui peuvent difficilement justifier de leurs achats illicites auprès des services de police… Or, la plupart de ces commerces n'étant pas particulièrement préoccupés de se bâtir des réputations commerciales qui fidéliseraient leur clientèle, les déceptions sont nombreuses. Produits non conformes ou jamais livrés, données revendues à des tiers, vol d'argent… l'éventail des désagréments subis est assez vaste.

Notes

[1] www.twitter.com

[2] Karen Nelson , Richard Price et Brian Rountree , *Do Investors Pay Attention to Stock Spam?*, Rice University, (Texas), mars 2009.

[3] Zhi Da , Joseph Engelberg et Pengjie Gao , *In Search of Attention*, University of Notre Dame, (Indiana), juin 2009.

[4] Son rapport annuel est disponible sur son site Internet : www.ftc.gov

[5] Tribunal de commerce de Paris, 7 mai 2009, Direct Energie/Google Inc.

[6] Fabrice Nicolino et François Veillerette , *Pesticides, révélations sur un scandale français*, Paris, Fayard, 2007.

[7] « Une attaque pas très net(te) », *Le Canard enchaîné,* 21 mars 2007.

[8] « “Climategate” : courriels piratés, une tentative pour discréditer les scientifiques du Giec », afp, 7 décembre 2009.

[9] Sondage réalisé auprès d'un panel d'internautes de plus de 15 ans se connectant à partir de leur domicile ou de leur bureau.

[10] www.google.org/fluetrends

[11] Yann Gaillard , *La Politique du livre face au numérique*, Sénat, février 2010.

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

[13] Alain Bauer , *Jeux en ligne et menaces criminelles*, Paris, La Documentation française, 2009.

[14] Symantec Corp., Symantec Report on the Underground Economy, novembre 2008.

[15] Version de travail disponible en avril 2010 : http://trade.ec.europa.eu/doclib/docs/2010/april/tradoc_146

[16] Arrêt Deutscher Apothekerverband ev / 0800

DocMorris nv et Jacques Waterval, 11 décembre 2003.

[17] www.conseil-concurrence.com /user/avis.php?avis=07-D-07

[18] http://fr.eaasm.eu

[19] Loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne.

Chapitre IV

Les parties prenantes de la cybersécurité

La cybersécurité – à la différence des opérations militaires des siècles précédents – n'est donc pas l'apanage des gouvernements ni des armées régulières. Ceux-ci ne sont qu'un acteur parmi d'autres : du simple particulier aux organisations de dimension mondiale.

I. Les États

Si, dans l'opinion publique, la Toile est perçue comme un terrain de jeu planétaire qui rompt avec les contraintes géographiques et politiques physiques, il n'en est rien dans les faits. Les États, en effet, ne sont aucunement prêts à renoncer à leurs prérogatives sur ces « territoires »

numériques. Et chacun de se doter de services, administrations ou états-majors spécialement dédiés au Net, non sans générer, au final, une certaine cacophonie juridico-politique, puisque les valeurs et les spécificités culturelles ne sont séparées que par un clic de souris. Ce qui relève de la liberté d'expression dans telle grande démocratie est considéré comme une apologie du nazisme dans telle autre. Et on ne parle pas là des régimes autoritaires qui se donnent le droit de filtrer toutes les informations accessibles dans leurs pays, comme ils le font avec les correspondances postales et la presse écrite ou audiovisuelle.

Dans nombre de pays, en outre, l'État n'est pas seul à la manœuvre. Il lui faut composer avec des opérateurs commerciaux, qui sont immanquablement moins souples et réactifs que des services de police intégrés, mobilisables à l'envi. On verra dans le chapitre V que les gouvernements ont apporté des réponses institutionnelles disparates, fruits de leur culture… et de leur capacité budgétaire.

Dans la limite du droit et de ses engagements internationaux (participation à l'Organisation mondiale du commerce ou à l'Union européenne par exemple), chaque

État va donc tenter d'encadrer le développement de ces activités cybersécuritaires privées.

En France, un arrêté du 2 juin 2006 établit la liste des secteurs d'activités d'importance vitale. Ce qui signifie qu'ils participent à l'exercice de la souveraineté nationale et que les investissements étrangers (c'est-à-dire non issus de l'Union européenne) doivent y faire l'objet d'une autorisation du ministre de l'Économie. Ils sont au nombre de onze et concernent tous peu ou prou la sphère informatique. On y trouve les matériels conçus pour l'interception des correspondances et la détection à distance des conversations, les équipements permettant l'évaluation de la sécurité offerte par les produits et les systèmes des technologies de l'information, les moyens et les prestations de cryptologie…

Notre pays s'est efforcé d'établir une liste close, même si celle-ci est sujette à interprétation, notamment parce qu'elle inclut les biens et technologies dits duaux, c'est-à-dire pouvant avoir des usages aussi bien militaires que civils. Disposer au préalable de l'énumération des secteurs « protégés » a au moins le mérite de la clarté aux yeux d'éventuels investisseurs. Soucieux de ne pas se lier les

mains par avance, les États-Unis ont, de leur côté, choisi une règle qui les favorise : est considéré comme stratégique tout domaine, organisation ou activité désigné comme tel par le Président. Une mise sous protection qui peut intervenir à tout moment, quitte à prendre de court un candidat non-états-unien à l'investissement. Soit une démonstration supplémentaire de la marge de manœuvre que les États comptent bien conserver dans cette course permanente à l'innovation technologique.

Ainsi en octobre 2009, l'agence de l'us Army spécialisée dans la recherche, la darpa (Defense Advanced Research Projects Agency), a reconnu avoir chargé différents prestataires privés (on trouve parmi eux Lockheed Martin, Microsoft, Juniper Networks, ou encore la prestigieuse université de Stanford) de développer un nouveau protocole de réseau. Baptisé *Military Network Protocol* (mnp [1]), celui-ci serait donc distinct du protocole tcp/ip actuellement utilisé pour Internet. Ce programme est doté pour commencer d'un budget d'environ 30 millions de dollars. Outre l'indispensable sécurité des communications, ce nouveau protocole devra s'adapter aux utilisateurs en allouant, à la demande, les volumes de bande passante nécessaires. Notamment pour l'émission et la

consultation de vidéos ou de systèmes lourds de cartographie. Cet Internet robuste et capable de véhiculer simultanément des masses très importantes de données devrait *in fine* être réservé à l'usage exclusif des militaires états-uniens. L'ancrage national dudit réseau ne fait donc ici aucun doute.

II. Les organisations internationales

Un constat : aucune organisation transnationale établie n'a pu ou su asseoir son autorité sur les thématiques relatives à Internet ou à la cybersécurité. C'est au contraire un véritable patchwork institutionnel qui tente de répondre à ces enjeux d'avenir. Si de nombreuses organisations internationales se sont tour à tour saisies de la question d'Internet, notamment en matière de cybersécurité, aucune approche réellement coordonnée n'en est sortie.

1. L'Organisation des Nations unies (onu)

À l'instar des sommets de Kyoto et de Rio sur l'environnement – réunis sur des thématiques jugées si vastes et stratégiques pour l'avenir de la collectivité humaine qu'elles supposaient une coopération effective à l'échelle de la planète –, l'onu a jugé qu'Internet méritait une rencontre solennelle des chefs d'État et de gouvernement.

Celle-ci a été dès l'origine conçue pour se dérouler en deux temps. D'abord, à Genève en décembre 2003 pour le premier volet de ce Sommet mondial sur la société de l'information (smsi [2]), organisé par l'Union internationale des télécommunications (uit, l'agence spécialisée de l'onu). Mais rien de véritablement concret n'émergea et ce fut essentiellement un défilé de gouvernants d'États plus ou moins démocratiques qui se sont succédé à la tribune pour vanter les mérites de la société de l'information, même si nombre d'entre eux étaient loin de laisser pratiquer ce libre exercice de l'information sur leur territoire ; ce décalage flagrant affaiblissait d'autant la portée d'une telle réunion.

Le second volet, à Tunis, en novembre 2005 ne s'est guère montré plus productif. Principale avancée : la constitution

d'un Forum sur la gouvernance de l'Internet (fgi [3]) qui réunit les parties prenantes : associations d'utilisateurs, États, groupes de pression, entreprises… D'un point de vue très prosaïque, les sociétés commerciales sont mises à contribution. Et c'est ainsi que l'on retrouve des géants industriels tels AT&T, Cisco Systems ou l'allemand Siemens comme partenaires soutenant cet organisme international. Parmi ses missions : discuter des politiques publiques permettant la sécurisation de l'internet.

Ce n'est sans doute pas un lieu de prise de décision immédiate mais bien un terrain d'influence à part entière, comportant de nombreux groupes de travail et de réunions plénières disséminés aux quatre coins du globe : en 2009 à Charm el-Cheikh (Égypte) ou en septembre 2010 à Vilnius (Lituanie).

