MYTHES ET LEGENDES DES TIC

28 mars 2011

Collection ATENA

Une réalisation de Forum ATENA avec la collaboration de *(par ordre alphabétique)* **:**

Christian Aghroum, Jean-Pierre Archambault, Luc Baranger, Jacques Baudron, Eric Bourre, Jean-Pierre Cabanel, Ladji Diakité, Michel Elie, Jean Christophe Elineau, Franck Franchin, Laura Garcia, Jean-Denis Garo, Gérard Gaudin, Thierry Gaudin, Jean-Marc Grémy, Jean-Yves Gresser, David Grout, Daniel Guinier, Daniel Hagimont, Bruno Hamon, Mauro Israël, Dominique Lacroix, Michel Lanaspèze, Sophie de Lastours, François Letellier, Fabrice Mattatia, Jean Papadopoulo, Jean-Claude Patin, Gérard Peliks, Guy Perrot, Sadry Porlon, Philippe Poux, Bruno Rasle, Yvon Rastteter, Christophe Rembert, Grégoire Ribordy, Nicolas Ruff, Yanis Taieb, Philippe Vacheyrout

Livre collectif sous la direction de Gérard Peliks

Les ajouts depuis la version du 1er mars apparaissent en bleu

INTRODUCTION

Ce livre collectif de forum ATENA propose une approche originale pour expliquer différentes facettes des **T**echnologies de l'**I**nformation et de la **C**ommunication (**TIC**).

En soulignant les croyances largement partagées mais fausses, ce livre s'adresse à tous les utilisateurs des **TIC** qui désirent acquérir des connaissances et dominer les problèmes posés par l'Information, les systèmes d'information et les réseaux connectés à Internet. Ce livre apporte des réponses à leurs interrogations, leurs doutes, rétablit la vérité et donne des conseils pratiques basés sur nos expériences du terrain. Il aborde non seulement les aspects techniques mais aussi les aspects juridiques, humains, organisationnels et métiers qui se posent à tous.

Pour aller plus loin dans la connaissance des TIC, des références à des livres écrits par les auteurs de celui-ci sont conseillés en fin d'ouvrage.

Le fichier PDF de la version la plus récente du livre est en téléchargement libre à partir du Web de Forum ATENA en www.forumatena.org/?q=node/12, rubrique "Mythes et légendes des TIC", en laissant votre adresse e-mail.

Gérard Peliks
Président de l'atelier sécurité de Forum ATENA
Coordinateur de cet ouvrage

SOMMAIRE

L'ETHIQUE

FAUT-IL DEMYSTIFIER L'INTERNET ?

Michel Elie

L'objectif poursuivi dans cet ouvrage est clairement exposé dans son introduction : il s'agit de souligner « les croyances largement partagées mais fausses » à propos de l'internet. L'objectif n'est pas seulement de décrire des mythes et légendes qui se sont développées à son propos et de s'interroger sur leur persistance, mais aussi de les combattre : en un mot, il s'agit d'une entreprise de démystification. Cette recherche de vérité rationnelle peut-elle aller à son terme alors que chacun reconnaît dans l'internet et dans ses propres usages une part d'imaginaire, de rêve ? Ne faut-il pas conserver une part au doute, au flou, à l'incertain ?

Bien sûr, prétendront les rationalistes, l'internet n'est qu'un dispositif technique dont l'universalité fait la force. Tout y est raisonnable et explicable. Tous les points soulevés dans cet ouvrage ne se rattachent d'ailleurs pas à la catégorie des mythes ou à celle des légendes. Certains ne sont que correctifs techniques, surgeons de caractéristiques dépassées, voire une forme de règlement de comptes.

Peut être les mythes décrits dans ce livre sont-ils inventés, peut-être est il licite et utile de les expliquer, de débusquer au passage petits et grands mensonges, petites et grandes illusions, petites et grandes incertitudes, s'il s'agit d'erreurs, ou de les combattre s'il s'agit de mensonges. Leur existence et leur diffusion n'en a pas moins un sens allégorique, une réalité imaginaire mais significative. Le monde virtuel de l'internet est un espace particulièrement favorable au développement de mythes, de légendes, en plus des rumeurs, mensonges, qui l'alimentent à jet continu. Selon Wikipedia, « un mythe est un récit qui se veut explicatif et fondateur d'une pratique sociale. Il est porté à l'origine par une tradition orale, qui propose une explication pour certains aspects fondamentaux du monde et de la société qui a forgé ou qui véhicule ces mythes » La Toile, gigantesque écheveau de liens ne confine-t-elle pas à la religion, celle qui relie ? Le mythe est plus tenace que la rumeur : il franchit les siècles et a trait aux racines profondes de l'homme.

L'internet propose à l'humanité un miroir déformant. Celle-ci l'alimente en problèmes philosophiques : la mémoire et l'oubli, la liberté et la censure, l'identité et l'anonymat. C'est aussi un outil à faire tomber des murs qui structuraient les organisations humaines, les langues, les frontières, les préjugés… Il modifie donc le monde réel tout en créant un monde virtuel propice au développement d'utopies, de mythes et de légendes. Et parfois, comme nous l'expérimentons avec force dans les bouleversements actuels des pays arabes, il contribue à l'incarnation dans le réel de situations rêvées. Cette part d'imaginaire ne constitue-t-elle pas d'ailleurs l'un des moteurs du succès de l'internet, largement exploitée par certaines applications commerciales ?. L'Internet n'est-il pas aussi une machine à faire rêver ? Par la couverture physique de la terre entière et l'ouverture sur un autre monde, le monde virtuel, l'internet constitue un terreau fertile à la prolifération de mythes, légendes, rumeurs : attachons-nous à ce qui de prime abord y évoque des mythes fondateurs de notre civilisation, puisque l'internet en est un produit, tout en se voulant mondial et comme me le disait à la fin des années 90 un administrateur de l'ISOC « une offrande des Etats Unis d'Amérique à l'humanité ». Quels liens entre les mythes et légendes de ce recueil, et ceux de l'antiquité grecque ?

Comme dans tous les champs de l'humain, le monde de l'internet est un terrain de lutte entre le bien et le mal. Contrairement au Cosmos ou à la Genèse, la création de l'internet est un événement historique et documenté. Ce qui n'empêche pas de discuter de l'identité de son ou de ses créateurs, de ses inspirateurs, du rôle dans son développement de multiples contributeurs anonymes, souvent bénévoles, (tant de gens auraient-ils consacré autant de leur temps libre à nourrir l'internet de leurs connaissances et de leur expérience s'il n'était pas un grand véhicule d'utopies ?) et de celui de l'évolution concomitante des techniques et de la libéralisation de la société.

Pour certains détracteurs de l'internet, ce ne serait qu'une vaste poubelle d'où ne jailliraient que l'erreur et la confusion, comme du Chaos antique ne pouvait naître que Frèbe, les ténèbres, et Nyx, la nuit. C'est néanmoins du Chaos qu'est né le Cosmos, dans une construction fragile et sujette à bien des dangers.

Sisyphe pour avoir défié Zeus s'était vu condamné à remonter éternellement sur une montagne une roche qui, dès le sommet atteint, roule jusqu'en bas. L'internaute, lui n'est-il pas condamné à combattre sans fin des virus perpétuellement renouvelés par des humains malfaisants et qui tel le phénix, renaissent constamment de leurs cendres ?

L'internaute ne se contemple-t-il pas à travers l'éclat de son site personnel ou de son blog, jusqu'à parfois s'y perdre comme Narcisse qui s'abreuvant à une source, voit son reflet dans l'eau, en tombe amoureux et meurt de désespoir à ne pouvoir rattraper sa propre image ?

Ceux qui cherchent à contrôler l'internet ne se heurtent-ils pas à des adversaires qui ressurgissent dès qu'ils ont réussi à juguler l'une de leurs multiples identités, tels l'hydre de Lerne dont les têtes repoussent à peine coupées ?

Il n'est pas étonnant que le monde virtuel engendre comme le monde réel, ses propres mythes et légendes, bâtis sur « l'imaginaire de l'internet », les peurs ou les espoirs qu'il suscite, donnant naissance à une théogonie du virtuel.

Comme le ciel du monde réel au temps des grecs, le ciel du monde virtuel, qui se construit sous nos yeux, se peuple de dieux, demi dieux, héros, gourous et autres papes. Chaque jour peuple notre monde virtuel de nouveaux héros qui entraînent notre monde réel dans de nouvelles aventures : certains sulfureux comme Julian Assange avec Wikileaks ou affairistes comme Mark Zuckerberg, créateur de facebook et l'un des hommes les plus riches au monde, qui construit sa fortune en même temps que sa légende ; d'autres angéliques et bienfaiteurs comme les blogueurs Han Han en Chine ou Abdel Kareem Nabil en Egypte qui parviennent à déstabiliser des régimes, à qui le monde réel destine sa reconnaissance et qu'il couronne ou couronnera de prix nobel de la paix. Entre eux et avec le peuple des internautes, se construisent autant de mythes, se bâtissent des légendes et se développe une sagesse à rapprocher de la sagesse populaire où l'internaute pourrait puiser, par exemple dans ce sage proverbe nordique sur la protection de la vie privée: « Confie tes pensées à un seul, mais méfie toi de deux. Ce qui est su de trois est connu de tous »…

LA "SOCIETE DE L'INFORMATION", UN MYTHE ?

Thierry Gaudin, Ingénieur général des mines (honoraire)

L'expression « société de l'information » est utilisée habituellement pour faire comprendre et accepter que le traitement d'information est devenu la nouvelle manière de vivre ensemble. S'y ajoute une connotation implicite selon laquelle ce serait un progrès. Or, le mot progrès, qui avait autrefois un sens plutôt neutre de progression, a été connoté positivement, sans doute comme encouragement à accepter l'inévitable. La transition de la société industrielle vers la société de l'information a acquis l'image d'un puissant mouvement de l'Histoire qu'il vaut mieux accompagner et même, si possible, devancer.

S'il est exact que plus de la moitié des emplois sont maintenant tertiaires, il n'en reste pas moins que la nourriture, les vêtements, les bâtiments, les équipements des familles et des entreprises sont des choses bien concrètes produites par l'agriculture et l'industrie. Une bonne partie de ces productions ont d'ailleurs été délocalisées dans des pays à bas salaires.

Est-ce que les services rendus par les emplois tertiaires de la « société de l'information » aux producteurs constituent une contrepartie équitable et durable ? Il est assez vraisemblable que la réponse est non. La profusion d'information mène à la saturation cognitive alors que les producteurs de biens concrets sont sous rémunérés et marginalisés. Dès lors, comment se fait-il que cette « tertiarisation » de l'économie se poursuive et s'amplifie ?

La réponse à cette question n'est pas facile à accepter. Elle ne se trouve pas dans la presse ni dans les médias ni dans les cours d'économie. La voici : au Moyen Âge, pour traverser un pont, il fallait acquitter un péage. Aujourd'hui, c'est pour écouter de la musique, visionner des vidéos et même pour accéder aux informations d'utilité publique telles que le texte des normes ou le contenu des manuels scolaires qu'il faut payer des péages.

En outre, la société a multiplié les formalités. Chacune a, bien entendu, ses justifications. Et, globalement, on ne peut qu'admirer l'ingéniosité qui permet de rémunérer même ceux qui entravent ou ralentissent les activités productrices, à croire qu'elles seraient devenues si performantes que la population serait bien en peine de consommer tout ce qu'elles pourraient produire.

En prenant un peu de recul, il apparaît que le fonctionnement de l'économie a permis la prolifération des intermédiaires. Par exemple, l'enquête menée il y a quelques années par le Wüppertal Institute a évalué que le yaourt aux fraises faisait un trajet de plusieurs milliers de kilomètres avant d'arriver sur la table du consommateur, consommant au passage un bon quota de carbone.

Sans doute l'espoir d'une désintermédiation par Internet a-t-il commencé à se concrétiser dans la vente aux enchères ou les banques, par exemple. Et le projet de développer le travail à distance évoque déjà, malgré la timidité de ses initiatives, la possibilité d'aller vivre à la campagne tout en exerçant un métier urbain. En se rapprochant du pis de la vache et du potager, on peut alors rêver de faire son yaourt soi-même, désintermédiation alimentaire, reconquête de l'autonomie dans un monde presque totalement hétéronome, comme disait Ivan Illich.

Néanmoins, la transition vers le web 2.0 s'est accompagnée de nouvelles intermédiations : les réseaux sociaux, les plateformes vidéo, les magasins en ligne et les moteurs de recherche

émaillés d'irruptions publicitaires. Les lois de l'économie sont comme celles de la nature : quand une nouvelle niche écologique s'ouvre, il se trouve vite un animal pour s'y fourrer.

D'autre part, avec trois heures de médiatisation par jour, la saturation neuronale se fait sentir. En témoigne cette enquête menée dans le Bade Wurtemberg et publiée dans le journal Die Welt. La première ligne montre des dessins d'enfants qui passent moins d'une heure par jour devant la télé, la seconde d'enfants de même âge et même origine sociale qui y passent plus de trois heures par jour.

Pour compléter, j'ajouterai que les neurophysiologistes (voir *Les Neurones de la lecture* de Stanislas Dehaene) ont mesuré assez précisément le temps que met un cerveau à reconnaître une personne ou un objet connu : entre 100 et 300 millisecondes. Ce qui donne un ordre de grandeur : si le microprocesseur travaille en nanosecondes, il va cent millions de fois plus vite que les neurones.

Est-ce à dire que la micro-électronique, Internet et la communication ATAWAD (*Any Time, Any Where, Any Device*, selon l'expression de Xavier Dalloz) va rendre cent millions de fois plus de services à l'usager ? Non, bien entendu. Un tel ordre de grandeur induit un changement qualitatif. Il donne un pouvoir nouveau et peut-être démesuré aux producteurs et diffuseurs d'informations, lesquels s'emploient évidemment à programmer le psychisme du public dans le sens de leurs intérêts. C'est pourquoi on pourrait plaider que l'expression « société de l'information » n'est qu'un leurre dissimulant une autre réalité, la « société de désinformation ».