Au final, hormis la déclaration généreuse mais guère réaliste faite en février 2010 par le directeur général de l'uit lors du Forum de Davos d'édicter un traité international interdisant la cyberguerre, l'onu n'est pas un acteur de la cybersécurité à l'échelle mondiale.

2. Le G 8

Il faut reconnaître aux États membres du G 8 (Allemagne, Canada, États-Unis, France, Italie, Japon, Royaume-Uni, Russie) leur antériorité en matière de perception de la cybermenace. En effet, lors d'une rencontre des ministres de l'Intérieur et de la Justice de cette organisation informelle qui s'est tenue les 9 et 10 décembre 1997, les participants ont mis en place un réseau de correspondants, dit 24/7 (High Tech Crime Point of Contact Network). Ces équipes sont à même de communiquer entre elles sept jours sur sept, 24 heures sur 24, afin de réagir le plus promptement possible en cas de cyberattaque.

Il est frappant de constater que dès 1997, ces ministres des huit pays les plus riches du monde avaient perçu [4] avec une grande lucidité les menaces futures ainsi que les obstacles techniques et juridiques qui ne manqueraient pas de survenir.

Depuis lors, la coopération internationale bute effectivement sur les divergences juridiques des droits nationaux face à une criminalité naturellement mondialisée, sur des différences normatives en matière d'analyse des ordinateurs qui fragilisent les enquêtes transnationales ou les délais trop longs qui ne permettent pas de traiter en

temps opportun des affaires où les délinquants sont particulièrement mobiles et réactifs.

Là encore, c'est bien la volonté politique qui fait défaut et non l'absence d'une vision claire de la situation. Ainsi, dans une enquête [5] menée en 2008 auprès des polices du Canada, le cabinet Deloitte mentionne le témoignage d'un procureur obligé de patienter entre six et neuf mois avant d'obtenir des réponses à ses questions quand il sollicite un homologue étranger. Des calendriers guère compatibles avec la volatilité des technologiques numériques…

3. L'Organisation de coopération et de développement économiques (ocde)

Ancrée dans son domaine de compétence qu'est le monde économique, l'ocde s'est inquiétée depuis les années 1970 de la possible exploitation malintentionnée des données privées accumulées par les systèmes informatiques qui se généralisaient alors dans les entreprises. Régulièrement depuis, ces rapports avertissent les autorités politiques chargées de l'économie des périls des cyberattaques sur la

communauté des affaires. Fait certain, il ressort de ces analyses – à l'instar des travaux[6] désignant dans les logiciels malveillants une menace mortelle pour l'économie Internet (2008) – que le secteur privé compte avant tout sur les pouvoirs publics pour sécuriser le cybermonde.

L'aspect positif, si l'on peut dire, de cette inquiétude exprimée par les sociétés commerciales réside dans le fait qu'elles semblent chaque jour davantage prêtes à entamer un dialogue avec les autorités. Alors que jusqu'à présent l'omertà prévalait généralement, chaque entreprise se gardant bien de confier aux services étatiques les malheurs qu'elle avait pu rencontrer sur le Net. Une attitude qui ne favorise évidemment pas l'identification précise des menaces et donc la mise en place de mesures protectrices.

4. L'Union européenne

Sur le papier, les Vingt-Sept sont parés pour la guerre numérique, puisqu'ils disposent, depuis 2004, d'une Agence européenne chargée de la sécurité des réseaux et de l'information, l'enisa [7] (European Network and Information Security Agency). Mais celle-ci n'a jamais reçu les moyens réels de se développer, ni de travailler sur

le fond des dossiers. Basée à Héraklion en Crète, ses maigres financements (8 millions d'euros de budget annuel) ne lui permettent guère une activité débordante. D'autant que ses pères fondateurs ont eu l'idée saugrenue de lui fixer une durée d'existence de cinq ans. Conséquence : à partir de 2008, ses équipes se sont concentrées sur le seul sujet qui les intéressait alors vraiment : la préservation de leur emploi !

À l'issue d'un lobbying intensif, l'enisa a été prolongée au moins jusqu'au 13 mars 2012. Il y a fort à parier que le même activisme sera déployé à partir de 2011, au détriment des sujets de cybersécurité. En attendant, l'Agence publie quelques rapports ; par exemple, en 2010, des publications relatives aux réseaux sociaux, aux jeux en ligne et au Web 2.0.

Tandis qu'une décision-cadre du Conseil européen du 16 mars 2005 invite l'Union à mettre en place des « outils et des procédures efficaces » pour lutter contre les attaques visant les systèmes d'information. Belle ambition ! Néanmoins, les gouvernements européens tardent à la transposer dans leur droit national.

Au final, l'essentiel de la stratégie de l'ue en matière de

cybersécurité se limite à inciter ses membres à participer au réseau 24/7 du G 8.

5. L'Organisation du traité de l'Atlantique Nord (otan)

À l'occasion des cyberattaques qui frappèrent l'Estonie (tout jeune membre de l'otan) au printemps 2007, l'Alliance atlantique a été la première organisation internationale réellement confrontée à cette guerre numérique. Tallinn n'a pas tardé, en effet, à faire appel à ses puissants alliés pour contrer les assauts dont elle faisait l'objet. La République balte invoqua même l'application *hic et nunc* de l'article 5 du traité fondateur de 1949 qui prévoit que si un membre de l'Alliance est attaqué, celle-ci doit lui venir en aide et participer éventuellement à la riposte. Les alliés ne firent pas la même lecture et estimèrent qu'il n'y avait pas là matière à intervention. Si la cible avait été plus grosse et l'assaillant présumé moins gros, peut-être l'appréciation des faits aurait-elle été différente…

Depuis 2008, l'otan a ouvert, à Tallinn, un centre[8]

d'analyse et d'expertise en matière de cybersécurité. C'est pour l'essentiel un think-tank chargé de réfléchir aux enjeux et perspectives en matière d'attaques numériques. Seuls sept États y participent à ce jour : l'Estonie, la Lituanie, la Lettonie, l'Espagne, l'Allemagne, l'Italie et la Slovaquie. Clin d'œil à l'Histoire, il est donc installé dans le premier pays à avoir connu une cyberattaque globale sur les principaux pans de ses systèmes d'information nationaux.

Autre nouveauté : en avril 2008, l'otan a créé une Autorité politique chargée de la cyberdéfense (Cyber Defense Management Authority, cdma). Son rôle ? Lancer et coordonner « des mesures immédiates et efficaces de cyberdéfense chaque fois que les circonstances l'exigent ». Soit une fonction de commandement central pour les activités techniques, politiques et de partage de l'information menées par les membres de l'Alliance. La cdma pilote en outre des exercices de simulation de cyberattaques à grande échelle impliquant plusieurs pays.

6. Interpol

Face à la montée en puissance de la cybercriminalité organisée, en 2008, Interpol [9] (188 États membres) s'est

dotée d'une unité d'informatique légale et dispose de son propre maillage de correspondants internationaux qui sont en contact 24 heures sur 24. Il s'agit là d'une avancée supplémentaire en matière de coopération policière internationale. En outre, cette instance organise tous les deux ans une conférence réunissant praticiens, universitaires, juristes et experts techniques du secteur privé afin d'échanger sur les pratiques cybercriminelles présentes et à venir. Dans un souci d'efficacité, Interpol a réparti par zones géographiques ses différents groupes de travail qui planchent sur la criminalité numérique : Asie-Pacifique Sud, Afrique, Amériques, Europe, Afrique du Nord-Moyen-Orient. Cette sectorisation évite ainsi les pesanteurs d'une assemblée pléthorique et permet de prendre en compte les spécificités régionales. À charge ensuite, pour ces entités, d'échanger entre elles de la manière la plus fluide possible.

III. III. – Les entreprises

Les sociétés commerciales sont dans une logique pour le moins ambivalente, pour ne pas dire schizophrénique, au sujet d'Internet, des technologies de l'information et de la

communication en général. Elles veulent à la fois apparaître sous leur meilleur jour sur la Toile, profiter de la mobilité désormais facilitée par les outils électroniques (téléphones portables, assistants personnels, portables ultralégers…) permettant de faire travailler ses collaborateurs au plus près du terrain et faire des économies en externalisant à des prestataires ses infrastructures informatiques. Or, chacune de ces intentions a son revers en matière de cybersécurité.

La prolifération des attaques informationnelles, les connexions à distance et les occasions de perte des supports numériques sont autant de facteurs de faiblesse potentiels. De même, le transfert systématique à des sous-traitants de toute la capacité informatique de l'entreprise peut représenter une menace sur la confidentialité des données et une dépendance à des fournisseurs qui peuvent aisément conserver par-devers eux certaines informations sensibles une fois le contrat arrivé à échéance. Voire, pendant que celui-ci est en train de courir, si les serveurs en question se trouvent dans des pays dont les gouvernements exigent – et obtiennent – la coopération des sociétés présentes sur son territoire. Cette dimension de la guerre économique ne doit pas être sous-estimée : elle fait partie intégrante de la stratégie de cybersécurité. La

recherche d'économies à court terme peut ainsi se révéler finalement un facteur de destruction de richesses à moyen terme.