Néanmoins, une fois ce diagnostic critique énoncé, il convient de le dépasser. Wikileaks n'est pas le seul exemple de réaction, portée par Internet, contre les excès de pouvoir, qu'ils soient politiques ou commerciaux. Il se dessine donc une nouvelle sorte de conflit, mondial, dans le registre de la persuasion, dont Internet est le champ de bataille. On peut déjà anticiper que l'affrontement sera long et peut-être même dévastateur. Aujourd'hui, environ le tiers de la population mondiale est internaute. Dans quinze ans, ce seront plus des deux tiers, donc le grand public de tous les pays. L'affrontement sera planétaire.

Les forces en présence sont d'un côté les anciens intérêts à court terme, commerciaux et financiers, de l'autre les nouveaux venus : par exemple l'agriculture biologique, les énergies nouvelles et les économies d'énergie ainsi que les défenseurs de l'intérêt général, de la préservation de la planète et des « biens communs » mondiaux.

À l'évidence, les premiers sont actuellement les mieux armés. Ils ont réussi une performance extraordinaire : engendrer une crise financière mondiale sans en subir eux-mêmes les

conséquences. Cette crise, commencée en 2008, n'était pas vraiment une surprise. Elle fait suite, d'après Stiglitz, à une série de 176 crises en 25 ans, depuis que la monnaie circule autour du monde par Internet à la vitesse de la lumière.

Elle a été amplifiée par de la création de liquidités, en trillions de $, adossée à des créances notoirement fragiles. Si ces turpitudes se poursuivent, les monnaies alternatives sur Internet apparaîtront comme un refuge. Ce sera le début du web 3.0.

Inévitablement, les seconds, les nouveaux venus, parce qu'ils s'orientent par rapport au long terme, auront le dernier mot. Reste à savoir dans quel état sera alors la planète et comment pourra se développer et se structurer le nouvel état de conscience.

MYTHES ET LEGENDES DE L'HISTOIRE DE LA CRYPTOLOGIE

Sophie de Lastours

« Pandore[1] avait l'Ancêtre, et le chiffre a la Fille,
Ce dernier rejeton de l'illustre Famille
Des boîtes d'où jaillit l'espoir du lendemain,
L'inconnu convoité, souci du genre humain.[2] »

L'Etat quelle que soit sa forme est sans relâche exposé à d'innombrables menaces, des plus intenses comme la guerre aux plus subtiles comme la trahison, le terrorisme, l'espionnage, le pillage économique…qui exigent la mise en œuvre de moyens de défense appropriés.

Dès l'Antiquité, les Etats ont eu des fortifications pour protéger leurs territoires, mais ils ont eu aussi pour protéger le secret de leurs communications, ce que les Anglo-saxons désignent par la formule « le pouvoir invisible » et qui est la cryptologie.

La cryptologie est aussi un des piliers du monde du renseignement et a joué et joue un rôle primordial. Elle est une arme à double tranchants au cœur de nos sociétés.

LE SECRET DU SECRET

Le chiffre a une longue histoire puisqu'il est plus ancien même que l'écriture,

Les hommes comptant sur les doigts de leurs mains pouvaient ainsi élaborer des codes, et leur imagination leur faisait dessiner, créer des symboles, puis l'écriture elle-même est devenue une sorte de code puisque peu de personnes sachant lire, tout lecteur devenait un décrypteur. Longtemps la lecture fut le monopole de la classe sacerdotale comme en Egypte et à Babylone.

Flechter Pratt[3] affirme que les Grecs ont inventé la transposition et les Romains la substitution, les deux grands systèmes de chiffrement. Un chiffre est un symbole. La différence entre chiffre et nombre est à rapprocher de celle qui existe entre lettre et mot. Mais le système établi des chiffres romains utilise les lettres latines. Les termes chiffre et code sont souvent employés comme synonymes alors qu'ils ne le sont pas, le chiffre et le nombre sont aussi confondus La « Française des jeux » elle-même le fait.

[1] *Pandore naquit du ressentiment de Zeus, voulant punir les hommes du don du feu que Prométhée leur avait fait. Héphaïstos la modela dans l'argile, Athéna lui insuffla la vie, Aphrodite lui octroya la beauté, Apollon le don de la musique.*

[2] *Claude Ducellier, « B.211 », Aux Armées , le 9 octobre 1939, Bulletin de l'Arcsi, no2 et 3, juin à septembre 1955.la B.211 est une machine à chiffrer achetée par l'armée française à la fin des années 30 à son concepteur, l'industriel Boris Hagelin.*

[3] *Flechter Pratt,* Histoire de la cryptographie, Les écritures secrètes depuis l'Antiquité jusqu'à nos jours, *Payot, 1940.*

Selon les civilisations, les nombres sont porteurs du destin : le quatre[4], le sept, le douze[5], le treize, le dix-sept[6]…sans oublier le fameux nombre d'or[7] Le mythe du chiffre est porté par la puissance de l'énigme que constitue toute existence. Le don de la pomme d'Eve à Adam, n'est-il pas le moyen de casser le code en accédant à la connaissance ?

Mythe fondateur du péché originel que celui contenu dans la Bible[8]. Depuis toujours, il est affirmé que le texte de la Bible repose sur une structure cachée obéissant à des règles mathématiques. L'informatique a permis d'approfondir cette recherche. Trois scientifiques israéliens[9] ont publié en 1994 un article détaillé sur le sujet. Ils évaluent la probabilité que le hasard dans leur démonstration ne s'élève qu'à une chance sur 2,5 milliards.

Ils affirment que les messages codés formant un ensemble cohérent qu'ils ont retrouvés, ont été intentionnellement inclus dans le texte par une intelligence supérieure[10].

La Shoah, la création de l'Etat d'Israël, l'assassinat de Rabin seraient annoncés.

Ceci ne prouverait pas nécessairement que si ces codes sont véritablement présents que Dieu les y a introduits. Une bataille d'experts est né, où partisans et sceptiques se sont affrontés[11]. Le journaliste Michael Drosnin entra alors en scène. C'était d'autant plus intéressant que ce dernier se définissait comme juif agnostique. Il publia « La Bible, le code secret[12] ». Il l'attribua lui à une intelligence extra-terrestre, écornant le mythe.

C'est alors que de nombreux chercheurs voulurent relever le défi, parmi eux des Chrétiens, des Juifs pratiquants ou pas. Leurs études ont gravement remis en cause ces affirmations et démontré que des « codes secrets » identiques à ceux de la Bible se trouvaient dans toute langue intelligible avec une probabilité plus grande que dans un ensemble incohérent de lettres sans aucune signification.

On trouva dans Moby Dick, la déclaration codée de la mort de Lady Di accompagnée du nom de son amant Dodi et même celui du chauffeur de la voiture !

Des codes dits négatifs et contradictoires furent aussi trouvés dans la Bible, tel que « Dieu est une chose détestable » ou tantôt « Il y a un Dieu », « il n'y a pas de Dieu.»

La conclusion a été que la Bible est un livre irremplaçable mythique et qui s'il a été inspiré par Dieu, celui-ci n'y a mis aucun code secret. Des partisans acharnés de l'existence de messages cachés poursuivent toujours leur combat. Mais Dieu, peut-être pour nous mettre à l'épreuve, a aussi bien pu introduire des messages codes en faisant croire qu'il s'agissait d'un

---

[4] *Le 4 porte malheur en Asie. Selon la prononciation, le mot peut signifier « mort » en Chinois.*

[5] *Le 12, nombre divin : 12 dieux dans l'Olympe, 12 tribus d'Israël, 12 signes du zodiaque, 12 apôtres…*

[6] *Le 17 porte malheur en Italie.*

[7] *Matila Ghika (1881-1965), Le nombre d'or, Gallimard, 1931. Prince diplomate et ingénieur naval roumain.*

[8] *On s'accorde à dater les textes de la Bible hébraïque du VIIIe siècle au IIe siècle avant J.C.*

[9] *Dorson Witztum, Eliahu Rips et Yoav Rotenberg, respectivement physicien, professeur de mathématiques et étudiant en informatique*

[10] *Ces messages codés ne se trouveraient que dans la version du texte hébreu canonique dite massorétique de la Bible. Elle serait due aux copistes respectant très fidèlement les textes, lesquels sont dits « Seigneurs de la tradition ».*

[11] *Les sceptiques étant Brebdan Mc Kay, mathématicien ; James D. Price, ingénieur et professeur d'Hébreu, Barry Simon mathématicien et juif orthodoxe.*

[12] *Michaël Drosnin,* La Bible : le code secret*, Laffont, 1997.*

pur hasard, car il exige de nous la véritable foi[13]. « Parce que tu m'as vu, tu as cru. Heureux ceux qui n'ont pas vu et qui ont cru ![14] »dit le Christ de l'Evangile à Thomas.

Selon Hérodote que l'on s'accorde à reconnaître comme le « Père de l'Histoire », le récit de l'Iliade aurait été rédigé entre 850 et 750 avant J.C., soit quatre siècles après la guerre mythique qu'il relate. Un passage de l'Iliade mentionne que Bellérophon fut chassé d'Argos par le roi Proetos car la reine Antée l'avait faussement accusé de harcèlement, comme la tradition considérait que la mise à mort d'un hôte était un crime impardonnable, il l'envoya donc chez son beau-père en Lycie, lui confiant une tablette d'argile recouvertes de signes inconnus à remettre à ce dernier. Ces dessins symboliques gravés étaient des lettres d'un alphabet différent que le grec et demandaient que Bellérophon soit tué. Reconnu comme d'essence divine, ce petit-fils de Sisyphe qui eut à combattre sur d'autres cieux[15] ne fut pas assassiné.

LE CHIFFRE, CLE DE VOUTE DE L'HISTOIRE

La cryptologie, discipline vieille de plusieurs milliers d'années est aujourd'hui à l'avant-garde de l'histoire de l'humanité : son côté pile défend notre liberté individuelle, son côté face nous protège de celle des autres mais elle affiche deux visages, tel Janus, le dieu des portes, celle de la paix alors fermée, celle de la guerre alors ouverte, Janus tourné vers le passé et tourné vers l'avenir.

Une sculpture symbolisant la cryptologie se dresse à l'entrée du siège de la CIA à Langley en Virginie. Des centaines de lettres y sont gravées reproduisant un message chiffré. Seul l'artiste, créateur de l'œuvre et le directeur de l'institution connaitraient le texte clair de ce message. La clé se transmettrait-elle de directeur en directeur comme le code de l'arme atomique de président en président ? Il semblerait que ce texte ait été décrypté il y a maintenant plusieurs années. Gageons qu'il prône la paix et l'entente entre les peuples.

En politique, diplomatie, économie, la cryptologie est une arme de premier plan.

Les *hackers* ayant infiltré Bercy ne s'inscriraient-ils pas dans un mouvement de contestation numérique, une sorte d' « altermondialisme numérique » comme le proclame haut et fort Eric Filiol[16]. Le mythe de la cryptologie s'effondrerait-il quand le site hyper protégé de l'Etat est attaqué avec succès ? Combien de vols, d'intrusions, d'informations capitales, de documents perdus à jamais constatés. ?

Le mythe du fruit défendu de la Bible est de retour, car la cryptologie longtemps sous contrôle militaire présente maintenant aussi de grands dangers, elle dissimule des actes condamnables, l'activité des mafias, le blanchiment d'argent, le terrorisme…

Le contrôle de la cryptologie ne peut être négligé et à l'inverse il faut créer à l'exemple de la Corée du Sud des unités de cyberdéfense. L'existence du décryptement comme source d'information et l'explication qui a pu en être donnée par les services de renseignement lorsqu'elle a été révélée, est restée souvent cantonnée dans des milieux restreints. Ce fut le cas pour le radiogramme de la Victoire de juin 1918, pour les travaux d'Ultra chez les

[13] *http://jewsforjudaism.org/response.html*

[14] *Evangile de Jean, 20.24-29. Le Christ s'adresse à l'apôtre Thomas.*

[15] *Allusion à sa fin et à celle de son destrier mythique Pégase.*

[16] *Il se définit comme un « corsaire » de la sécurité informatique. Il a dirigé le laboratoire de virologie et de cryptologie de l'ESAT et enseigne maintenant à l'ESIEA de Laval.*

Britanniques et Magic chez les Américains. On peut même prétendre que les autorités civiles et militaires sont restées dans leur majorité, ignorantes du rôle joué par la cryptologie lors des conflits.

Vassili Mitrokhin[17] affirme que la CIA n'a pas été mise au courant avant fin 1952 des révélations décryptées dès 1948 par l'US Army Security Agency (ASA). Le président Truman avait été tenu à l'égard de ces informations, de crainte qu'il en fasse mention au directeur de la CIA.

Il a fallu attendre 1945 pour que la défection d'un employé du chiffre de l'ambassade soviétique à Ottawa, Igor Gouzenko soit correctement exploitée et permette de découvrir l'extraordinaire ampleur de l'espionnage soviétique par l'URSS des secrets nucléaires alliés.

Les décryptements qui ont changé le cours de l'Histoire n'apparaissent que peu nombreux, ce qui signifie que beaucoup sont demeurés inconnus, que le secret de réussite avait été bien gardés mais lorsqu'ils le furent, la réalité en fut éblouissante.

La suprême réussite de la cryptologie au cours du temps a été de rester secrète, tour de force dans une société qui a aujourd'hui le culte de la transparence. Antoine Rossignol[18] ne cessa de répéter que pour qu'un chiffre militaire soit performant, il devait retarder le décryptement jusqu'à ce que l'ordre ait été exécuté ou jusqu'à ce que le renseignement n'ait plus aucune valeur. Ce principe reste fondamental dans l'usage de cette science même si tous les aspects de notre vie tendent à devenir dépendants de la cryptologie avec les ordinateurs, les cartes bancaires…

Ne pas avoir de secrets est un renoncement. Si pour Madame de Staël « La gloire était le deuil éclatant du bonheur », ne peut-on pas dire sous forme de boutade que « *facebook* est le deuil éclatant du secret. »

De nombreuses affaires d'espionnage en tout genre où la cryptologie joue le premier rôle se sont additionnées depuis le développement de cette discipline dans notre quotidien. Les satellites et les systèmes d'écoute et de décryptement quadrillent la planète depuis longtemps, les *hackers* ou ne faut-il pas préférer le mot les *crackers*[19]sont de plus en plus jeunes, de plus en plus performants. Cette sorte de montée aux extrêmes ne finira t'elle pas par produire une sorte d'équilibre de la terreur comme le nucléaire en son temps ?