Il convient en outre de diffuser une véritable culture de la sécurité auprès de tous les échelons hiérarchiques, bien au-delà des seules équipes de direction ou du service informatique. Dès lors que des salariés disposent d'un ordinateur relié à l'internet ou à un réseau interne sur lequel circulent des informations qui participent à la stratégie de l'entreprise, ils doivent être considérés comme partie prenante du processus global de sécurité.

Dans ce domaine de la protection de l'information, la fragilisation de l'ensemble d'une structure peut émaner d'un échelon subalterne. Par exemple, en janvier 2009, plusieurs dizaines de milliers d'ordinateurs fonctionnant sous Windows de Microsoft ont été contaminés par un ver informatique répondant au nom de *Conficker.* Parmi les équipements ainsi infectés par ce dispositif, on trouvait certains ordinateurs du ministère français de la Défense. Dans ce cas, après enquête, l'infection aurait été causée par une clé usb. En principe interdit sur des équipements militaires, l'usage d'un accessoire aussi banal a rendu

obligatoire une inspection complète du réseau informatique incriminé.

Malgré la diffusion croissante dans le grand public et chez les professionnels d'appareils numériques fixes ou mobiles de plus en plus sophistiqués, le principe même de risque informatique reste encore largement théorique au sein de la population française. Qui se partage essentiellement entre les inconscients et celles et ceux qui considèrent que cela ne concerne que les autres. Un constat que l'on fait également dans les entreprises et les administrations. Un *a priori* de confiance semble préserver les utilisateurs de toute inquiétude sécuritaire.

Tableau 8. – **Actions menées à la suite d'un incident informatique dans les entreprises françaises en 2009**

		Au cours des 12 derniers mois, vous avez eu connaissance, concernant votre entreprise, d'un incident de sécurité informatique :				
		Tout type d'incident	Un non-respect des directives de sécurité	Un virus ou un ver	Des spams	Une perte de données
Les actions suivantes ont-elles été menées à la suite de ces incidents ? (en %)	Une révision de la politique de sécurité	**29**	43	42	26	43
	Une enquête interne	**53**	69	63	55	58
	La mise en place de contre-mesures	**27**	62	36	21	33
	L'activation d'un processus disciplinaire	**10**	29	7	7	19
	Une action en justice	**5**	3	2	3	8
	Non, aucune	**30**	3	22	34	17

Source : « L'insécurité numérique des entreprises », volet chefs d'entreprise, institut Sofres, octobre 2009.

Tableau 9. – Incidents de sécurité subis par les entreprises

françaises en 2008-2009

Dirigeants en %		*Salariés en %*	
Des spams	43	Des spams	43
Un virus ou un ver	26	Un virus ou un ver	27
Un non-respect des directives de sécurité	13	Une perte de données	23
Une perte de données	13	Un non-respect des directives de sécurité	17
Une attaque immobilisant une partie du système d'information	7	Une attaque immobilisant une partie du système d'information	14
Un vol de données	5	Un vol de données	7
Une atteinte à la réputation de votre entreprise	4	Une usurpation d'identité	7
Une usurpation d'identité	2	Une fraude financière	6
Une fraude financière	1	Une atteinte à la réputation de votre entreprise	6
Non, aucun	39	Non, aucun	34

Source : « L'insécurité numérique des entreprises », institut Sofres, octobre 2009.

Les grandes firmes de l'Internet ont désormais formalisé leurs relations avec les services de police des différents pays dans lesquels elles opèrent. Même si la discrétion est, dans ce domaine, une vertu largement revendiquée par ces sociétés. Pour s'en convaincre, il a suffi de constater la célérité avec laquelle l'opérateur de messagerie Yahoo Inc. a tenté de faire disparaître du Net son livret d'instructions rédigé à l'usage des services de police. Mis en ligne le 2 décembre 2009 par le site www.cryptome.org ce « guide de conformité à l'application des lois » révélait notamment les tarifs pratiqués par Yahoo pour divulguer des informations sur ses clients à la demande d'un juge. Il faut débourser de 20 à 60 dollars pour connaître l'intimité numérique d'un individu : ses recherches sur la Toile, le contenu de sa messagerie instantanée, ses photographies compilées sur la plate-forme « Flickr » et ses diverses correspondances sur les Yahoo Groups, les forums maison.

En février 2010, Microsoft a vu à son tour les 22 pages de son manuel de conformité légale, *The Global Criminal Compliance Handbook,* publiées sur le Net à son insu. Dans les deux cas, les opérateurs n'ont pas nié l'authenticité de ces documents. Ils se sont contentés d'invoquer une atteinte à leur propriété intellectuelle, en

violation du *Digital Millennium Copyright Act* (dmca).

IV. Les associations et les organisations non gouvernementales

Il existe au final peu de secteurs équivalents à l'internet où les acteurs associatifs jouent un si grand rôle. Même si les États y agissent également en sous-main, la gestion de l'internet inclut néanmoins une série d'entités au statut disparate qui ont toutes pour point commun d'accorder une large place au débat avec la société civile.

Trop ? Peut-être. Car, sous prétexte d'ouvrir tous les sujets à la consultation des internautes, on risque de mobiliser surtout les équipes de lobbying des grands acteurs institutionnels et, l'ouverture affichée n'étant qu'un leurre, de laisser les termes du débat bel et bien maîtrisés sur le fond par les administrations établies et les professionnels patentés. Il convient donc d'identifier ces enceintes technico-politiques et de comprendre leurs rôles respectifs. Puisque ce sont elles qui bâtissent l'internet

d'aujourd'hui et de demain. Et qu'elles sont largement ignorées du grand public.

1. L'Internet Corporation for Assigned Names and Numbers (icann [10])

Depuis 1998, année de sa création, l'icann est une structure de droit privé californien à but non lucratif. Son fonctionnement repose sur un protocole [11] signé avec le ministère états-unien du Commerce. Bien que fort discrète, cette structure dispose d'un pouvoir considérable.

D'une part, elle gère au niveau mondial les noms de domaine *(Domain Name System)*. C'est-à-dire qu'il lui revient d'octroyer aux États, aux entreprises, aux simples individus… l'adresse qui leur permettra d'exister sur la Toile. Par exemple, www.puf.com pour le site des Presses universitaires de France ou www.arpagian.net pour celui de l'auteur de ces lignes. À tout moment, l'icann peut ainsi retirer cette adresse et rendre *de facto* un site inaccessible sur le Net. D'ailleurs, en cas de contentieux, ses décisions devaient jusqu'à la fin 2009 être portées en appel devant le

ministre de la Justice *(Attorney General)* de l'État de Californie et, en dernière instance, devant le ministre du Commerce des États-Unis. Une telle hiérarchie des normes était sans équivalent dans le monde ou dans un autre domaine d'activité. Par exemple, lorsque l'icann a décidé de son propre chef de suspendre temporairement l'enregistrement de sites Internet en Irak (adresses en.iq) et en Afghanistan (adresses en.af), les gouvernements de ces deux États souverains, s'ils avaient contesté cette décision, auraient dû se soumettre à la sentence d'un ministre californien.

Ainsi, c'est bien grâce à cet organisme que les pays disposent de suffixe Internet à leur nom (.be pour la Belgique .ca pour le Canada .fr pour la France .ch pour la Suisse…). Il en va de même pour les suffixes « thématiques » comme les.info .bizz ou.org. Ce mode d'adressage permet en outre l'envoi et la réception des courriers électroniques. Dans ce contexte, l'icann prend seule des décisions qui ont un impact sur l'ensemble du globe. Par exemple, le 30 octobre 2009, son directoire de quinze membres a voté pour l'ouverture, à partir du 16 novembre suivant, en faveur de l'enregistrement de noms de domaines en arabe, chinois, coréen et japonais. Une

démarche logique quand on sait qu'environ la moitié des quelque 2 milliards d'internautes recensés dans le monde ne communiquent pas en utilisant l'alphabet latin. Même si le sujet était en discussion depuis 2000, il aura fallu attendre une décennie pour que l'icann en fasse une réalité.

D'autre part, il revient à l'icann de piloter l'infrastructure technique sur laquelle repose Internet. Soit un maillage de treize serveurs racines qui sont l'incarnation physique du réseau : dix sont disséminés en Californie et dans les alentours de Washington dc, deux se trouvent en Europe (en Suède et au Royaume-Uni) et un autre au Japon. À ce propos, on peut reprendre l'analogie[12] avec la suprématie maritime qu'exerça la Grande-Bretagne au xix e siècle. En partant du principe que celui qui contrôle les voies de communication physique détient un réel pouvoir sur les échanges économiques. Et donc politiques. Avec, ici, un effet démultiplicateur certain : les canaux électroniques permettent la circulation avec des volumes et une rapidité qui dépassent largement ce que pouvaient alors transporter les fleurons de la marine de Sa Très Gracieuse Majesté.

Régulièrement, la tutelle états-unienne sur l'icann fait donc

l'objet de polémiques. Pour l'instant, elles restent cantonnées aux cercles des militants les plus en pointe sur les questions de droits numériques et ne semblent guère passionner le grand public. Il suffit pour s'en convaincre de voir la relative passivité des États en septembre 2009, quand le contrat triennal qui lie l'icann et le gouvernement fédéral est arrivé à échéance. Même l'Europe, forte de sa puissance démographique et financière, n'a pas fait de ce sujet une réelle priorité. Seul Pékin s'est inquiété à haute voix de laisser ainsi à une seule nation le pouvoir sur les territoires cybernétiques : sur cette question de la gouvernance de l'internet, les partisans du parti unique se montrent de sérieux défenseurs du pluralisme… Au point, en tout cas, de vouloir que la Chine, et ses quelque 400 millions d'internautes, participe dorénavant au pilotage de la Toile.

Voulant se distinguer de ses prédécesseurs qui n'envisageaient nullement un relâchement de la tutelle des États-Unis, Barack Obama a montré des signes d'ouverture : l'*Affirmation of Commitments* (ou aoc) instaure – à la place de la hiérarchie directe exercée par le Department of Commerce de Washington – des comités d'audit interne dans différents domaines (la concurrence, le respect du

consommateur, la sécurité et la stabilité du réseau…) auxquels l'icann devra rendre des comptes. Toutefois, leurs membres étant largement issus de l'organisation ou sélectionnés par elle, leurs conclusions n'étant pas contraignantes et la liste des thèmes de compétence de ces groupes étant prédéfinie, on peut s'interroger sur le progrès effectif que représentent de telles annonces en termes de transparence et d'indépendance.

D'autant que le même Président Obama a encouragé la désignation, fin 2009, de son compatriote Rod Beckstrom à la présidence de l'icann. Entre autres fonctions, il a été auparavant conseilleur du directeur du renseignement des États-Unis puis responsable de la cybersécurité au sein du ministère de la Sécurité intérieure de son pays. Ou comment la gouvernance du Net est résolument abordée par le biais de la sécurité.

2. Le World Wide Web Consortium (w3c [13])

Le w3c est un organisme à but non lucratif créé en 1994 à l'initiative de Tim Berners-Lee. Cet ancien ingénieur de

l'Organisation européenne pour la recherche nucléaire (cern) l'a fondé au sein du prestigieux mit (Massachusetts Institute of Technology) en bénéficiant du soutien de la Commission européenne et de la darpa [14], l'Agence gouvernementale des États-Unis spécialisée dans la recherche technologique.

Le w3c est un organisme de standardisation destiné à assurer l'interopérabilité des différentes technologies qui cohabitent sur la Toile, telles que le html – le format de données utilisé pour mettre en forme et ordonner le contenu des pages Web – ou le xml, qui, en balisant les données, facilite leur échange sur la Toile.

Le mode de gestion du w3c est particulièrement original car il s'appuie sur une collaboration essentiellement académique. Avec des structures pivot comme le mit pour les États-Unis, l'université Keio de Tokyo et l'European Research Consortium for Informatics and Mathematics (ercim [15]) pour l'Europe. Cette entité rassemble les principaux centres de recherche informatique de l'Union européenne. La France y est représentée par les équipes de l'Institut national de recherche en informatique et en automatique (inria).

Ce w3c ne conçoit pas des programmes de certification qui auraient une valeur contraignante. Il ne produit que des recommandations qui sont transmises aux industriels. Toutefois, le principe même de la communication *via* Internet étant fondé sur la possible interconnexion des différentes technologies afin que la navigation s'effectue sans heurts, tout ce qui contribue à la fluidité technique des échanges numériques est le bienvenu.

La structure, qui emploie environ 70 permanents, est financée par des dons ou des cotisations privées.

3. L'Internet Engineering Task Force (ietf [16])

Cet ietf est sans doute l'incarnation la plus caractéristique de l'esprit du Net, puisque cette organisation n'en est précisément pas une : ici, pas de structure formalisée, ni de carte de membre ou de cotisation à acquitter. Tout est virtuel.

Chacun peut se saisir d'une thématique technique et commencer à rédiger un « appel à commentaires » ou rfc

(Request for comments). Le document doit être envoyé sur le site Internet de l'ietf et se trouve donc soumis aux critiques, avis et analyses de la communauté des internautes. Soit il laisse tout le monde indifférent et devient donc caduc, soit il suscite des réactions telles que l'ietf constituera un groupe de travail qui lui sera consacré. Au final, ces différents documents – une fois remaniés par ce travail collectif en ligne – finissent par décrire par le menu les aspects techniques d'Internet.

Le haut degré de technicité des thématiques abordées, et la nécessaire maîtrise de la langue anglaise et de son vocabulaire spécialisé, restreignent naturellement les contributions à un public de spécialistes (concepteurs de réseaux, opérateurs de télécommunications, fournisseurs de services Internet, chercheurs…). Mais cette procédure reste théoriquement ouverte à toute personne intéressée.

Néanmoins, ce mode original de production des différents protocoles sur lesquels repose le Net constitue un processus sans équivalent dans le monde normatif classique. D'autant que les contributeurs, même s'ils sont employés par une société commerciale pour participer aux travaux de l'ietf, sont toujours considérés par celle-ci

comme étant des individus isolés. En termes de lobbying, certains industriels du secteur des télécommunications y voient donc un moyen de faire passer avec une certaine discrétion leurs idées et préoccupations. Toutefois, le fait qu'une centaine de groupes de travail différents cohabitent simultanément peut sembler un peu déroutant pour des professionnels habitués à conduire des opérations d'influence plus traditionnelles telles qu'elles peuvent intervenir dans des enceintes parlementaires ou gouvernementales ayant un agenda et un ordre du jour connus, fixes et limités dans le temps. Comme le disent très clairement les conditions de participation aux sessions de cette task force : « Les contributeurs à l'ietf n'aiment guère la bureaucratie ! »

4. Internet Architecture Board (iab [17])

L'iab est l'un des comités qui compose l'ietf. Il est plus spécialement chargé des décisions qui affecteront l'architecture d'Internet à long terme. De même, en cas de discussion lors du processus de normalisation, c'est l'iab qui a autorité pour trancher la question. Fondé en

septembre 1984, cet organisme a intégré l'Internet Society (isoc, voir ci-dessous) en 1992, dont il devient le conseil technique. À ce titre, cette entité veille au bon fonctionnement de l'architecture d'Internet et participe également à la procédure d'élaboration des normes et protocoles de la Toile.

5. L'Internet Society (isoc [18])

L'Internet Society est une organisation à but non lucratif qui a vu le jour en 1992. Son ambition ? « Assurer le développement, l'évolution et l'utilisation de l'internet pour le bénéfice des individus, à travers le monde. » Plus prosaïquement, cette structure abrite les groupes techniques chargés de l'infrastructure des standards de l'Internet, tels que l'Internet Engineering Task Force (ietf) et l'Internet Architecture Board (iab). En 2010, l'isoc dispose de 85 sections (on parle de « chapitres ») et revendique quelque 28 000 adhérents dans 180 pays. Les particuliers peuvent y participer en payant une cotisation annuelle qui va de 20 à 80 euros. Les chômeurs et les étudiants sont les bienvenus avec un tarif spécial de 10 euros. Pour les entreprises, en fonction de leur chiffre

d'affaires, le tarif peut atteindre 10 000 euros l'année.

Parmi ses dogmes fondateurs, l'isoc promeut l'universalité et l'accessibilité du Net, le respect des standards ouverts, la non-discrimination du réseau et l'interopérabilité des solutions techniques. C'est en tout cas une interface entre les mondes de la technique et du droit, notamment quand le législateur se pique d'intervenir dans ces territoires numériques où l'application des lois nationales est loin d'être automatique. Enfin l'isoc participe aux travaux de l'icann.

6. L'Internet Engineering Steering Group (iesg [19])

L'iesg est un groupe de l'ietf chargé du pilotage de l'activité normative et de la rédaction de standards concernant la technologie Internet. C'est cette entité qui valide la production des différents groupes de travail et fait en sorte que les *Requests for Comments* (rfc, ou appels à commentaires) ainsi rédigés puissent être ou non endossés par l'ietf. En cas de contestation, la discussion est portée devant l'iab. Les domaines relevant de sa compétence

technique sont très étendus : qu'il s'agisse des modalités d'acheminement des paquets de données ou des conditions d'authentification et de confidentialité des transmissions. Ce qui en fait un contributeur important au débat sur la sécurité des échanges sur le réseau des réseaux.

Ce rapide tour d'horizon institutionnel donne une idée de la complexité de l'évolution d'Internet en tant que corps social. Tandis que nos économies et nos systèmes administratifs s'appuient chaque jour un peu plus davantage sur cette technologie, les règles et les organes qui régissent le Net sont largement inconnus des élites politiques et administratives ainsi que de la très grande majorité des citoyens et consommateurs. Or, laisser un tel enjeu entre les seules mains des industriels ou des techniciens ne semble pas une option réellement satisfaisante.