Concluons sur l'expression « chiffre-clé », ces deux mots qui sont un double sésame au sein de la cryptologie où tout repose sur chacun de leur respectif secret. Amusons-nous de la richesse du vocabulaire en ce domaine : avancer un chiffre, le doubler, le gonfler, il est là employé au singulier mais l'est aussi ailleurs au pluriel comme : être fâché avec les chiffres, jongler, maquiller, falsifier les chiffres !

Le mot code prolifère de même : code de conduite, civil, postal, pénal, de la route, génétique sans oublier jamais le code d'honneur Le mythe de la cryptologie dans l'Histoire résiste à toutes les démonstrations car il s'apparente au divin alors que la réalité quotidienne remet tout en cause, fausse tout.

Une spirale infernale nous entraîne en accélérant la vitesse du temps, devenu temps numérique où une information en chasse une autre dans la seconde. Parallèlement le pouvoir

[17] *Transfuge russe qui a écrit avec Christopher Andrew Mitrokhin Archives.*

[18] *Antoine Rossignol (1600-1682), eut le titre de Conseiller du roi, son fils Bonaventure et son petit-fils furent aussi d'éminents cryptologues.*

[19] *Expression de Eric Filliol*

du chiffre a augmenté dans les mêmes proportions et celui des décrypteurs tout autant, sinon davantage ? L'humain est le maillon faible : Marie Stuart, Le chevalier de Rohan, Marie-Antoinette, le général Pichegru, Murat moururent du chiffre pour des raisons différentes, traîtrise, oubli, vantardise, compromissions. Painvin[20] en tomba malade, Olivari[21] eut de terribles maux de tête, Betty Pack y perdit la santé. Certains ont du être atteints de folie !

Le chef des renseignements britanniques Stewart Menzies en fut prisonnier au point de ne pouvoir évoquer la machine Enigma pour assurer sa propre défense.

Flechter Pratt relate qu'un officier du Bureau du chiffre anglais a calculé qu'un tiers des messages chiffrés passant dans son service au cours de la Première Guerre était erroné car des fautes avaient été faites dans le chiffrement.

Quand une information est secrète, l'adversaire mettra tout en œuvre pour l'obtenir. Francis Walsingham, le maître-espion d'Elisabeth d'Angleterre avait pour principe de demander que les archives des messages des chiffreurs du royaume soient détruites.

Souvenons-nous de Pandore évoquée plus haut. Dotée de nombreuses qualités, elle avait aussi quelques défauts : Hermés lui avait appris le mensonge et Héra la curiosité.

C'est pourquoi elle ne sut résister et ouvrit la fameuse boîte que Zeus lui avait offerte pour son mariage, tout en la mettant en garde du danger de soulever le couvercle. Les maux de l'humanité furent ainsi libérés : la guerre, la maladie, la famine, la pauvreté, le mensonge, le vice, la passion destructrice ainsi que l'Espoir, mais Pandore affolée voulut refermer le couvercle, il était hélas trop tard, seul l'Espoir, dernier à s'échapper y resta.

Ce n'est pas un hasard si Pandore que Hésiode[22], l'aède qui affronta Homère selon la légende dans un tournoi dialectique est appelée « le si beau mal ». La strophe sibylline qui introduit ces pages devrait être déchiffrable[23] pour tout Arcsien encore que l'on puisse avoir différentes interprétations…

Du Cantique des Cantiques, au Quantique des Quantiques sans omettre le possible CANTIQUE des QUANTIQUES…l'histoire du chiffre est mythique. Longtemps la cryptologie quantique nous a été présentée comme ouvrant les clés du paradis. On a appris depuis que celle-ci ne serait pas invulnérable[24].

Sir Charles Napier, lors de la conquête des Indes, télégraphia du front d'où il commandait la campagne du Sindh, le plus bref message de l'Histoire du chiffre : PECCAVI (I have Sinned)

Ceci n'est pas une légende.

---

[20] *Le capitaine Georges-Jean Painvin qui décrypta le Télégramme de la Victoire en juin 1918.*

[21] *Le colonel Henry Olivari appartenait à la section du chiffre pendant la Première Guerre Mondiale. Il sera envoyé en mission en Russie pendant six mois.*

[22] *Poète grec du VIII ème siècle avant J.C.*

[23] *Arcsi : Association des Réservistes du Chiffre et de la Sécurité de l'Information.*

[24] *Constatation que le professeur d'informatique quantique Hoi-Kwong Lo à Toronto résume par cette phrase lapidaire : « Nous avons tout autant besoin de hackers quantiques que de cryptographes quantiques ». Le Monde, internet Actu.net, du 26.06.2009.*

LA NEUTRALITE DU NET, UN MYTHE PARADOXAL

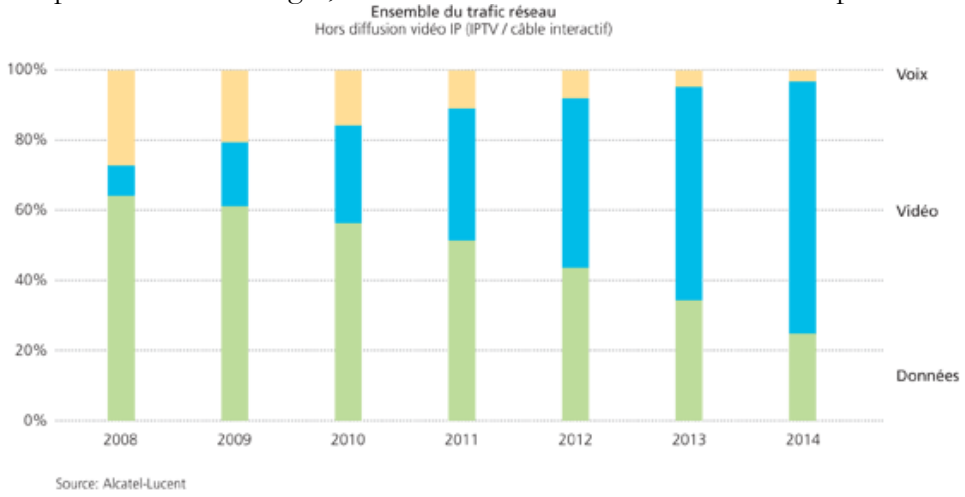
Dominique Lacroix, présidente de la Société européenne de l'Internet (SEI)

L'expression « neutralité d'Internet », trompeuse pour les non initiés, désigne un principe d'architecture des réseaux électroniques. Ce principe fait l'objet d'un débat mondial depuis plus d'un an : Union européenne, USA, Japon, Norvège, Suède, Royaume-Uni etc. La France y a consacré l'année 2010 et va légiférer sur ce thème en 2011, notamment dans le cadre de la transposition du Paquet Télécom européen de 2009.

De quoi s'agit-il ? Les opérateurs réseaux qui font circuler les paquets d'information ne doivent pas y toucher. Sauf force majeure comme une congestion de réseau ou une attaque, ils doivent les transporter sans discrimination, que ce soit selon la source, la destination ou le type de message auquel le paquet appartient (données, voix, audio, vidéo). Ce principe est étendu aux services et applications, ce qui interdit les pratiques commerciales de distribution exclusive, d'exclusion et de traitement prioritaire au sein des offres Internet. La transparence est requise sur les opérations de gestion des flux et sur le contenu réel des offres de services Internet. À première vue, ce sont des principes basiques : protection de la confidentialité et de l'intégrité de la correspondance (principe au moins aussi vieux que le télégraphe), droit de la concurrence et droits d'information du consommateur.

Et pourtant, les affrontements sur ce thème sont mondiaux et véhéments. Pourquoi ?

Des motifs économiques, d'abord, permettent de comprendre ce paradoxe. La dernière décennie a consacré l'organisation économique d'Internet en quatre groupe d'acteurs : producteurs d'éléments de réseaux et de terminaux (ex. Intel, Microsoft, Cisco, Alcatel-Lucent, Dassault Systems), opérateurs réseaux (ex. AT&T, Verizon, France Telecom), fournisseurs de services et intermédiaires (ex. Google, Amazon, eBay, Pages Jaunes) et producteurs de contenus (ex. The Walt Disney Company, Time Warner, Lagardère, Reed Elsevier). La catégorie la plus récente, les intermédiaires, est celle participe le moins à l'investissement dans les réseaux, échappe largement à l'impôt et réalise les bénéfices les plus importants. C'est aussi celle qui occupe une part croissante des ressources en bande passante. Cet effet ciseau ressort bien des tableaux de l'évolution de la part relative de la vidéo dans le trafic d'une part et taux de marges, d'investissement et de bénéfices d'autre part.



Taux de marge, effort d'investissement et retour sur investissement par couche en 2008 (en %)

	Taux de marge	Effort d'investissement	Retour sur investissement
Producteurs de contenus	9.9	5.1	28.2
Intermédiaires	14.5	6	69.5
Opérateurs de réseaux	12	17.5	17.0
Product. d'éléments de réseaux	6.6	6.1	32.3

Source : Coe-Rexecode. Ce tableau a été réalisé à partir de l'analyse d'un échantillon de 347 firmes provenant de la base Reuters. Après un travail de répartition des firmes parmi les couches, il a été procédé au calcul de plusieurs ratios financiers : le taux de marge qui est le résultat net après impôts rapporté au chiffre d'affaires (NOPAT/CA), l'effort d'investissements qui est l'investissement rapporté au chiffre d'affaires (CAPEX/CA), le retour sur investissements (*return on investment*, ROI), qui est le résultat opérationnel (EBITDA) rapporté au total de l'actif.

En bref, « la vidéo sature les réseaux ». Pour renouveler et améliorer les infrastructures, tant fixes que mobiles, les opérateurs réseaux sont tentés de facturer soit aux offreurs de contenus des services de livraison prioritaire, soit aux abonnés une qualité de service privilégiée ou des bouquets de contenus exclusifs. Toutes offres en infraction avec le principe de neutralité.

On en est là. Comment réguler ? Et qui va réaliser les investissements d'infrastructures en très haut débit reconnus indispensables ?

Le décor une fois planté, on devine le sourire entendu des professionnels et initiés.

La neutralité d'Internet ? Pfi ! Un principe mythique. La neutralité n'existe pas et, si elle a jamais existé dans l'Internet, il y a belle lurette qu'on l'a abandonnée.

L'examen successif des trois niveaux d'Internet, physique, logique et contenus, étonne en effet au regard de la neutralité.

La matérialité sous-jacente, quoique souvent occultée, repose d'abord sur une épine dorsale de câbles qu'il faut bien fabriquer et poser, sous la terre et sous les mers, puis gérer pour distribuer l'accès, en principe le plus largement possible à travers le globe.

Or, ce monde du silence, terriblement opaque et sans régulation, est tenu par un club très fermé, celui des plus gros fournisseurs de premier niveau. Ces acteurs échangent par troc (*peering*) entre homologues et ce simple jeu les connecte à l'ensemble des réseaux.

Plus on s'éloigne de ce qu'il faut bien appeler le centre d'un réseau réputé acentré, plus les acteurs échangent par accords de transit, c'est à dire d'achat de transport facturé, mécanisme où les acteurs les plus éloignés du centre ont un faible pouvoir de négociation sur les prix.

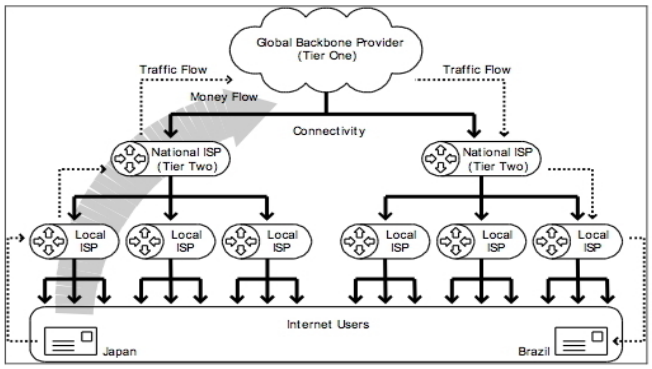
Mis à part le japonais NTT, l'indien Tata et TeliaSonera qui est finno-suédois, ces gros transporteurs sont états-uniens. Ils contrôlent donc le trafic de quasiment l'ensemble de la planète et en font remonter l'essentiel des bénéfices puisque l'exploitation de la fibre optique à ce niveau est réputée permettre des marges confortables.

Le niveau logique n'est guère plus équilibré. Le système Isoc-Icann, mis en place par le Ministère américain du commerce, a dévolu le contrôle des ressources critiques — adresses IP, extensions et noms de domaines — à l'Icann, association de droit californien. On aimerait croire aux engagements pris pour gérer ces ressources comme l'exige un espace public mondial. Mais pour le moment, ni la transparence requise, ni la reddition de comptes devant une instance internationale ne sont au rendez-vous. Et, par exemple, la France gère toujours son domaine national le *.fr* en vertu d'une délégation accordée par cette association californienne.

On sait par ailleurs qu'en termes géostratégiques les États-Unis ont défini l'espace et le cyberespace comme réservoirs de croissance et de puissance. Les observateurs peinent donc

Connectivity flows down, and money flows up.

Figure 2. Traffic and payment flows across the Internet



Source : Adam Peake, pour l'Association for Progressive Communications (APC) June 2004

List of Tier 1 networks

The following network s are believed to be Tier 1

Name	AS number
Qwest	209
Verizon Business UUNet	701
Sprint	1239
TeliaSonera International Carrier	1299
NTT Communications	2914
Tinet	3257
Level 3 Communications (L3)	3356
Global Crossing (GBLX)	3549
Savvis	3561

à croire les promesses de partage du pouvoir sur le réseau mondial sans démonstrations tangibles.