V. Les particuliers

Selon le baromètre 2009 de l'Association de l'économie numérique (Acsel [20] réunit les principaux acteurs du commerce électronique en France), cette activité a

enregistré un total de 250 millions de transactions (en progression de 33 % par rapport à 2008) pour 22,49 milliards d'euros, soit une hausse de 31 % par rapport à 2008. En clair, nos compatriotes dépensent de plus en plus en ligne, et le font de plus en plus souvent.

Les Français se sont pleinement appropriés l'outil Internet [21] : 68 % sont des internautes réguliers et, parmi ces derniers, 76 % se connectent tous les jours. En outre, 89 % ont déjà effectué une démarche administrative en ligne et 85 % d'entre eux ont acheté *via* le Net, tandis que 80 % consultent leurs comptes bancaires par ordinateur.

Publié en mars 2010, ce sondage national commandé notamment par la Caisse des dépôts et consignation témoigne de la banalisation de l'usage d'Internet : les particuliers, quels que soient leur niveau d'étude ou leur connaissance des arcanes de l'informatique, ont appris à jongler avec différentes identités sur la Toile.

En moyenne, les internautes français disposent de douze comptes en ligne. Ils se répartissent ainsi : deux ou trois adresses *e-mail* pour la messagerie instantanée, un ou deux profils pour la messagerie, deux pseudonymes pour les utilisateurs de forums et un compte sur quatre sites de

commerce électronique. Comme s'ils avaient perçu de manière intuitive la nécessité de changer d'identité lorsqu'ils s'exposent sur le réseau.

Car il est intéressant de constater que les Français n'appréhendent pas la sécurité sur Internet par rapport au Net en lui-même, avec ses failles technologiques qui rendent accessibles leurs données et autres patrimoines numérisés. Mais bien en fonction de leurs sites de destination. Leur confiance varie donc selon qu'il s'agit d'une administration, d'une banque ou d'un cybercommerçant. Ainsi, selon le Baromètre Acsel-Caisse des dépôts de mars 2010 réalisé auprès d'un panel représentatif d'internautes âgés de plus de quinze ans, on constate que leur intérêt à utiliser des services en ligne prime sur les risques encourus. Une attitude qui s'explique sans doute, en partie, par l'absence de culture de sécurité et par le choix stratégique fait par les banques, dès les années 2000, de faciliter autant que possible le remboursement en cas de prélèvement frauduleux sur un compte bancaire. Établie au nom du déploiement voulu du e-commerce, cette politique commerciale a probablement contribué pour sa part à diluer l'impact dans les esprits d'une cybersécurité imparfaite.

Tableau 10. – **La valeur d'usage des services en ligne l'emporte sur les risques identifiés**

	Valeur d'usage	*Taux de confiance*
Commerce en ligne	85 %	51 %
Banque en ligne	80 %	69 %
Administration en ligne	89 %	86 %

Source : Acsel-Caisse des dépôts-Idate, *Confiance des Français dans le numérique,* mars 2010.

Comme si la tradition colbertiste survivait jusque dans les réseaux numériques, l'État et ses services disposent d'un réel capital de confiance. En surfant sur un site de l'administration, seuls 11 % des Français redoutent en effet que leur identité soit utilisée abusivement ou consultée par quelqu'un d'autre. Alors que pour les banques en ligne, ils sont 24 % à craindre le piratage de leur compte ou son utilisation abusive. Chez les cybercommerçants, le score des inquiets grimpe à 43 %, notamment en ce qui concerne le piratage de leurs données bancaires. 16 % des Français ont également peur que leurs données en ligne soient

utilisées à des fins publicitaires.

Pour les Français de 2010, constitue une information sensible, qu'il convient donc de protéger : les données sur la santé (71 %), sur la vie personnelle (51 %) et l'état civil (49 %). Preuve néanmoins que les particuliers ne sont pas tout à fait au clair sur ces questions : ils sont 94 % à ne pas hésiter à communiquer leurs nom et prénom sur la Toile, ainsi que leur numéro de téléphone (82 %). Et 63 % des Français n'ont pas de scrupule à diffuser en ligne leur numéro de carte bancaire.

Enfin, les internautes accordent moins de confiance aux réseaux sociaux. Alors que les Français sont 84 % à communiquer leurs nom et prénom auprès des collectivités locales, ils ne sont que 47 % à faire de même sur les réseaux sociaux. En revanche, ceux-ci recueillent facilement des informations relatives à la vie personnelle des internautes : 38 % d'entre eux publient des données personnelles sur les réseaux sociaux contre 11 % sur les sites de vente.

Ce n'est pas là l'un des moindres paradoxes d'Internet. L'individu, selon qu'il s'exprime en tant que citoyen, consommateur ou électeur, va formuler en matière de

cybersécurité des attentes et des exigences diverses, voire contradictoires. Car il veut à la fois circuler librement mais que l'on puisse piéger les internautes indélicats ou pédophiles. Que son commerçant en ligne comptabilise sa fidélité afin de lui offrir des tarifs préférentiels tout en étant attentif à la confidentialité de ses achats. Ou qu'un moteur de recherche lui apporte les réponses à ses questions, sans pour autant avoir pondéré ses résultats par l'analyse de ses requêtes antérieures. Un peu comme la règle non écrite qui veut qu'il n'y ait jamais de policier dans la rue au moment où on en aurait besoin.

C'est donc toute la difficulté pour le politique, qui mettra en place des outils de sécurisation du Net ou d'encadrement des pratiques de compilation de données des cybermarchands et autres moteurs de recherche, que de trouver le bon équilibre entre le modèle économique des uns, la nécessité de surveillance des autres et le droit à la vie privée des utilisateurs du Net.

Notes

[1] www.darpa.mil//solicitations/09-11/index.html
[2] www.itu.intl/wsis/index-fr.html
[3] http://intgovforum.org/cms
[4] Communiqué final : www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/
[5] Deloitte, *Report on cybercrime in Canada,* Canadian Association of Police Boards, 2008.
[6] http://www.oecd.org/dataoecd/53/34/40724457.pdf
[7] www.enisa.europa.eu
[8] http://www.ccdcoe.org
[9] www.interpol.int/Public/TechnologyCrime/default.asp
[10] www.icann.org
[11] Disponible sur le site de l'Agence gouvernementale des télécommunications (ntia) : www.ntia.doc.gov/ntiahome/domainname/icann.htm
[12] Nicolas Arpagian , *La Cyberguerre*, Paris, Vuibert, 2009.
[13] www.w3.org
[14] www.darpa.mil
[15] www.ercim.eu
[16] www.ietf.org
[17] www.iab.org
[18] www.isoc.org
[19] http://www.ietf.org/iesg

[20] http://www.associationeconomienumerique.fr

[21] Source : Acsel-Caisse des dépôts-Idate, *Confiance des Français dans le numérique,* mars 2010.

Chapitre V

Des modèles d'organisation étatique disparates

I. La France

La France n'a pas attendu la bulle Internet pour se préoccuper de sa cybersécurité. En effet, le pays dispose depuis 1986 d'une Délégation interministérielle pour la sécurité des systèmes d'information. De cette époque date au contraire une fâcheuse habitude d'additionner les organismes dédiés à cette question : des Finances à l'Intérieur, en passant par la Défense ou Matignon, chaque ministère revendique alors une part de compétence. C'est finalement en 1996, le Secrétariat général de la Défense nationale (sgdn), rattaché au Premier ministre, qui est désigné pour répondre aux risques informatiques ; puis, en

juillet 2001, est créée une Direction centrale de la sécurité des systèmes d'information (dcssi) au sein dudit sgdn. Toutefois, chaque ministère reste responsable de la sécurisation de son informatique interne. Ce qui n'incite pas vraiment à la cohésion des choix technologiques ni à l'élaboration d'une culture commune en la matière.

La situation est finalement clarifiée par la parution, en juin 2008, de *Défense et Sécurité nationale, le Livre blanc* qui fixe les axes stratégiques pour les quinze années à venir et annonce la création d'une structure autonome dédiée à cette mission. L'Agence nationale de la sécurité des systèmes d'information (anssi [1]) voit le jour par un décret publié au *Journal officiel* le 8 juillet 2009.

Ses missions ?

- Détecter les attaques informatiques et permettre de réagir au plus tôt, grâce à un centre opérationnel renforcé de cyberdéfense. Actif 24 heures sur 24, il est chargé de la surveillance permanente des réseaux les plus sensibles de l'administration ;

- prévenir la menace. L'agence contribuera au développement d'une offre de produits et de

services de confiance pour les administrations et les acteurs économiques ;

- conseiller les administrations et les opérateurs d'importance vitale (centrales nucléaires…) ;

- informer régulièrement les entreprises et le grand public sur les menaces et les moyens de s'en protéger, en développant une politique de communication et de sensibilisation active.