Les contenus enfin. La neutralité va de pair avec le principe de bout-en-bout (*end-to-end*). L'intelligence est placée en bout de ligne et le pouvoir donné aux utilisateurs. C'est, disait la légende, la fin des intermédiaires. Or, jamais les intermédiaires n'ont été si puissants et concentrés : Google, Amazon, eBay, Apple, Yahoo, MSN, Facebook et autres compagnies, commercialisent tout ce qui peut l'être dans le nouveau monde : données personnelles, données de connexions, statistiques, musique, livres, interstices d'espace sur les sites, transactions entre les personnes etc.

Cette économie numérique, florissante pour une poignée d'acteurs, s'établit sur des fondamentaux bien analysés : la quasi-nullité du coût marginal de production et la non rivalité, cette espèce de magie qui empêche un objet numérique de disparaître quand on le « consomme ».

Est-ce pour autant que les simples citoyens peuvent, eux aussi, explorer les bénéfices inouïs de cet univers conçu aux origines pour l'échange et le partage ? Cet univers toujours décrit comme le véhicule d'une société d'information, de création et d'émancipation ? Cet univers où l'attention des individus ne serait plus captée à leur insu ou contre leur gré mais désormais dédiée à la coopération, à la coproduction de savoirs et à la résolution de problèmes sociétaux ?

On peut en douter et craindre que les internautes ne soient au contraire la cible de producteurs de contenus en recherche de consommateurs. Le temps humain disponible n'est pas extensible dans les mêmes proportions que les supports numériques et les catalogues de droits fabriqués. Un autre effet ciseau se profile à l'horizon. Le choc risque d'être violent. C'est avec leurs cibles commerciales elles-mêmes que les producteurs de contenus entrent en concurrence. L'enjeu se révèle clairement. Sans garde-fous énergiques, l'Internet serait en train d'involuer vers un dispositif de Minitel amélioré. Le renforcement et la défense du *copyright* met en place aux quatre coins de la planète un arsenal juridique et répressif, fruit de

la convergence des besoins de surveillance entre sociétés commerciales candidates à péages et pouvoirs politiques enclins au contrôle sécuritaire.

Revenons donc à notre neutralité du net. On peut hausser les épaules et, sourire en coin, faire mine de clairvoyance face à un mythe écorné : « Ce fut un mythe fondateur, mais soyons modernes et réalistes. *Business as usual...* »

Par delà l'éviction fréquente face à ces interminables débats à fondements techniques, on peut se demander qui a vraiment intérêt à refuser l'analyse et la régulation visant à restaurer la neutralité des réseaux.

Le fait est que le décalage entre discours et réalité est d'une ampleur rare. Plus on s'éloigne de la neutralité des réseaux plus les proclamations d'attachement au principe se multiplient, comme l'expression d'un inconscient inquiet, comme dans une sorte de schizophrénie sociale.

La Commission européenne a assorti le Paquet Télécom d'une déclaration explicite en faveur de la neutralité. Elle a consacré le rôle des agences nationales de régulation dans la défense d'Internet ouvert et neutre.

La France est le pays qui s'illustre simultanément avec d'un côté la riposte graduée au partage de fichiers présumé illégal qui fait d'elle le héraut mondial de la Walt Disney Company et de l'autre côté une agence de régulation, l'Arcep, qui donne l'exemple du travail sérieux et méthodique d'un régulateur engageant les acteurs à restaurer l'Internet.

Aux États-Unis, le régulateur, la *Federal Communications Commission (FCC)*, peine à énoncer et défendre quelques principes bien en deçà de ceux de l'Arcep. Pourtant, le président Obama lui-même est un partisan déclaré de la neutralité du net, qui était même l'un de ses thèmes de campagne.

La neutralité du net apparaît comme un rêve qui hante des pouvoirs impuissants, comme une patate chaude que tout le monde se passe en espérant que le problème sera résolu sans avoir à le traiter, sans avoir à affronter les intérêts divergents.

Aussi peut-on être tenté d'affirmer que le mythe n'est pas la neutralité du net. Le véritable mythe, ce qui n'existe pas ou plus, c'est un pouvoir tutélaire et cohérent, qui, par nature, veillerait aux intérêts des populations. Le pouvoir politique actuel est plutôt un vaste champ de bataille où s'affrontent des groupes d'influence, une instance chargée de préparer l'avenir incertain avec des valeurs du passé.

L'autre mythe, ce qui n'existe pas encore, mais pourrait advenir, ce serait une humanité consciente, qui prendrait son sort et celui de la planète entre ses mains et se mettrait au travail sur ce qui importe vraiment.

Peut-être cette prise de conscience pourrait-elle se produire ? Grâce à l'Internet, justement, grâce à un Internet neutre et ouvert !

LE MYTHE DE L'INUTILITE D'UNE DISCIPLINE INFORMATIQUE DANS L'ENSEIGNEMENT GENERAL

Jean-Pierre Archambault, président de l'association Enseignement Public et Informatique (EPI)

Si, au fil des années, un consensus s'est progressivement dégagé sur l'idée que l'informatique était désormais une composante de la culture générale de notre époque et, à ce titre, un élément de la culture générale scolaire, ce ne fut pas sans douleur. Les discours selon lesquels l'informatique n'était qu'une mode qui passerait comme passent les modes ont pris un sacré coup de vieux. Pourtant on les entendait encore à la fin du siècle dernier jusqu'à ce que le développement d'Internet leur torde le cou.

Mais, s'il y a désormais consensus sur l'objectif général, des divergences fortes subsistent encore sur le contenu même de la culture informatique et les modalités pour la donner véritablement à tous les élèves. Avec un mythe qui a la vie dure : point ne serait besoin d'un enseignement d'une discipline scientifique et technique en tant que telle. Un mythe qui réserve ainsi un sort particulier à l'informatique qui représente pourtant 30% de la R&D au plan mondial (18% seulement en Europe). En effet, heureusement, on enseigne les mathématiques et les sciences physiques qui sous-tendent les réalisations de la société industrielle. Or le monde devient numérique comme l'a dit Gérard Berry dans sa leçon inaugurale au Collège de France, le 17 janvier 2008 (Pourquoi et comment le monde devient numérique).

Au nom de ce mythe, assorti d'un non-dit sur la récupération de postesd'enseignants, une option informatique présente dans la moitié des lycées d'enseignement général, mise en place dans les années quatre-vingt, fut supprimée une première fois en 1992, rétablie en 1994 puis à nouveau supprimée en 1998. Singulière façon d'entrer dans la société numérique ! Entorse au mythe, il y avait des éléments d'informatique dans le cours de technologie au collège.

Le mythe fonctionne sur un certain nombre de présupposés. Son cœur de doctrine est que l'utilisation des outils informatiques suffit à se les approprier et à donner une culture en la matière. Les compétences attribuées aux « natifs numériques » sont souvent invoquées. Or des thèses universitaires montrent qu'il faut relativiser fortement les compétences acquises hors de l'École, qui restent limitées aux usages quotidiens. Elles sont difficilement transférables dans un contexte scolaire plus exigeant. Les pratiques ne donnent lieu qu'à une très faible verbalisation. Les usages reposent sur des savoir-faire limités, peu explicitables et laissant peu de place à une conceptualisation.

Le mythe a inspiré le B2i (brevet informatique et internet) censé donner aux élèves une culture informatique à travers son utilisation dans les autres disciplines. Mais les faits ont montré que cela ne marchait pas. Rendu obligatoire pour l'obtention de brevet des collèges, on a assisté à des attributions massives et systématiques du B2i afin que les élèves ne soient pas recalés à l'examen. Le B2i s'est révélé être une machine administrative, donnant lieu à des « courses à la croix » sans réalités ni finalités pédagogiques.

Cela doit-il étonner ? Pas vraiment. En effet, le B2i suppose implicitement un apport de connaissances mais ne dit pas où les trouver, dans quelles disciplines et avec quels enseignants. Il n'est déjà pas évident d'organiser des apprentissages progressifs sur la durée lorsque les compétences recherchées sont formulées de manière très générale (du type « maîtriser les fonctions de base » ou « effectuer une recherche simple »), éventuellement

répétitives à l'identique d'un cycle à l'autre, et que les contenus scientifiques, savoirs et savoir-faire précis permettant de les acquérir, ne sont pas explicités. Mais, quand, en plus, cela doit se faire par des contributions multiples et partielles des disciplines, à partir de leurs points de vue, sans le fil conducteur de la cohérence didactique des outils et notions informatiques, par des enseignants insuffisamment ou non formés, on imagine aisément le caractère ardu de la tâche au plan de l'organisation concrète. Ainsi, un rapport de l'Inspection générale de l'Education nationale a-t-il souligné que, « si différentes circulaires précisent les compétences qui doivent être validées et le support de l'évaluation (feuille de position), elles laissent néanmoins dans l'ombre de l'autonomie les modalités concrètes de mise en œuvre ». Pour se faire une idée de ces difficultés, il suffit d'imaginer l'apprentissage du passé composé et du subjonctif qui serait confié à d'autres disciplines que le français, au gré de leurs besoins propres (de leur « bon vouloir »), pour la raison que l'enseignement s'y fait en français. Idem pour les mathématiques, outil pour les autres disciplines. Avec une approche dans laquelle on placerait l'étude des entiers relatifs dans le cours d'histoire (avant-après JC) et celle des coordonnées en géographie au gré des notions de latitude et de longitude !

Le mythe n'empêche pas les entreprises du secteur des TIC d'avoir du mal à recruter les personnels qualifiés dont elles ont besoin. Or l'on sait bien l'importance de la précocité des apprentissages. L'on sait également que le lycée est l'espace et le moment où les élèves construisent leur autonomie intellectuelle et où naissent les vocations. Les lycéens choisissent d'autant plus une voie par goût aux contenus qu'ils l'ont effectivement rencontrée concrètement dans leur scolarité. En 2009, le rapport « *Stratégie nationale de recherche et d'innovation », le SNRI, a fait le constat que « la majorité des ingénieurs et chercheurs non informaticiens n'acquièrent pendant leur cursus qu'un bagage limité au regard de ce que l'on observe dans les autres disciplines. Pourtant, ils utiliseront ou pourront avoir à décider de l'utilisation d'outils informatiques sophistiqués. Il est à craindre qu'ils ne le feront pas avec un rendement optimal ou que, en position de responsabilité, ils sous-estimeront l'importance du secteur.* »

Le vote de la loi Création et Internet dite loi Hadopi, la transposition de la directive européenne sur les Droits d'auteur et les droits voisins dans la société de l'information (DADVSI) par le Parlement en 2006 ont été l'occasion de débats complexes où exercice de la citoyenneté a rimé avec technicité et culture scientifique. En effet, s'il fut abondamment question de copie privée, de propriété intellectuelle, de modèles économiques…, ce fut sur fond d'interopérabilité, de DRM, de code source, de logiciels en tant que tels. Dans un cas comme dans l'autre on n'a pu que constater un sérieux déficit global de culture du numérique largement partagé. La question se pose bien de savoir quelles sont les représentations mentales opérationnelles, les connaissances scientifiques et techniques qui permettent à tout un chacun d'exercer pleinement sa citoyenneté (lors des débats concernant le nucléaire le citoyen peut s'appuyer sur ses connaissances acquises dans le cours de sciences physiques ; pour ceux concernant les OGM sur le cours de SVT). Sans risque de se tromper on peut affirmer que « cliquer sur une souris » et utiliser les fonctions simples d'un logiciel ne suffisent pas à les acquérir, loin de là. N'en déplaise au mythe, qui a du mal à concevoir que l'informatique, outil pour enseigner, outil dans les autres disciplines et l'informatique objet d'enseignement en tant que tel, sont complémentaires et se renforcent mutuellement.

Mais le mythe vacille. De nombreuses actions ont été menées en faveur d'une discipline informatique au lycée, notamment par l'EPI. Un enseignement de spécialité optionnel « Informatique et sciences du numérique » a été créé en Terminale S. Il entrera en vigueur à la rentrée 2012. C'est un premier pas positif qui en appelle d'autres...

LES MYTHES DE LA SOCIETE DE LA CONNAISSANCE

Laura Garcia Vitoria, directrice scientifique de la Fondation des Territoires de Demain

Toute société en pleine reformulation de ses valeurs et de ses objectifs se trouve être une grande productrice de mythes renvoyant à son passé aussi bien qu'au futur qu'elle s'imagine devoir construire.

Le premier niveau de la fabrique des mythes réside naturellement largement dans les images mentales qu'elle génère, qu'il s'agisse d'images d'anticipation qui s'avèrent toujours erronées, mais aussi d'une absence dans ces mêmes images du passé qui est le sien et dont nos contemporains regrettent à l'avance leur absence ! Nous savons tous au travers de l'expérience de nos années passées combien ces deux catégories de représentations s'avèrent évidemment éminemment fausses et qu'elles font partie habituellement des mythes ici évoqués.

Aux côtes des images, c'est le vocabulaire qui se voit producteur de mythes multiples. C'est le cas de tous les fossés sociaux et psychologiques que n'arrêtent de dénoncer ceux qui y voient le seul horizon possible pour justifier leurs fantasmes politiques et économiques. Le savoir - pourquoi ne pas le dire ici - est pourtant bien moins vecteur de fractures sociales que l'ignorance !

Il en est de même des expertises qui devront être les nôtres dans la société de demain: elles seront en effet basées sur des stratégies d'appropriation des savoirs déclinées au quotidien, que des outils technologiques naissants nous permettront de réussir et qui ne seront en aucun cas des vecteurs d'échecs dans la mémorisation de ce qui assure la gestion de nos identités.

De même encore, font parties des mythes de la société naissante, à l'évidence, les soi-disantes déviations des savoirs et des savoir-faire : il ne saurait bien sûr en être autrement, tant les mutations des sociétés tonnent pour assurer les fins de leurs habitudes de lire et de penser, de regarder et de déduire, de croire et de s'assurer. Nous savons là encore - au travers de tous les exemples que l'histoire des deux ou trois millénaires nous propose - qu'il n'en est rien, souvent bien au contraire !

C'est le cas précisément des nouvelles façons de travailler et de vivre qui s'esquissent sous nos yeux. Jamais nous n'avons eu autant de moyens de nous souvenir, de nous référer à notre passé, de nous le projeter dans les endroits les plus adéquats, d'en associer les composantes à l'heure qui nous sied le plus.

Nous imaginons de même les individus plongés dans de nouvelles formes d'isolement, alors même que l'économie du lien émergente qui nous environne nous aide à fabriquer des rapports aux autres démultipliés.

La mise en réseau de ce qui rend notre présence au monde plus pertinente nous permet d'ailleurs de créer à cet égard le meilleur des imaginaires alliant des environnements tactiques producteurs de sens à des écosystèmes nous offrant toutes possibilités de changement, au fur et à mesure des objectifs qui se proposent à nous.

Aussi, à peine sortis d'horizons sociaux aux contraintes multiples, nous nous forgeons des mythes de contraintes nouvelles qui ne tiennent en réalité, là encore, qu'à nos propres ignorances, à nos visions de problèmes de toutes natures sans d'abord voir autour de nous ce

qui permet précisément d'y mettre fin. Constitue à ce propos un vrai paradigme la naissance d'un réseau international de journalistes se proposant, en liaison avec de nombreux acteurs économiques et technologiques, d'évoquer les solutions plus que les problèmes, les possibilités humaines plus que les impossibilités matérielles...

Certes, la mythologie ainsi esquissée ne saurait être bien évidemment univoque, elle sait aussi agencer des inquiétudes - même si celles-ci résident surtout dans notre appréhension à ne pouvoir y faire face -.

Plus sombre donc peut paraitre la liste des défis et notre propension à penser d'abord la difficulté pour y faire face. Et là aussi, nous nous fabriquons un horizon mythologique conséquent.

Ainsi s'enrichit d'abord une imagerie de l'autre qui n'est pas loin de forger un nouveau chapitre des imageries d'Epinal qui nous montrent des pouvoirs qui n'en sont pas au travers notamment de la démultiplication des réseaux sociaux. De même en sera-t-il des pensées qui n'en sont pas, des références sans consistance, des copier-coller sans mesure, des amis célèbres parce qu'inconnus, des propos qui s'entrechoquent, des mises en liaison rapides, des compréhensions lentes devant des listes de micro-bloging interminables...

La galerie s'avère donc d'ores et déjà consistante, avec ses enthousiasmes faciles et ses craintes qui ne le sont pas moins, avec un horizon social où les uns ont le sentiment de pleinement se retrouver et d'autres démultiplient des regrets dont la vacuité ne saurait les accompagner dans le futur.

1° PARTIE : ASPECTS INFORMATION ET SYSTEMES D'INFORMATION

MYTHES ET LEGENDES D'INTERNET

Gérard Peliks, CASSIDIAN
an EADS Company

LES FAUSSES CERTITUDES

L'Internet est tellement ancré dans notre vécu quotidien que comme pour toute chose qui s'est rapidement imposée, il s'est bâti autour de ce phénomène, des croyances devenues certitudes qu'il n'est même pas envisageable de remettre en question sans passer pour quelqu'un qui n'a rien compris à ce qui semble évident à l'homo vulgaris.

Mais ces certitudes ont parfois leur part d'erreurs et peuvent figer le développement de ce moyen irremplaçable de communication qui a bien besoin d'évoluer, peut-être même en changeant de base.

Mieux comprendre l'Internet d'aujourd'hui, en particulier dans ses couches basses est indispensable pour appréhender les travaux qui sont menés actuellement dans des centres de recherche, et qui pourraient bien changer les bases de l'Internet du futur.

MYTHE N° 1 : L'INTERNET BENEFICIE LARGEMENT DE L'INNOVATION

En fait très peu d'innovations ont été réalisées depuis la fin des années 70 dans les couches basses d'Internet. Comme le système fonctionne, porté par l'augmentation des performances prévue dans les lois de Moore, comme les protocoles sont entérinés par des organismes de standardisation, l'IETF en particulier, ceux qui avaient le pouvoir de faire évoluer l'Internet ont préféré se servir de l'existant pour asseoir leur business. Notons que la standardisation d'Internet n'est pas le fait d'organismes internationaux de normalisation comme l'ISO, l'UIT ou l'ETSI, et que l'IETF est un organisme essentiellement sous contrôle des Américains.

La recherche et le développement des couches basses d'Internet ont été laissés à l'abandon car les retombées en revenus immédiats n'ont jamais été perçues de manière évidente et l'aspect économique a primé et écarté l'innovation. Il fallait que l'Internet rapporte de l'argent. Pour cela, il ne fallait surtout pas toucher aux couches basses qui devaient rester stables.

Certes, côté applicatif, il y a eu de grandes innovations, comme bien sûr le Web, aujourd'hui participatif et demain sémantique, comme les nouveaux usages : musique, vidéo, films, P2P, ToIP, forums. Il y en aura de nombreux autres à peine croyables aujourd'hui, comme la 3D et la réalité augmentée... Mais justement, ces avancées peuvent difficilement reposer sur des couches basses qui n'ont pas évolué en rapport avec ce que réclament les nouvelles applications, en sécurité, en mobilité, en sans-fils, en multihoming (connexion à plusieurs réseaux).

MYTHE N° 2 : L'INTERNET EST UN RESEAU QUI APPARTIENT A TOUT LE MONDE

Ça c'est un mythe tellement répandu que l'accès à la toile, l'envoi des courriels, les forums de discussion sont devenus aussi naturels que l'air qu'on respire et qui appartient à tous, comme semble l'être l'Internet, abonnement à un fournisseur de services mis à part. Et pourtant

l'Internet est loin d'être neutre. Il "appartient" à l'ICANN (Internet Corporation for Assigned Names and Numbers). En effet, l'ICANN gère l'espace d'adressage du sommet de la hiérarchie des noms de domaines d'Internet, et ses serveurs de noms de domaines racines, ce qui en fait de facto son véritable propriétaire car qui détient le nommage détient le pouvoir.

Créé en 1998, l'ICANN est une organisation de droit privé, plus précisément de droit californien. Vinton Cerf, un des intervenants de notre grand événement sur le futur d'Internet du mois de janvier en avait été le président durant près d'une dizaine d'années. Il est vrai que ces derniers temps, la gouvernance de l'ICANN est devenue un peu moins américaine, mais à peine moins. On dit que le président des Etats-Unis dispose (ou disposera) d'un gros bouton rouge, pour désactiver l'Internet mondial en cas de cyber attaque grave sur son pays. D'ailleurs les Etats-Unis avaient déconnecté pendant un certain temps le domaine de l'Irak du reste d'Internet. Aucun autre pays ne pourrait en faire autant.

Les Chinois ont déjà pris leurs distances par rapport à ce qu'on appelle encore communément "l'Internet" (au singulier), en constituant leur propre Internet indépendant de celui du reste du monde. Les Iraniens penseraient sérieusement à faire de même. Ces dissidences pourraient faire effet domino, ne serait-ce que pour prendre en compte des alphabets non latins, des lettres accentuées ou une philologie non américaine. On parlera alors non pas d'Internet mais "des" internets, tout ceci pour une question d'adressage et de gestion des noms de domaines !

MYTHE N° 3 : L'INTERNET EST ISSU DU RESEAU ARPANET

Ce n'est pas faux. L'Internet a beaucoup bénéficié des travaux réalisés pour le réseau ARPANET et en particulier du développement des protocoles IP et des protocoles au dessus (TCP, UDP, ICMP, FTP, SMTP, HTTP …).

Toutefois si on mène une recherche en paternité d'Internet, on peut remonter plus loin, jusqu'aux travaux autour du projet CYCLADES de l'IRIA (qui allait devenir l'INRIA) et de l'idée du datagramme, objet logiciel qui permet de travailler en mode sans connexion. A la tête du projet CYCLADES, il y avait le Français Louis Pouzin, à qui revient le titre d'inventeur d'Internet. Mais dans la France des années 70, sous la présidence de Valéry Giscard d'Estaing, les PTT avaient imposé le circuit virtuel (mode avec connexion) qui allait donner X25 puis ATM.

Et c'est ainsi qu'une idée française, un mode sans connexion, ne s'est pas concrétisée en France et que les Etats-Unis sont devenus les maîtres incontestés d'Internet.

MYTHE N° 4 : LE ROUTAGE D'INTERNET EST DECENTRALISE

Décentralisé comme le routage du téléphone ou du GSM ? On voudrait bien que ce soit vrai mais c'est loin d'être le cas. Si on prenait une image, utiliser le routage d'Internet, c'est comme si on demandait à un facteur de distribuer le courrier, mettons rue de Vaugirard. Mais le premier immeuble de cette rue ne serait pas le "1 rue de Vaugirard", mais le "232 boulevard Eisenhower", en face ce ne serait pas le "2 rue de Vaugirard" mais le 12 avenue Mao Tse Toung, et ainsi de suite.

Vous voyez le surcroit de travail pour le pauvre facteur obligé de consulter un répertoire qui fait la liaison entre l'implantation de l'immeuble dans la rue et son adresse ? Et pour les

employés du centre de tri postal, quel cauchemar pour classer le courrier ! Il faut donc des répertoires (serveurs DNS).

Tout ceci suite à de mauvaises options dans l'attribution des adresses IP, dans le nommage des domaines et dans la répartition des tâches entre les couches IP et TCP. Mais c'est ainsi que fonctionne le routage sur l'Internet car la plupart des routes sont statiques.

Chaque message, chaque fichier est découpé en datagrammes et chaque datagramme qui connaît son adresse de destination (contenue dans le champ IP) est acheminé de proche en proche, via des routeurs, dans les réseaux connectés. Et chaque routeur doit connaître vers quel routeur de proximité transmettre le datagramme qui ne lui est pas destiné, en fonction des routes qu'il connait et de celles qu'on lui fait connaître.

Ceci entraine une explosion en taille des tables de routage, des performances dégradées car les routeurs arrivent à la limite de leur capacité de calcul et le problème va vite devenir insoluble.

MYTHE N° 5 : L'ADRESSE IP IDENTIFIE UN ORDINATEUR

Ça vous semble évident ? Et bien non, l'adresse IP identifie le contrôleur réseau par lequel votre ordinateur se connecte à l'Internet ou à un Intranet. On aurait bien voulu qu'une adresse IP indique qui en est le possesseur, ou au moins l'ordinateur qui possède cette adresse si ce n'est qui est l'utilisateur de cet ordinateur, à quel endroit se trouve cet ordinateur et quelle est sa fonction. On est loin du compte.

Tous ces renseignements (qui, où, quoi), ne peuvent être donnés qu'en rajoutant constamment des rustines au dessus de la couche IP d'Internet.

Comme l'a fait remarquer le professeur Kavé Salamatian de l'Université du Jura, l'Internet bien conçu il y a quarante ans pour un nombre très petit de nœuds, à ses début dans le projet ARPANET, avait une couche IP fine et élégante, mais elle s'est très vite engraissée et présente aujourd'hui de grosses poignées d'amour qui sont IPsec, NAT, Diffserv, Mcast...

Un poids trop élevé et un corps trop potelé, tous les nutritionnistes vous le diront, ce n'est pas bon pour la santé.

MYTHE N° 6 : L'IPV6 VA RESOUDRE TOUS LES PROBLEMES EVOQUES

L'IPv6, nouveau protocole d'Internet, résout le problème du nombre d'adresses IP devenu très insuffisant, avec l'IPv4, pour satisfaire aux exigences de la demande pour les objets communicants, pour les voitures électriques, pour les compteurs électriques intelligents et d'une manière générale pour l'explosion du nombre d'utilisateurs. Un utilisateur, en particulier pour la mobilité a besoin aujourd'hui de nombreuses adresses IP. Et les objets intelligents communicants, les étiquettes RFID vont encore faire exploser ce nombre d'adresses nécessaires.

L'IPv6 ajoute également des solutions pour assurer la sécurité, la qualité de service, la mobilité et la diffusion en multicast (un émetteur et plusieurs récepteurs).

Mais l'IPv6 conserve la philosophie de l'IPv4, en particulier celle du mode sans connexion et la notion de "best effort".

Si l'IPv6 n'est pas la solution, faut-il faire table rase de l'existant et repartir à zéro, et non de protocoles couverts de rustines, et de protocoles qui s'empilent et parfois coexistent mal

entre eux, comme le préconisent plusieurs chercheurs, tels John Day et Louis Pouzin qui ont été à la base d'Internet ?

LE POST-IP

En conclusion de ces mythes et des réponses qu'on peut apporter pour démystifier le phénomène, John Day propose, par exemple, un nouveau socle pour l'Internet, non plus bâti sur les couches IP mais sur un modèle de communication interprocessus (Inter Process Communications : IPC) récursif : les protocoles RINA qu'il décrit dans son livre "Patterns in Network Architecture, a return to fundamentals"

Dans ce nouveau principe, qui est une technologie de rupture par rapport à l'existant, le réseau n'est plus un moyen de transporter les données mais un mécanisme d'échange entre processus qui transportent les données. Seuls les processus accèdent aux données qu'ils transportent. L'extérieur n'a pas accès aux adresses internes, ce qui rend difficiles les attaques classiques, basées sur la connaissance des adresses IP vulnérables, pour compromettre les données et renforce la sécurité.

Si le mode avec connexion et le mode sans connexion se rencontrent pour assurer un transport de l'information sûr et performant, dans une architecture où les IPC remplaceront le modèle en couches, et se dupliqueront de manière récursive pour s'adapter aux réseaux physiques, il est certain que l'Internet du futur pourra reposer sur un socle plus solide que celui sur lequel repose l'Internet d'aujourd'hui.

MYTHES ET LEGENDES DE LA NAVIGATION SUR L'INTERNET

Michel Lanaspèze, SOPHOS

Vous pensez être bien protégé lorsque vous naviguez sur Internet ? Avec une nouvelle page infectée toutes les deux secondes, il est pourtant quasiment impossible de disposer d'une sécurité permanente sur le Web, même en étant parfaitement informé ou conscient des risques potentiels.

Posez-vous juste les questions suivantes :

Pratiquez-vous une navigation prudente sur le Web ? Evitez-vous les sites à risque ? Utilisez-vous un navigateur sécurisé ? Savez-vous reconnaître lorsqu'un site présente un risque quelconque ? Limitez-vous la navigation pendant les heures de travail ? Avez-vous mis en place une politique stricte d'accès à Internet ?