L'anssi emploie 130 personnes et entend atteindre les 250 collaborateurs en 2012. Elle dispose en 2010 d'un budget annuel de 90 millions d'euros. Si les opérations défensives sont conduites par l'anssi, les missions offensives relèvent en principe des services de la Direction générale de la Sécurité extérieure (dgse).

Côté policier, l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (oclctic) a été créé en mai 2000 au sein de la Police judiciaire. Il est compétent pour les infractions spécifiques à la criminalité technologique ainsi que pour celles qui sont facilitées ou liées à l'utilisation de ces outils numériques. La Gendarmerie nationale dispose d'une

division de lutte contre la cybercriminalité au sein du Service technique de recherches judiciaires et de documentation (strjd). Avec notamment une compétence reconnue en matière d'analyses d'images pédopornographiques. Le ministère de l'Intérieur a ouvert un site Internet [2] destiné à recueillir les demandes d'informations et les signalements des internautes victimes d'attaques sur le Net, qu'il s'agisse d'escroquerie, de pourriels ou même d'avoir trouvé un site ayant une activité manifestement illicite (appel à la haine, pornographie enfantine…).

La France dispose d'un arsenal juridique spécialement adapté aux enjeux de la cybersécurité. Ainsi l'article 323-1 du Code pénal prévoit que « le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende. Et lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 euros d'amende ». Selon l'article 323-3 du même Code pénal, « le fait d'introduire frauduleusement des données dans un

système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende ».

On notera enfin que le législateur a prévu que la simple tentative de commettre chacun de ces actes doit être punie des mêmes peines (article 323-7 du Code pénal). L'article 23 du projet de loi d'orientation et de programmation pour la sécurité intérieure (lopsi 2) adopté par l'Assemblée nationale en février 2010 et depuis en discussion au Sénat autorise, pour les dossiers de grande criminalité, les services de police à pirater – sous l'autorité d'un juge – les ordinateurs de personnes privées à leur insu, afin de surveiller les fichiers informatiques et leurs correspondances électroniques.

L'interception des télécommunications, en dehors des cadres judiciaires ou administratifs, reste illicite. L'article L.226-15 du Code pénal établit que le fait d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, reçues ou transmises, ou d'installer des appareils dans ce but, est puni de 45 000 euros d'amende et d'un an de prison. La peine encourue grimpe à trois années s'il

s'agit d'une personne dépositaire de l'autorité publique ou d'un opérateur de télécommunications intervenant en dehors des cas prévus spécifiquement par la législation (article L.432-9 du Code pénal).

II. Les États-Unis

« Quand on me demande ce qui m'empêche de dormir la nuit. Je réponds : la cybermenace. » Cette formule en forme de boutade énoncée en janvier 2010 par William J. Lynn III, le secrétaire adjoint à la Défense des États-Unis et reprise sur le site Internet officiel de son ministère, justifie, mieux que de longs discours, l'investissement des autorités de Washington en matière de sécurité numérique.

Si le gouvernement fédéral ne distingue pas les sommes allouées précisément à cette activité, on apprend néanmoins, à la lecture des documents budgétaires [3], que le Pentagone recevra une enveloppe supplémentaire de 105 millions de dollars en 2011 par rapport à l'année précédente pour financer des actions de cybersécurité. En outre, la *Quadriennal Defense Review* [4] – sorte de feuille de route stratégique pour les quatre années à venir –,

publiée en février 2010, l'indique clairement : le cyberespace doit désormais être considéré comme un lieu d'affrontement à part entière. La menace est envisagée de manière globale : on en veut pour preuve qu'en juin 2009, le comité chargé des questions de renseignement à la Chambre des représentants a officiellement demandé dans l'*Intelligence Authorization Act for fiscal year 2010* au directeur du Renseignement national (dni) qui supervise l'ensemble de ces activités au niveau national, un état des lieux de la contamination par des services étrangers de l'ensemble des logiciels utilisés par les espions américains. Il doit remettre sa copie d'ici la fin de l'été 2010.

Toutefois, la préoccupation de Washington en matière de cybersécurité n'est pas nouvelle : le 22 mai 1998, Bill Clinton signait le décret présidentiel n° 63 qui instaurait la « protection des infrastructures de base des États-Unis », incluant d'ores et déjà les activités de télécommunications. La création d'une structure centralisée, le National Infrastructure Protection Center (nipc), pour coordonner cette protection semblait la solution idoine. En fait, ce nipc ne parvint jamais à faire réellement travailler ensemble les différentes administrations concernées (fbi, ministères de la Défense, de l'Énergie ou des Transports…). Une situation

régulièrement dénoncée par les commissions parlementaires chargées du suivi de ces thématiques de sécurité.

Ce sont les attentats du 11 septembre 2001 qui vont forcer ces administrations à collaborer davantage. La loi dite de *Homeland Security* (Sécurité intérieure) du 25 novembre 2002 donne naissance au ministère du même nom. Les années qui suivent s'illustrent surtout par la création successive d'une myriade d'organismes et de programmes spécialisés : la National Cyber Investigative Joint Task Force, le National Cyber Security Center, le programme *Cyber Initiative*… À chaque fois, l'objectif affiché est de sécuriser le cybermonde. Dans les faits, on assiste à un doublonnement des activités et à la création d'une technostructure particulièrement confuse.

Dans le même temps, un serpent de mer fait régulièrement surface : l'établissement d'un état-major spécialement dédié à la défense numérique, le *Cybercommand.* Annoncé en juin 2007, ce commandement devait être basé en Louisiane et fédérer tous les services de l'us Army concernés par la cybersécurité. Mais des luttes intestines entre les différentes armes, dont certaines telle l'Air Force

avaient déjà déployé des équipes conséquentes sur le sujet, ont conduit au report régulier du projet. Il est réapparu au printemps 2010 et devrait être confié au général Keith B. Alexander, actuellement directeur de la National Security Agency (nsa), les « grandes oreilles » des États-Unis. Sa mission ? Être le bras armé du Président pour conduire des attaques *via* les réseaux informatiques, pirater les systèmes d'information ennemis.

Les États-Unis organisent régulièrement des opérations de simulation d'attaques cybernétiques à grande échelle. La première édition de ce *Cyberstorm* a eu lieu en février 2006 et la deuxième en mars 2008. En associant plusieurs dizaines d'entreprises partenaires (Cisco Systems, Microsoft, McAfee, Dow Chemicals ou abb Group) ainsi que des gouvernements étrangers (Canada, Nouvelle-Zélande, Royaume-Uni…), ils cherchent à éprouver la robustesse de leurs équipements informatiques. Le programme des opérations et, *a posteriori,* certains enseignements sont d'ailleurs officiellement présentés sur le site Internet [5] du ministère de la Sécurité intérieure, lequel en fait fort opportunément un exercice de communication destiné à rassurer la population, sans pour autant dévoiler le bilan complet de ces entraînements.

L'administration ne mise pas uniquement sur ses propres ressources. Elle publie régulièrement sur les forums de *hackers* des petites annonces de recrutement explicites. Par exemple au printemps 2009, le ministère de la Sécurité intérieure (Department of Homeland Security) a ouvert un poste de *Senior Ethical Hacker* qui disposerait d'une accréditation *Top Secret/Secure Compartmented Information.* Condition requise pour décrocher cet emploi ? Le candidat devra être en mesure de « penser comme un criminel ». Le Pentagone fait également partie des recruteurs de ces profils atypiques.

Grand consommateur à titre personnel d'outils informatiques, le Président Obama a sollicité, dans les premiers jours de son mandat, la réalisation d'un audit de la cybersécurité de son pays. Il a nommé à ses côtés, en décembre 2009, un coordonnateur gouvernemental pour la cybersécurité. Le premier titulaire du poste, Howard Schmidt, était déjà en charge de ces questions au sein de l'équipe de George W. Bush. Passé par le fbi, il a également une expérience du secteur privé – notamment chez Microsoft. Un parcours qui correspond au caractère transversal des enjeux de l'internet.

Autre grande première : la décision[6] de la Maison Blanche, en mars 2010, de lever le secret Défense sur certaines parties de son programme de cybersécurité, le cnci *(Comprehensive National Cybersecurity Initiative).* Celui-ci est expliqué en douze points, de la présentation des programmes *Einstein* qui servent à protéger les ordinateurs fédéraux contre des intrusions informatiques à la mise en place d'une stratégie de « contre-renseignement » pour identifier les cyberattaques qui viseraient les administrations et les entreprises états-uniennes. Largement présentée comme une démarche de transparence, cette mise en avant de la politique de cybersécurité est également un bon moyen de justifier aux yeux de l'opinion publique le bien-fondé d'une surveillance accrue de la Toile. Puisque la description ainsi faite est délibérément elliptique et ne révèle, *in fine,* aucun secret réellement stratégique. C'est en revanche l'occasion de réaffirmer un leitmotiv de Barack Obama : « La prospérité de l'Amérique passera par la cybersécurité. »

Principale étape annoncée en 2010 : la mise en conformité progressive de l'ensemble du parc informatique des administrations fédérales et des systèmes de communications stratégiques aux standards de sécurité

édictés par le *Federal Information Security Management Act* [7]. Un cahier des charges technique qui n'était donc pas réellement appliqué depuis sa publication en… 2003 ! Un retard d'autant moins compréhensible que les États-Unis sont l'un des rares pays à détenir un « baromètre » de la cyberinsécurité. En effet, chaque année l'Internet Complaint Center [8] (ic3) publie en collaboration avec le fbi les statistiques des plaintes déposées et relatives à des fraudes sur le Net. S'il ne s'agit certainement pas d'une photographie exhaustive de la situation, c'est en tout cas un indicateur très instructif pour suivre l'évolution des cyberattaques visant des particuliers ou des entreprises. Sachant que ne sont évidemment pas prises en compte les intrusions dont les victimes n'ont pas conscience, ni les cas où celles-ci ne veulent pas porter plainte. De peur de ternir leur image de marque.