Si répondez "oui" à l'une de ces questions, alors nous vous recommandons vivement de lire la suite. Vous pourriez être la victime de préjugés sur la sécurité d'Internet. Mais ne vous inquiétez pas, vous n'êtes pas seul. Ces dernières années ont vu beaucoup de désinformations circuler sur les risques du Web, leurs effets potentiels et ce qu'il faut faire pour s'en protéger.

MYTHE N° 1 : LE WEB EST SUR CAR JE N'AI JAMAIS ETE INFECTE PAR DU MALWARE EN NAVIGUANT SUR LE WEB

Si vous faites partie des rares internautes à ne pas encore avoir pris conscience du danger, il est malheureusement assez probable que vous ayez déjà été infecté sans le savoir.

En effet, depuis plusieurs années déjà, la navigation Web est devenue le principal vecteur d'infection par des malwares. Une nouvelle page Web est compromise toutes les deux secondes pour être transformée en page Web infectieuse. De plus, la majorité du spam qui arrive dans vos boîtes aux lettres électroniques essaie de vous diriger vers une de ces pages Web infectieuses, un site Web contrefait (attaque par hameçonnage ou « phishing ») ou des sites de vente en ligne douteux.

Comme l'écrasante majorité des infections est silencieuse, les internautes sont rarement conscients d'avoir été infectés quand ils ne bénéficient d'aucun système de protection. Généralement, les attaques de malware sur le Web sont conçues pour dérober des mots de passe et des informations personnelles, ou pour utiliser votre poste à votre insu comme plate-forme de distribution de spam, de malwares ou de contenu inapproprié.

MYTHE N° 2 : SEULS LES SITES A CARACTERE PORNOGRAPHIQUE, JEUX D'ARGENT ET AUTRES SITES "SUSPECTS" PRESENTENT UN DANGER

Plus de 80 % des sites hébergeant du malware sont en fait des sites dits de confiance qui ont été piratés. Les internautes les consultent quotidiennement sans savoir qu'ils ont été piratés pour distribuer des malwares.

Pourquoi ? Parce qu'ils sont populaires, ces sites attirent un fort trafic et permettent de distribuer du malware aux visiteurs à leur insu et en grande quantité.

Même s'il est avéré que certaines catégories de sites sont considérablement plus affectées que d'autres, les sites d'entreprises réputées sont susceptibles d'être infectés. Il suffit pour cela d'une page Web mal codée ou d'une nouvelle vulnérabilité du serveur Web non corrigée pour ouvrir la porte aux pirates.

Il est donc essentiel que les internautes restent vigilants, même quand ils limitent leur navigation à des sites de confiance.

MYTHE N° 3 :
AU MOINS, LES RESEAUX SOCIAUX SONT-ILS SURS PUISQUE JE M'Y RETROUVE ENTRE AMIS.

C'est un mythe qu'il faut combattre de toute urgence, pour que les internautes ne baissent pas la garde quand ils socialisent sur ces nouveaux espaces d'échanges.

En effet, les réseaux sociaux sont rapidement devenus le nouveau champ d'action privilégié des pirates informatiques et autres cybercriminels. Il n'y a rien d'étonnant à cela, les attaques informatique de masse suivant leurs victimes potentielles là où elles se retrouvent en nombre. Qui plus est, ce nouvel espace représente une cible de choix car les internautes s'y sentent en confiance, étant en principe entourés d'amis.

Les pirates sont ainsi passés experts dans le vol de comptes et mots de passe de réseaux sociaux, qu'ils utilisent pour infecter et arnaquer les cercles d'amis. Un moyen relativement simple utilisé par les pirates pour récupérer ces informations de comptes consiste à envoyer des messages de spam vous enjoignant de vous connecter de toute urgence sur votre réseau social préféré, prétextant la nécessité d'une supposée mise à jour ou d'une vérification administrative. Le lien qui vous sera proposé n'est autre qu'une version contrefaite de la page d'accès au réseau social, créée dans le seul but de voler votre compte et votre mot de passe. Une fois en possession d'un accès à votre compte, le pirate s'empressera de modifier votre mur ou d'ajouter des messages invitant vos amis à cliquer sur un lien intéressant, qui n'est autre qu'une page infectieuse ou un site d'arnaque.

L'intérêt croissant des pirates pour les réseaux sociaux les a mené à créer des malwares spécialisés, tels que la célèbre famille Koobface. Les malwares de cette famille sont si sophistiqués qu'ils sont capables de créer automatiquement un compte Facebook, de l'activer en confirmant le courriel envoyé à une adresse Gmail (qu'ils auront pris soin de créer auparavant automatiquement), de devenir amis avec des inconnus inscrits sur le site, de rejoindre des groupes Facebook et de diffuser des messages sur les murs de ses amis, prétendant diriger vers des vidéos sexy contenant en réalité du malware. De plus, il cherche à assurer sa discrétion en restreignant le nombre de nouveaux amis qu'il accepte par jour. Au départ limité à Facebook, dont il a d'ailleurs tiré son nom, Koobface a depuis élargi sa cible en visant un grand éventail de sites. Apparue en 2008, cette famille ne cesse de se raffiner et se diversifier, faisant preuve d'une longévité tout à fait exceptionnelle dans le monde des malwares, ce qui illustre l'engouement des pirates pour les réseaux sociaux.

MYTHE N° 4 :
VOUS NE POUVEZ ETRE INFECTE QU'EN TELECHARGEANT DES FICHIERS

La plupart des infections par malwares se produisent aujourd'hui par téléchargement passif, qui ne requiert aucune action de la part de l'internaute si ce n'est le simple fait de visiter un site.

Les pirates injectent du code malveillant dans le contenu de leur page web, qui se télécharge et s'exécute automatiquement dans le navigateur comme une sous-fenêtre de visualisation de la page Web.

Un bon exemple de ce type d'attaque est fourni par la famille Gumblar. Cette famille de malwares a représenté jusqu'à 40% de toutes les infections de sites Web. Après une éclipse en fin d'année 2009, elle est revenu sur le devant de la scène début 2010. Il s'agit d'un code JavaScript malveillant infecté au sein de sites web légitimes, dans le but de rediriger les visiteurs vers des sites web contrôlés par les pirates, qui tentent d'exploiter des vulnérabilités d'Acrobat Reader et de Flash/Shockwave pour infecter le système. C'est un type d'attaque par téléchargement passif auquel appartient également la célèbre injection iFrame.

MYTHE N° 5 :
SEULS LES UTILISATEURS NAÏFS SE FONT INFECTER PAR DES VIRUS ET DES MALWARES

Comme mentionné précédemment, la plupart des infections s'effectuant par téléchargement passif, l'infection n'a donc rien à voir avec les compétences informatiques de l'utilisateur. En réalité, dès lors que vous visitez des sites Internet, le risque existe.

Ces malwares sont très souvent créés à partir de kits de code malveillant professionnel, commercialisés et vendus aux pirates, qui les utilisent pour exploiter les failles dans le navigateur, le système d'exploitation et les plug-ins et infecter les systèmes. Encore une fois, cela s'effectue de manière totalement invisible aux yeux de l'utilisateur qui visite simplement un site piraté.

Un système parfaitement tenu à jour des derniers correctifs de sécurité contre les vulnérabilités connues du système d'exploitation, du navigateur, de ses plug-ins et des applications Web présente cependant un défi certain pour les pirates. Ils peuvent néanmoins toujours s'appuyer sur les vulnérabilités non corrigées ou, plus simplement, la naïveté de certains utilisateurs face aux attaques par « ingénierie sociale ».

Une des attaques les plus en vogue consiste à proposer les services d'un faux antivirus. En naviguant ainsi sur une page Web compromise, l'internaute sera d'abord soumis, en général, à une première tentative d'infection silencieuse par l'intermédiaire d'une faille de sécurité éventuelle. Si cette attaque échoue, le malware passe alors au « plan B », celui du faux antivirus. Pour cela, il ouvre des fenêtres présentant à s'y méprendre l'aspect d'un antivirus ordinaire, mais de marque inconnue, qui va après quelques secondes déclarer avoir détecté plusieurs virus. Il vous proposera alors de désinfecter gratuitement votre ordinateur, en vous demandant de valider son activation. En cliquant sur « oui », vous donnez en réalité l'autorisation à un malware de s'installer sur votre système. En guise de « cerise sur le gâteau », beaucoup de ces faux antivirus vous proposeront ensuite d'acheter une licence illimitée à prix cassé, qui n'aura d'autre but que de récupérer votre numéro de carte de crédit !

Dans ces cas d'attaque par ingénierie sociale, il est effectivement recommandé d'être constamment sur ses gardes et ne pas pêcher par naïveté.

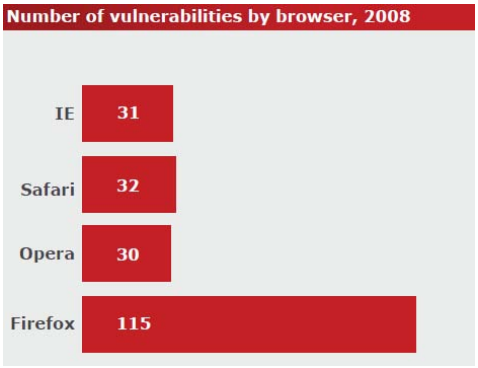
MYTHE N° 6 :
FIREFOX EST PLUS SUR QU'INTERNET EXPLORER

Tous les navigateurs sont exposés de façon identique aux risques car ils constituent tous un environnement d'exécution de JavaScript, qui est le langage de programmation employé pour Internet.

C'est pourquoi tous les auteurs de malwares l'utilisent pour initier des attaques. De plus, de nombreuses failles exploitent les plug-ins, tels que le logiciel Acrobat Reader, qui fonctionnent avec tous les navigateurs.

Bien que les navigateurs les plus utilisés sont plus connus pour leurs failles sans correctifs, ce sont les failles qui ne font pas parler d'elles qui devraient vous alerter le plus. En réalité, il n'existe aucun navigateur sûr.

Quant à Firefox, une étude réalisée par la société de recherche en sécurité Secunia portant sur le nombre de failles des navigateurs en 2008, a montré qu'il n'occupait pas nécessairement la première place des navigateurs les plus sûrs, et de loin.



Source : http://secunia.com/gfx/Secunia2008Report.pdf

D'une manière générale, quel que soit le navigateur que vous utilisez, il est essentiel de le tenir parfaitement à jour des plus récents correctifs de sécurité.

Ceci présente un défi particulier en entreprise, où nombre d'utilisateurs souhaiteraient utiliser leur navigateur préféré, quitte à importer une version mal corrigée d'un navigateur. Il faut rappeler aux internautes qu'un des premiers bénéfices que leur peut apporter leur entreprise est une navigation sûre, et qu'à ce titre il est non seulement légitime mais dans leur propre intérêt que l'entreprise contrôle les versions des navigateurs utilisés sur son réseau.

MYTHE N° 7 :
LORSQUE L'ICONE DE VERROUILLAGE APPARAIT DANS LE NAVIGATEUR, JE SUIS EN SECURITE

L'icône de verrouillage indique la présence d'une connexion chiffrée SSL entre le navigateur et le serveur afin de protéger contre l'interception des informations sensibles personnelles. Mais il n'apporte aucune sécurité contre les malwares.

En fait, c'est même le contraire.

En effet, la plupart des produits de sécurité Web ignorent complètement les connexions chiffrées : c'est donc le parfait vecteur pour infiltrer du malware sur un poste.

De plus, certains malwares peuvent exploiter des vulnérabilités pour imiter des certificats SSL, donnant ainsi aux utilisateurs l'impression d'être sécurisés, ou activer des connexions détournées vers de faux sites bancaires. De nombreux cas récents illustrent comment les pirates créent des techniques sophistiquées de phishing qui permettent de reproduire des sites complets de banque en ligne, avec cartes de crédit et comptes PayPal, via l'imitation de certificats SSL, extrêmement difficiles à identifier pour l'utilisateur moyen. Ces méthodes engendrent des risques de sécurité de plus en plus élevés.

MYTHE N° 8 :
NOUS CONTROLONS L'UTILISATION DU WEB ET NOS UTILISATEURS NE PEUVENT PAS CONTOURNER NOTRE POLITIQUE

Beaucoup d'internautes sont passés maîtres dans l'utilisation de « proxies anonymes » pour contourner la politique de filtrage Internet et consulter les sites Web de leur choix. D'abord popularisés dans les milieux étudiants, les proxies anonymes sont nombreux et facilement accessibles par les utilisateurs. Chaque jour, des centaines de proxies anonymes sont conçus et mis en ligne dans le but de contrer les barrages de sécurité des entreprises et les utilisateurs les plus sophistiqués établissent même leur propre proxy privé à la maison pour pouvoir naviguer sur le Web en toute liberté et échapper à tout contrôle.

Si vous avez tendance à minimiser le problème, il vous suffit de consulter les très nombreuses pages proposant des moyens d'éviter le filtrage Internet sur Google pour vous rendre compte de l'ampleur du phénomène.

Il est donc fortement recommandé de mettre en place des solutions de protection permettant d'éviter le contournement des politiques de sécurité par des proxies anonymes.

MYTHE N° 9 :
DE TOUTE MANIERE, NOUS NE POUVONS RIEN CONTROLER QUAND LES CONNEXIONS SONT CHIFFREES PAR HTTPS

Les connexions chiffrées présentent un défi particulier car dans ce cas, il n'est pas possible de vérifier que des malwares ne sont pas introduits dans l'entreprise ou que des informations sensibles, comme des informations à caractère personnel au sens de la CNIL, ne sont pas diffusées hors de toute légitimité.

De nombreuses solutions de protection de la navigation Web permettent cependant de filtrer le trafic HTTPS. Généralement installées en passerelle, elles n'autorisent l'établissement de connexions HTTPS qu'à condition de leur donner un droit de regard pour appliquer les politiques de sécurité de l'entreprise.

Bien entendu, ce type de filtrage doit être déclaré explicitement dans la charte des politiques de sécurité de l'entreprise, revue et validée par les représentants du personnels et acceptée explicitement par les employés eux même. Ce filtrage exclut en général les connexions vers certains sites, comme ceux d'établissement bancaires et financiers reconnus, afin de préserver la confidentialité complète et légitime de certaines communications.

Il est bon de rappeler que si l'utilisation d'Internet pour des motifs personnels est tolérée en entreprise, elle reste soumise aux politiques de sécurité définies par l'entreprise, qui s'attachent à défendre aussi bien les propriétés intellectuelles de l'entreprise, les droits collectifs des individus comme définis par la CNIL et le droit des employés à pouvoir naviguer sur le Web en toute sécurité.

MYTHE N° 10 :
LA PROTECTION DU WEB SUPPOSE UN COMPROMIS ENTRE SECURITE ET LIBERTE

Internet est devenu un outil indispensable pour les entreprises. Mais que ce soit Facebook pour les ressources humaines ou Twitter pour les relations publiques, il n'y a pas de compromis à faire entre liberté d'accès et sécurité.

Une bonne solution de sécurité doit permettre d'accéder aux sites dont vos utilisateurs ont besoin dans le cadre de leur travail, tout en maintenant l'entreprise sécurisée.

Même quand l'entreprise décide d'appliquer des restrictions sur les types de sites accessibles, il faut toujours garder à l'esprit que pour les utilisateurs, la première des libertés consiste à pouvoir naviguer sur le Web en toute sécurité.

CONCLUSION

Comme dans tous les autres domaines de la sécurité informatique, l'éducation des utilisateurs représente la première protection contre les menaces. A ce titre, il est essentiel que les internautes prennent pleinement conscience des dangers qui les guettent, afin de se tenir sur leurs gardes et de ne pas se précipiter dans les pièges, parfois grossiers, qui leur sont tendus.

Il est également bon de rappeler la nécessité d'une bonne hygiène de son ordinateur, qui commence par l'installation régulière des derniers correctifs de sécurité, aussi bien sur le système d'exploitation que sur les applications Web, et par la mise en place d'une protection anti-malware parfaitement mise à jour, qui bénéficie si possible d'une fonction de blocage de l'accès aux pages Web malveillantes. En entreprise, cette protection sur les postes de travail sera en outre complétée par une protection au niveau de la passerelle Internet.

MYTHES ET LEGENDES DE L'IDENTITE NUMERIQUE PARTIE 1

Philippe Vacheyrout, CAPUCINE

La notion d'identité numérique apparait dans la loi Informatique fichiers et liberté de 1978 et le concept s'est imposé progressivement au fil des pratiques d'identification et d'authentification, notamment dans le cadre des procédures administratives et de la mise au point de processus de signature numérique.

Par ailleurs, l'utilisation du Web dans une perspective participative, le développement des réseaux sociaux ont permis l'émergence d'autres problématiques qui y sont liées.

On en arrive donc à l'utilisation du même terme dans deux contextes différents :

- L'identité numérique perçue en termes d'image de l'individu au sens social du terme, c'est-à-dire l'e-réputation.
- L'identité numérique en tant que support de procédures légales, recouvrant la notion d'identification et de possibilité d'authentification de documents à valeur probante, reliés à l'identité au sens légal du terme (authenticité). C'est dans ce sens là que nous l'envisagerons sous le terme de Cyber Identité en liaison avec les labels SuisseID, IDéNum et les cartes Nationales d'Identités Electroniques.

Techniquement, l'identité numérique se définit comme un « lien technologique entre une entité réelle et une entité virtuelle ». (voir Wikipedia)

MYTHE N° 1 : L'IDENTITE NUMERIQUE EST UNIQUE :

Ceci est à la fois vrai et faux.

L'entité réelle en cause étant l'individu, elle est unique malgré la diversité des moyens employés pour l'authentifier. Par contre, l'entité virtuelle, en tant que profil utilisateur (Avatar) : national, familial, professionnel, médical, juridique, consommateur, etc. - est multiple avec les données qui s'y attachent et qui ne sont pas nécessairement toutes les mêmes. Dans les deux cas l'individu doit pouvoir bénéficier de l'application de la loi Informatique et liberté et des recommandations diverses qui l'accompagnent :

- Anonymat
- Droit à l'oubli
- Protection des données personnelles
- Propriété intellectuelle
- Traçabilité des données
- Maitrise de son Identité Numérique au niveau international

En ce qui concerne les dispositifs, divers processus, méthodes, sont possibles. Plusieurs niveaux de certification existent, les autorités de certifications peuvent être privées ou publiques. Il en résulte une multitude de moyens et même de façons d'en aborder le concept.

En ce sens il est possible de parler de multiplicité des identités virtuelles, du simple pseudonyme à usage ciblé à l'identité certifiée à travers un acte authentique

Il en est de même des procédés, du couple login/ mot de passe au système basé sur des données biométriques dont le plus extrême serait l'ADN, en passant par les systèmes de certificats. Il convient de protéger cet identifiant par les dispositifs disponibles sur le marche (PKI, IGCP 2.0, OTP, SSO, Token etc.)

MYTHE N° 2 :
L'IDENTITE NUMERIQUE RELEVE DE L'AUTORITE REGALIENNE.

Les gouvernements délèguent à des tiers certificateurs le soin d'établir l'identité nationale par le biais d'une identité numérique (Carte bancaire, clé USB, mot de passe dynamique etc…)

De plus toute identité numérique n'est pas utilisée dans un cadre nécessitant une identification certaine (Cartes prépayées)

Il est possible de mettre en place des «cyber- identités » destinées à retracer une activité tout en permettant un certain anonymat – sous réserve des possibilités d'identification dans un cadre règlementé, par exemple à travers la possibilité d'indiquer simplement l'hébergeur dans le cas de blogs individuels. Cette Cyber Identité permet à l'utilisateur de conserver l'anonymat, assurer la protection de ses données personnelles et de préserver la propriété intellectuelle, mais elle n'est pas dépendante de l'autorité régalienne.

MYTHE N° 3 :
IDENTIFICATION ET AUTHENTIFICATION C'EST PAREIL.

L'identification repose sur les informations associées à un objet ou un humain dans un contexte donné pour le distinguer. Il s'agit de disposer des informations nécessaires pour déterminer que l'individu est bien, selon les données que l'on possède, celui qu'il prétend être. Elle s'applique à l'individu.

L'authentification consiste à s'assurer de l'authenticité, l'intégrité et la non-répudiation des informations fournies. Il peut s'agir des informations fournies pour l'identification ou de tout autre processus ou document. Elle s'applique à l'objet et non à l'individu.

MYTHE N° 4 :
LA SECURITE EST GARANTIE PAR LES REFERENTIELS DE SECURISATION ET D'INTEROPERABILITE (RGS [25]- RGI [26])

Selon le Référentiel Général de Sécurité :

« L'objectif du RGS n'est pas d'imposer une technologie, une architecture ou une solution technique, ni même les fonctions se sécurité décrites dans le RGS »

Le socle de sécurisation IAS (Identification, Authentification, Signature) sur lequel s'appuient les rapports de certification [27] pour les Carte d'Identité Électronique ne peut pas fonctionner, dans la mesure où les identifiants biométriques sont des données statiques numérisables et

[25] *Le référentiel RGS peut être trouvé sur le site : http://www.ssi.gouv.fr/IMG/pdf/RGSv1-0.pdf*

[26] *Voir le référentiel sur le site : https://www.ateliers.modernisation.gouv.fr/ministeres/domaines_d_expertise/architecture_fonctio/public/rgi/referentiel_general1617/downloadFile/file/Referentiel%20General%20Interoperabilite%20Volet%20Technique%20V0.90.pdf*

[27] *Voir sur le site du gouvernement : http://www.ssi.gouv.fr/IMG/certificat/anssi-cc_2009-56fr.pdf*

reproductibles. Il est donc possible, partant d'une fausse identité authentifiée, d'aboutir à une signature techniquement valide mais fausse.

En inversant les deux facteurs, le socle AIS permet à l'utilisateur de délivrer son identité dans un environnement authentifie avec une adresse ID (label IDéNum [28] pour la France) constituant un intranet ou réseau de confiance numérique qui rejoint le post-IP et la proposition de John DAY en y associant l'ID (SuisseID, IDéNum, CapucineID etc .). Ce dernier est compatible avec le RGS puisqu'il est précisé :

« En revanche lorsqu'une autorité de certification juge nécessaire, à l'issue d'une analyse de risque, de mettre en œuvre les fonctions de sécurité qui sont prévues dans le RGS, elle doit alors respecter les règles correspondantes ».

MYTHE N° 5 : LA GOUVERNANCE D'INTERNET RELEVE D'UNE ORGANISATION CENTRALISEE

La Gouvernance d'Internet ne se limite pas à une question d'adressage et la gestion des noms de domaine. L'objet de l'ICANN précise « Les autres questions concernant les internautes, telles que les règles relatives aux transactions financières, les contrôles de contenus sur l'Internet, les messages électroniques à caractère commercial non sollicité (*spam*) et la protection des données n'entrent pas dans le cadre des responsabilités de coordination technique de l'ICANN »

Les autres questions relèvent donc des Internautes, en complément du réseau constitué par la gestion des DNS avec des adresses IP il convient de créer un réseau de fédération d'Identité à l'instar de Shibboleth (qui est un mécanisme de propagation d'identités, développé par le consortium Internet [29], qui regroupe 207 universités et centres de recherches). Cette notion associée avec des adresses ID, à l'instar d'un réseau OpenID+ sécurisé, associés aux réseaux des Internets, pourrait constituer une gouvernance d'Internet qui relèverait alors de plusieurs organisations centralisées sur la base de « critères communs » évoqués précédemment, définis dans le Web sémantique.

Il revient donc à chaque usager de s'assurer du bon usage des TIC en réseau sécurisé pour participer à la gouvernance mondiale dans le cadre du Forum pour la Gouvernance d'Internet [30] et construire la Société de l'Information du XXIème siècle, en tirant parti des Technologie du Relationnel notamment avec les environnements 3D, pour partir de la réalité augmentée, vers un futur augmenté.

EN CONCLUSION : INTERNET EST LA PIRE ET LA MEILLEURE DES CHOSES

Cette formule fourre-tout n'est pas un argument mais est largement utilisée par les détracteurs d'Internet. Une formule ne fait pas la réalité et, si nous avons pu observer ce que pouvaient être les pires facettes d'Internet, à l'instar du « Le meilleur des mondes [31]» de Aldous Huxley. Reste à expérimenter ce que pourrait être un monde meilleur entre le « Big

[28] *Voir annonce IDéNum : http://www.gouvernement.fr/gouvernement/label-idenum-plus-de-securite-et-plus-de-facilite-pour-l-usage-des-services-sur-interne*

[29] *Voir la définition de ce concept sur Wikipédia sur http://fr.wikipedia.org/wiki/Internet2*

[30] *Site du Forum : http://www.intgovforum.org/cms*

[31] *Voir la page de Wikipedia http://fr.wikipedia.org/wiki/Le_Meilleur_des_mondes*

Brother » de George Orwell [32] et la « Big Society » de David Cameron , le premier ministre britannique, pour mieux responsabiliser les citoyens dans les collectivités locales afin de construire un réseau vertueux d'économie sociale et solidaire avec une démarche d'entrepreneuriat social, pour un développement soutenable.

[32] *Pour en savoir plus, voir la page de Wikipedia : http://fr.wikipedia.org/wiki/George_Orwell*

MYTHES ET LEGENDES DE L'IDENTITE NUMERIQUE PARTIE 2

Fabrice Mattatia,
Ancien responsable technique du programme de protection de l'identité au ministère de l'intérieur,
Concepteur du projet Idénum

Fondamentalement, l'identité d'une personne n'est pas définie en droit français. Le décret du 6 fructidor an II prescrit que chaque citoyen doit porter les noms et prénoms inscrits sur son acte de naissance. Mais l'identité ne peut se restreindre à ces éléments, car certaines personnes sont homonymes de nom, de prénoms, et même, c'est moins courant mais cela s'est vu, de date et de commune de naissance. On considère alors, de manière usuelle, que l'identité d'une personne consiste en ses nom, prénoms, date et lieu de naissance, ainsi qu'en sa filiation (les mêmes éléments pour ses parents).

Dans ces conditions, parler d'*identité numérique* ou d'*identité électronique* relève forcément d'un abus de langage. Cette expression entraîne de surcroît des confusions, car selon les auteurs elle recouvre deux réalités différentes :

- au sens large, l' « identité numérique » désigne l'image que l'individu donne de lui-même sur internet. Chacun a le droit d'utiliser des pseudonymes sur le web, et donc de se construire autant d'identités numériques qu'il a d'avatars.
- au sens régalien, on peut trouver le terme « identité numérique » utilisé par métonymie pour exprimer un « moyen numérique de preuve de l'identité ». Cette preuve peut servir uniquement dans le monde réel (par exemple un passeport électronique), ou bien servir aussi à prouver l'identité sur internet.

MYTHE N° 1 : L'IDENTITE NUMERIQUE EST UNIQUE

Tout dépend de ce que l'on entend par « identité numérique ». S'il s'agit des avatars sur internet, ils ne sont évidemment pas uniques. S'il s'agit de la preuve électronique de sa vraie identité, les moyens de preuve peuvent eux aussi être multiples, mais ils se rattachent tous à la même identité réelle. Par exemple, un passeport électronique et une carte d'identité électronique sont deux preuves numériques distinctes de la même identité dans la vie réelle. Deux certificats électroniques émis par deux tiers de confiance différents sont deux preuves de l'identité utilisables sur internet.

MYTHE N° 2 : IDENTITE, ANONYMAT ET DROIT A L'OUBLI SONT DES CONCEPTS OPPOSES

Au contraire, ces concepts sont complémentaires. Il y a des situations où l'anonymat ou le recours à un pseudonyme sont légitimes : la consultation d'informations, les jeux, la participation à des forums de discussion… Inversement, dans certains cas il serait absurde d'invoquer le droit à l'anonymat ou au pseudonymat : par exemple la consultation de son dossier médical, l'accès à son compte bancaire, la signature de contrats ou la souscription de produits… toutes situations où une garantie forte de l'identité réelle de la personne est indispensable, aussi bien dans la vie courante que sur internet.