Tableau 11. – **Plaintes déposées aux États-Unis relatives à des fraudes sur le Nets**

	Nombre de plaintes déposées	*Pertes en millions de dollars*
2009	336 655	559,7

2008 275 284	265
2007 206 884	239,09
2006 207 492	198,44
2005 231 493	183,12

Source : Rapport ic3, mars 2010 ; www.ic3.gov

III. La Chine

« Capacité de la République populaire de Chine à mener des cyberattaques » : c'est le titre fort explicite d'un rapport de 88 pages publié en octobre 2009 par la Commission [9] états-unienne d'étude économique et de sécurité sur la Chine (usa-China Economic and Security Review Commission) et destiné aux présidents du Congrès. Il explique comment des groupes de *hackers* chinois – par exemple Hack4.com à qui l'on impute les principales cyberattaques menées en décembre 2008 contre les représentations diplomatiques françaises en Chine et dans différents pays anglophones, travaillent en étroite collaboration avec le *Guoanbu,* la sécurité d'État chinoise. Et d'indiquer comment ce service recrute des pirates sur les forums spécialisés : en les arrêtant et les «

convainquant » de travailler au profit des services gouvernementaux.

Cette surveillance des réseaux Internet domestiques est effectuée par la Sécurité publique *(Gonganbu)*. Au sein de l'armée populaire de Chine (apl), les militaires du 3e Département sont plus spécialement chargés des interceptions cybernétiques. Issus des cursus des différentes académies militaires du pays, ils ont intégré depuis plusieurs années les technologies numériques dans la panoplie des armes offensives. L'Information Engineering University (ieu) de Zhengzhou, placée sous l'autorité du 2e Département de l'apl, chargée du renseignement militaire, dispose d'un centre de recherche qui conçoit une partie des logiciels de cyberguerre utilisés par l'armée nationale. En février 2010, la nsa, l'agence gouvernementale des États-Unis chargée de la collecte et l'analyse des communications, a annoncé que les tentatives répétées d'infiltration dont Google avait été victime un mois plus tôt remontaient jusqu'aux serveurs de la Shanghai Jiaotong University dont dépend l'ieu.

La Chine se caractérise en outre par une très forte imbrication public-privé. Par exemple, l'équipementier

télécoms Huawei (environ 15 milliards de dollars de chiffre d'affaires et plus de 60 000 d'employés) a été fondé en 1988 par un ancien officier de l'apl, Ren Zhengfei. Et compte de nombreux anciens des services de sécurité chinois au sein de ses équipes de direction. Au point qu'au début de l'année 2009, Huawei a été désigné par les experts britanniques du Government Communications Headquarters comme une menace pour la sécurité informatique du Royaume-Uni : depuis 2005, en effet, l'industriel chinois mène un vaste programme de modernisation du réseau Internet de British Telecom.

C'est sans doute le même raisonnement qui a conduit en février 2010 des responsables de services de sécurité français à s'inquiéter de la propension de leurs homologues chinois à récupérer des données de connexion à Internet, voire à mettre en place des dispositifs de filtrage de l'accès au Net, par le biais des clés 3g. Les modèles commercialisés en France sont pour l'essentiel fabriqués par Huawei, zte ou leur compatriote China Unicom – trois groupes très liés à la sphère de la sécurité d'État.

Le pays détient une véritable expérience en matière de surveillance de l'information sur la Toile. D'une part, parce

que l'internet chinois a été réparti entre deux sociétés : China Netcom au Nord et China Telecom au Sud. Ce qui facilite les contrôles. D'autre part, le programme de filtrage dit du « Bouclier d'or » *(Jindun)* fonctionne depuis 2000. Il permet aux autorités de bloquer des sites et des messageries électroniques jugés indésirables. Il agit principalement sur la base d'un dictionnaire, modulable à l'envi, de termes suspects. S'ils sont employés sur un site ou dans un message électronique, cela déclenche l'identification et la surveillance des personnes concernées. Un mode opératoire qui devra traiter à l'avenir des volumes toujours plus considérables de données puisque la Chine compte désormais quelque 400 millions d'internautes.

IV. L'Allemagne

Dix années de prison : telle est, selon le Code pénal allemand, la peine encourue pour des actions de sabotage informatique. Depuis qu'en 2006, les services de la Chancellerie et différents ministères ont fait l'objet de tentatives répétées de vols de données sensibles par le biais d'attaques cybernétiques, Berlin s'est doté, le 20 août

2009, d'une loi destinée à « renforcer la sécurité de l'information du gouvernement » afin de consolider les moyens et effectifs du Bundesamt für Sicherheit in der Informationstechnik (bsi)[10]. Créé en 1991, cet Office fédéral de la sécurité des technologies de l'information emploie d'ores et déjà près de 500 personnes avec un budget annuel d'une soixantaine de millions d'euros.

Le bsi a en outre l'originalité d'assurer ses propres travaux de R&D auxquels il consacre chaque année plus de 20 millions d'euros. Il est alors en mesure d'équiper les administrations fédérales avec des solutions technologiques dont il a défini le contenu, ou en tout cas suivi étroitement l'élaboration par des prestataires privés. Le bsi surveille ainsi en continu les flux de données qui partent et arrivent des ordinateurs de l'administration fédérale, de manière à intervenir dès que des sollicitations suspectes surviennent : virus, attaques massives en déni de service… Avec le pouvoir, le cas échéant, de réduire l'accès des ordinateurs gouvernementaux au réseau Internet.

En revanche, en ce qui concerne le reste des internautes, la coalition chrétienne-démocrate/libérale (cdu-fdp) sortie des urnes en septembre 2009 a renoncé à procéder au filtrage *a*

priori du Net. Pour lui préférer, notamment dans les affaires de pédopornographie, le retrait *a posteriori* des images ou films illicites. C'est-à-dire une fois qu'ils ont été mis en ligne.

Depuis une loi votée par le Bundestag en mai 2007, le fait d'obtenir des informations sécurisées en contournant ou désactivant des mesures de protection constitue un délit. Il en va de même pour la création, la vente, la distribution ou l'acquisition de solutions informatiques permettant de capter des données protégées. Le Bundesnachrichtendienst (bnd, le service de renseignements allemand) a cependant été fortement mis en cause au printemps 2009 quand l'hebdomadaire *Der Spiegel* [11] a révélé que ses équipes se seraient introduites dans plus de 2 500 ordinateurs, essentiellement situés hors de la République fédérale. En l'espèce, les agents de Berlin auraient infecté à distance les ordinateurs par l'envoi de *chevaux de Troie* – ces programmes espions dissimulés dans des messages anodins – pour ensuite recevoir directement l'ensemble des textes rédigés avec les claviers des machines ainsi ciblées. Un an auparavant, le bnd avait été soupçonné d'avoir intercepté des courriers électroniques entre le ministre afghan du Commerce et un journaliste du même *Spiegel*.

Lors du 12e Conseil des ministres franco-allemand qui s'est tenu le 5 février 2010, Nicolas Sarkozy et la Chancelière Angela Merkel ont décidé d'une collaboration étroite de leurs deux pays en matière de cybersécurité. Notamment en ce qui concerne la défense de positions communes sur le sujet dans les enceintes internationales et le partage d'informations en matière de cyberattaques.

La Bundeswehr, à l'initiative du ministre de la Défense d'alors, Franz-Josef Jung, a ouvert en 2006 une unité dédiée au cybermonde. Composée de 80 soldats diplômés en informatique, cette entité est opérationnelle depuis 2010. Elle devrait, à l'avenir, participer à des opérations offensives.

V. La Grande-Bretagne

Le Royaume-Uni n'échappe pas au bouillonnement institutionnel qui entoure les questions de cybersécurité. Avec même une certaine frénésie de ses gouvernements successifs à multiplier les entités spécialisées. Ainsi, en 2007, Tony Blair a-t-il créé le Center for the Protection of National Infrastructure (cpni [12]). Il lui revient de

surveiller les infrastructures critiques du pays : les réseaux d'alimentation en eau, électricité, télécommunications… La protection de l'informatique gouvernementale contre des cyberattaques est, quant à elle, confiée au Communications and Electronic Security Group (cesg [13]). Il a la particularité d'effectuer et de publier une enquête de satisfaction annuelle de ses « clients ». Une approche consumériste inhabituelle dans cet univers de la sécurité. Héritier du service de cryptographie datant du début du xx e siècle, le Government Communications Headquarter (gchq [14]) est chargé, depuis 1946, des activités de renseignement électronique. Victime ou presque de sa discrétion, il peine désormais à recruter de jeunes informaticiens qui sont davantage attirés par les carrières dans des groupes commerciaux.

Pour clarifier sa stratégie et son action en matière de cybersécurité, le Premier ministre Gordon Brown a souhaité rationaliser, en septembre 2009, les organisations chargées de ces dossiers. Le nouveau dispositif[15] est opérationnel depuis mars 2010. Il comporte d'une part un Cyber Security Operations Centre (csoc [16]) dédié à la surveillance du trafic Internet. Il a pour fonction de repérer les menaces (identification des virus et des campagnes

d'attaques massives par le biais d'ordinateurs contaminés contrôlés à distance, vols de grande ampleur d'informations sensibles…) et de coordonner les réponses techniques. Il lui revient en outre de contacter les entreprises et les responsables politiques afin de les associer à cette démarche de cybersécurité – soit, également, une mission de pédagogie. La lecture du rapport [17] annuel 2009-2010 du comité parlementaire chargé du suivi des questions de renseignement (Intelligence &Security Committee) nous apprend que le csoc employait 18 personnes en mars 2010. Et d'autre part, un Office for Cyber Security placé auprès du Premier ministre, qui a vocation à harmoniser les politiques gouvernementales en matière de cybersécurité et à entretenir des échanges sur ces questions avec les gouvernements et agences étrangers.

Autant d'efforts de cohésion qui ne portent pas encore tous leurs fruits. À l'instar du contentieux qui oppose depuis le début de l'année 2010 le gchq et le tandem des services de renseignements intérieur (mi 5) et extérieur du royaume (mi 6). Ces derniers souhaitent bâtir un centre de conservation de données informatiques en dehors de Londres afin de préserver leurs informations en cas

d'attaques sur la capitale. Ils ne parviennent notamment pas à trouver de consensus sur la capacité de stockage dudit centre… et sur son financement.

VI. L'Inde

L'Inde représente environ 40 % du marché mondial de la sous-traitance informatique. Ses universités produisent des bataillons d'ingénieurs qui rejoignent les sociétés de service comme Wipro Technologies ou Infosys, lesquelles font partie des leaders mondiaux du secteur.

Dès 2003, les services de renseignements indiens (raw, Research &Analysis Wing) ont mis sur pied une agence chargée de la cybersécurité : la ntro. Cette National Technical Research Organization est chargée, entre autres, de la sécurisation des systèmes d'information, des travaux de cryptologie et de l'élaboration de logiciels stratégiques pour la sécurité nationale. Elle exerce une tutelle sur le Centre de protection des infrastructures liées aux technologies de l'information (National Information Infrastructure Protection Center) et sur l'Institut national de recherche cryptologique (National Institute of

Cryptology Research), ainsi que sur les dispositifs de secours censés prendre le relais en cas de défaillance du réseau informatique principal (Disaster Recovery Centre). Sur le papier, les principaux domaines de la cybersécurité semblent, *a priori,* bien couverts. Toutefois, ces entités font régulièrement la une de l'actualité ces dernières années pour des affaires de corruption, de trafic d'influence, voire de mise en cause de la pertinence de leur travail. Tandis que des conflits récurrents entre les services de sécurité empêchent un véritable partage d'informations entre ces différentes entités administratives.

Forte de son savoir-faire ès logiciels, l'Inde a créé en 2007 un Cyber Forensics Laboratory [18] au sein de son ministère de l'Information et de la Communication, afin de doter le pays de solutions de sécurité informatique *ad hoc.* Il collabore notamment avec les services de la police technique et scientifique, le Forensics Science Laboratories [19].

Notes

[1] www.ssi.gouv.fr
[2] https://www.internet-signalement.gouv.fr/
[3] Disponibles sur le site du ministère de la Défense : http://comptroller.defense.gov/defbudget/fy2011/FY2011_E
[4] Téléchargeable en libre accès sur http://www.defense.gov//
[5] www.dhs.gov/xprepresp/training/gc_1204738275985.shtm
[6] www.whitehouse.gov/blog/2010/03/02/transparent-cybersecurity
[7] http://csrc.nist.gov/groups/sma/fisma/index.html
[8] www.ic3.gov
[9] Téléchargeable sur www.uscc.gov
[10] Son site Internet : http://www.bsi.bund.de/
[11] Holger Starck, « bnd infiltrierte tausende computer im Ausland », *Der Spiegel,* 7 mars 2009.
[12] www.cpni.gov.uk
[13] www.cesg.gov.uk
[14] www.gchq.gov.uk
[15] www.cabinetoffice.gov.uk/reports/cyber_security.aspx
[16] www.gchq.gov.uk/press/csoc_newsitem.html
[17] www.cabinetoffice.gov.uk/media/348175/isc-annualreport0910.pdf

[18] www.cyberforensics.in
[19] www.maharashtra.gov.in/english/homedept/forensicShow.pl

Conclusion

Face à la diffusion croissante des technologies de l'information dans notre vie quotidienne, l'omniprésence des systèmes informatiques semble inéluctable. La dépendance grandissante de pans entiers de notre existence (données médicales ou bancaires), de nos modes de production (informatique d'entreprise ou équipements industriels) et de notre Défense (numérisation de l'espace de bataille et des systèmes d'armes) à leur égard fait de la cybersécurité une nécessité vitale pour nos collectivités modernes.

En permettant à chaque individu d'accéder au réseau des réseaux, les occasions de le fragiliser sont multiples. Puisque la sécurisation de l'intégralité du maillage informatique passe par la responsabilisation de l'ensemble de ses utilisateurs, il convient de diffuser une culture de la cybersécurité auprès de l'opinion publique. Non pas pour transformer chaque citoyen en informaticien, mais bien pour en faire un consommateur de technologies

responsable, conscient de l'ampleur de la menace potentielle et de la valeur de l'information, dans un monde où les données circulent à la vitesse de la lumière. Car cette sécurité-là ne doit pas être l'apanage des seuls militaires ou des policiers. Elle doit au contraire être partagée entre le plus grand nombre. C'est en sachant ce que l'on risque de perdre sur la Toile que l'on peut entreprendre une démarche de sécurisation de nos données sensibles. Et commencer à s'interroger sur le juste équilibre entre une politique de surveillance très aboutie, et un droit à l'intégrité de son patrimoine numérique.

Cette cybersécurité n'existera donc que si elle est précédée d'une réflexion approfondie permettant de désigner ce qui constitue pour chacun une information stratégique que l'on souhaite protéger. Sachant que cette protection se fera vraisemblablement au détriment de l'intégrité totale de notre vie privée. Ce n'est qu'ensuite que viendra le temps de la quête technique – au résultat forcément précaire puisque chaque innovation technologique est guettée par l'obsolescence – pour répondre à ce besoin de sécurisation.

Afin de pallier les effets d'une fragilisation de nos sociétés modernes par le biais des cyberattaques, il convient donc

de faire de la sécurisation de nos systèmes d'information un enjeu sociétal à part entière.

Bibliographie

Arpagian N. , *L'État, la Peur et le Citoyen*, Paris, Vuibert, 2010.

– , *La Cyberguerre*, Paris, Vuibert, 2009.

Arpagian N. et Delbecque E. , *Pour une stratégie globale de sécurité nationale*, Paris, Dalloz, 2008.

Arpagian N. , *Liberté, Égalité... Sécurité*, Paris, Dalloz, 2007.

Arquilla J. Ronfeldt , *Networks &Netwars*, Rand Corporation, 2001.

Brzezinski Z. , *La Révolution technétronique*, Paris, Calmann-Lévy, 1971.

Couffignal L. , *La Cybernétique*, Paris, puf, 1963.

Défense et Sécurité nationale, le Livre blanc, Paris, Odile Jacob-LaDocumentation française, 2008.

Delbecque E. , *La Métamorphose du pouvoir*, Paris, Vuibert, 2009.

Feral-Schuhl C. , *Cyberdroit*, Paris, Dalloz, 2008.

Guisnel J. , *La Guerre dans le cyberespace*, Paris, La Découverte, 1999.

Huyghe F.-B. , *L'Ennemi à l'ère numérique*, Paris, puf, 2001.
Liang Q. et Xiangsui W. , *La Guerre hors limites*, Paris, Payot &Rivages, 2003.
Libicki M. , *Cyberdeterrence and Cyberwar*, Rand Corporation, 2009.
– , *Conquest in Cyberspace: National Security and Information Warfare*, Cambridge, Cambridge University Press, 2007.
Rid T. et Hecker M. , *War 2.0, Irregular Warfare in the Information Age*, Westport-Londres, Praeger Security International, 2009.