Quant au droit à l'oubli, il n'existe pas en tant que tel. Il s'agit d'une appellation « marketing » du droit d'opposition instauré par la loi Informatique et Libertés pour certains cas de traitements de données personnelles. Pour exercer ce droit à l'effacement de ses données, il faut d'ailleurs prouver son identité, pour montrer qu'on est bien la personne concernée ! Remarquons à ce propos que la loi Informatique et Libertés ne contient aucune disposition concernant l' « identité numérique », elle ne mentionne que « l'identité humaine » (notion floue et déclamatoire qui recueille la désapprobation des juristes) et « l'identité » tout court (pour faire valoir ses droits).

MYTHE N° 3 :
L'IDENTITE NUMERIQUE RELEVE DE L'ETAT

Si l'on fait référence aux passeports et cartes d'identité, c'est évident.

Si l' « identité numérique » signifie les moyens de preuve d'identité sur internet, ce n'est plus obligatoirement vrai. L'Etat peut fournir de telles preuves, par exemple en implantant des certificats dans des cartes d'identité électroniques, comme le font la Belgique, l'Estonie, l'Espagne, le Portugal, la Finlande, l'Italie, la Suède, la Lituanie… et Monaco[33]. Les internautes peuvent également se les procurer auprès de tiers de confiance privés, comme en Finlande, en Suède, en Italie, en Autriche… Dans ce dernier cas, l'Etat peut créer un label garantissant le niveau de sécurité des tiers de confiance. Des opérateurs suisses ont ainsi commercialisé en 2010 des certificats basés sur le label SuisseID du gouvernement fédéral helvétique. Le projet français de label Idénum repose sur le même principe.

MYTHE N° 4 :
IDENTIFICATION ET AUTHENTIFICATION C'EST PAREIL

De manière usuelle, on utilise ces termes avec les significations suivantes :

- identifier, c'est annoncer une identité ;
- authentifier, c'est la prouver.

Mais il arrive que le terme « identification » soit utilisé pour couvrir les deux significations. En effet, le terme « authentification » est mal compris aussi bien du grand public que des juristes, pour lesquels il fait plutôt référence à la notion, totalement différente, d' « acte authentique ».

MYTHE N° 5 :
IDENUM EST UN CONCURRENT DE LA CARTE D'IDENTITE ELECTRONIQUE

Il s'agit en fait de deux projets français complémentaires pour fournir aux internautes des preuves d'identité électroniques.

Le projet de carte d'identité électronique, au format carte à puce et comportant des biclés et des certificats d'authentification et de signature, a été lancé par le ministère de l'intérieur. Un projet de loi sur le sujet, qui a connu plusieurs versions depuis 2005, est toujours en attente d'examen devant le parlement.

[33] *Pour plus de détails, on consultera :*
Fabrice Mattatia, "An Overview of Some Electronic Identification Use Cases in Europe", in Practical studies in e-government*, S. Assar, I. Boughzala et I. Boydens (dir), Springer, 2011.*

Idénum est un projet de label, lancé en 2010 par la secrétaire d'Etat à l'économie numérique, visant à garantir le niveau de sécurité des biclés et des certificats d'authentification et de signature émis par des acteurs privés. Ces outils seront disponibles sur différents supports adaptés à la navigation mobile, comme des clés USB cryptographiques ou des cartes SIM. Le cahier des charges d'Idénum repose notamment sur le référentiel général de sécurité (RGS) de l'administration, publié en 2010. Idénum n'utilise pas la biométrie ; comme pour la carte bancaire, l'usage des clés privées est conditionné à la possession d'un objet (le support cryptographique) et à la connaissance d'un code secret.

Idénum et la carte d'identité électronique utilisent les mêmes standards. Un internaute pourra détenir une carte d'identité et un ou plusieurs outils Idénum de différents fournisseurs, et les utiliser indifféremment, tous offrant le même niveau de garantie. Il choisira ainsi celui qui a le support le plus pratique pour chaque circonstance, ou celui émanant de l'émetteur auquel il préfère avoir recours pour chaque authentification ou signature.

MYTHES ET LEGENDES DE L'IDENTITE NUMERIQUE PARTIE 3

Jean-Yves Gresser

Au 19e siècle, Condorcet définit l'identité comme le fondement du contrat social entre l'individu et l'État. Mais l'identité d'une personne n'est toujours pas définie en droit français.

La notion d'identité numérique apparait dans la loi Informatique fichiers et liberté de 1978 et le concept s'est imposé progressivement au fil des pratiques d'identification et d'authentification, notamment dans le cadre des procédures administratives et de la mise au point de processus de signature numérique.

Par ailleurs, l'utilisation de la toile dans une perspective participative, le développement des réseaux sociaux ont permis l'émergence d'autres problématiques qui y sont liées.

On en arrive donc à l'utilisation du même terme dans deux contextes différents :

- l'identité numérique perçue en termes d'image de l'individu au sens social du terme,
- l'identité numérique en tant que support de procédures administratives ou commerciales.

MYTHE N° 1 :
UN IDENTIFIANT ET UNE IDENTITE NUMERIQUE, C'EST LA MEME CHOSE

D'une manière générale, une *identité* est un ensemble de *propriétés* qui vont permettre à une personne ou une machine de reconnaître une autre personne, un objet ou une autre machine en la distinguant d'une personne, d'un objet ou d'une machine semblable.

Dans le monde numérique, il existe de multiples définitions du mot *identité* [34]. Une *identité numérique* est la représentation de cet ensemble de propriétés en un format assimilable par un ordinateur. Alors que les propriétés « appartiennent » à l'entité à laquelle elles se réfèrent, la représentation – on parle alors d'*attribut*[35] - passe par un *fournisseur d'identité*. Ce fournisseur peut être l'État ou un des ses représentants, administratif ou technique.

En bref, dans ce monde une même personne peut, de manière pratique, se voir dotée de plusieurs identités (voir mythe no 2).

Un *identifiant*[36] est un groupe de caractères (au sens typographique) permettant d'identifier ou de désigner des données, le cas échéant de préciser certaines de leurs propriétés (ISO 2382/IV). Un numéro de sécurité social ou un numéro SIREN d'entreprise sont des identifiants.

D'un point de vue pratique, un ensemble d'attributs peut être condensé en un seul identifiant, comme sur un passeport ou une carte d'identité. Le mot identité devient alors synonyme d'identifiant. Malgré cela il subsiste une différence majeure entre les deux. Un

[34] *Voir l'annexe A du document précité et la partie relative aux identités de J.-Yves Gresser, juin 2010, Draft Ontology Of Financial Risks & Dependencies Within & Outside The Financial Sector, Vol. 2 Glossaries, J.-Yves Gresser, juin 2010, 104 pages*

[35] *Un attribut est une « Information concernant un objet géré, utilisée pour décrire tout ou partie de cet objet. L'information se constitue d'un type d'attribut et de la valeur d'attribut correspondante qui peut être une valeur simple ou multiple. » (Source IUT- [X.790])*

[36] *L'Académie préfère* identificateur, *mieux formé, mais l'usage penche nettement en faveur d'identifiant.*

identifiant peut-être ou non décomposable en ses éléments constitutifs, une identité doit toujours l'être.

MYTHE N° 2 :
UNE IDENTITE NUMERIQUE ET UN CERTIFICAT NUMERIQUE, C'EST LA MEME CHOSE

Un *certificat numérique* est un objet informatique, un ensemble de données, fourni par un prestataire aux utilisateurs potentiels d'un service (fourni par un autre prestataire) pour leur permettre d'accéder à ce service dans des conditions jugées acceptables par l'ensemble des parties prenantes : prestataire principal, partenaires, autres utilisateurs, services de paiement associés, assureur, administration fiscale etc.

Un tel certificat peut comprendre :

- des éléments d'identifications des parties prenantes,
- des attributs relatifs aux droits et diligences des parties prenantes,
- des éléments qualifiant la robustesse du certificat, notamment celle des codes sécuritaires ayant servi à sa fabrication.

Dans le monde numérique l'expression *identité numérique*, raccourcie en *identité* désigne souvent ce genre de certificat.

Dans la plupart des contextes pratiques, cela ne prête pas à confusion mais il faut se rappeler qu'un certificat est produit dans l'optique d'une utilisation ou d'une famille d'utilisations déterminées. Ces utilisations reposent sur 4 types de processus :

- *identification,*
- *authentification,*
- *habilitation,*
- *autorisation (ou validation)*

MYTHE N° 3 :
L'IDENTITE NUMERIQUE EST UNIQUE

Au vu de ce qui précède la notion d'identité unique, au sens de clé d'accès à toutes les applications imaginables, est une vue de l'esprit qui ne peut avoir aucune portée pratique.

Un certificat électronique qui est calculé à partir d'un nombre fini d'attributs de cette entité. L'unicité est liée au choix et à la caractérisation (mode de représentation de ces attributs), au mode de calcul, aux entités chargées de la collecte de l'information, de l'élaboration du certificat.

Cela n'exclut pas que certains certificats aient une large portée. Mais cela tient d'abord à la *robustesse* de ces certificats et, à la *garantie* qui leur est attachée. Cette robustesse est liée à la robustesse des processus mis en place jusqu'à la diffusion et l'utilisation du certificat.

L'unicité est au cœur d'une série de paradoxes relevé lors des rencontres d'Autrans en 2006 :

- l'identité peut être anonyme,
- l'identité seule ne sert à rien, elle est vecteur d'échanges, elle appartient à une chaîne,
- l'identité peut être inconnue de son propriétaire,
- l'identité peut être contre-productive de confiance,
- une identité peut en cacher une autre,
- la force de l'identification proportionnelle au risque,

- une identité est concurrente d'une autre.

MYTHE N° 4 :
L'IDENTITE NUMERIQUE RELEVE DE L'AUTORITE REGALIENNE.

Il peut exister DES identités numériques relevant de l'État.

Le problème majeur est l'irresponsabilité juridique de l'État (de tout État) relative aux actes pouvant s'appuyer sur une telle identité.

LA *cyberidentité* étatique universelle est une vue de l'esprit. Par contre, l'État peut fournir un cadre juridique général incluant certification et labellisation… et, pour ses propres activités, technique.

MYTHE N° 5 :
IDENTIFICATION ET AUTHENTIFICATION C'EST PAREIL

Dans le contexte des identités numériques, *identifier* a deux sens. Il peut désigner :

- le processus par lequel une identité est attribuée à une entité (personne, objet, machine),
- la « visualisation » d'une identité, c'est à dire l'affichage des attributs ou propriétés identitaires d'une entité.

Une identité peut être ou non *authentifiée*. *L'authentification* est un processus ou le résultat d'un processus par lequel la véracité de l'identité d'une entité peut être prouvée ou sinon confortée. L'authentification donne à cette entité la capacité d'effectuer ou non certaines transactions. Ce processus est le fondement de la confiance sur l'internet. Il va de pair avec deux autres processus :

- *l'habilitation*, qui consiste à donner des droits, droit d'accès ou droit d'effectuer certaines tâches à une entité,
- *l'autorisation* ou la *validation*, qui donne au détenteur d'un droit la possibilité effective d'exercer ce droit.

NB La notion *d'acte authentique* est une notion purement juridique qui n'a pas de rapport direct avec la notion d'authentification.

MYTHE N° 6 :
ON PEUT MAITRISER SON IDENTITE SUR L'INTERNET.

Revenons un moment sur un des sens profond d'identité dans le monde numérique et qui a peu à voir avec la notion de certificat. C'est ce que certains désigne par le mot *persona* ou plus prosaïquement par *trace(s)*.

En fait, les sens sont légèrement différents. La *personne numérique* est pour certains l'ensemble des informations glanées sur la toile et censée représenter une personne physique de manière fidèle (et sincère).

Cela commence par la collecte de renseignements de toute nature, tirés de documents ou de messages échangés et qui sont publiquement accessibles sur des serveurs de toute nature, les traces.

Le problème est qu'à partir du moment où une information est numérisée et accessible, elle est indéfiniment reproductible et transportable. Quel que soit le dispositif de contrôle

d'affichage, d'impression etc. mis en place celui-ci peut être contourné. Certes plus ou moins facilement, mais il l'est toujours pour qui veut bien s'en donner la peine !

Se constituer un espace privé à côté d'un espace public est ainsi impossible même en utilisant des pseudonymes différents. Les moyens de recoupement existent toujours.

Le meilleur moyen pour qu'une donnée reste privée c'est de ne pas la publier du tout. Est-ce réaliste ?

NB Cette problématique concerne aussi toute identité numérique. Il ne peut pas en exister d'infalsifiable. Il serait donc dangereux d'essayer attribuer à une personne une identité unique et univoque. Que ferait cette personne en cas de vol ou d'usurpation ?

MYTHE N° 7 :
UNE IDENTITE NUMERIQUE EST TOUJOURS UN FACTEUR DE CONFIANCE.

En fait l'identité peut être contreproductive de confiance.

L'usage de méthodes propriétaires et secrètes ne permet pas d'évaluer correctement le niveau de sécurité de toute identité.

De plus, la gestion des identités et des certificats donne aux gestionnaires un pouvoir de surveillance et de connaissance des activités de leurs clients. La mainmise sur cette gestion par des sociétés hors contrôle des utilisateurs est une porte ouverte aux conflits d'intérêts, aux abus de dominance, et aux usages détournés d'informations confidentielles.

À grande échelle, c'est une dérive vers une tutelle économique et politique par des groupes hors d'atteinte juridique et prédateurs.

MYTHE N° 8 :
POUR ECHANGER DE MANIERE SURE SUR L'INTERNET IL SUFFIT DE PRESENTER UNE IDENTITE NUMERIQUE SUFFISAMMENT ROBUSTE.

L'identité seule ne sert à rien, elle est seulement un élément d'accès dans une *chaîne* plus ou moins complexe et plus ou moins étendue.

Dès qu'un échange est porteur de valeur, une simple identité ne suffit pas. Un processus d'authentification courant requiert un identifiant et un mot de passe. Une authentification à 2 facteurs va réclamer la fourniture d'informations concordantes via deux canaux différents. Une *preuve de présence* peut être demandée.

Une chaîne implique l'*interopérabilité* de processus mis en œuvre par plusieurs acteurs et celles des identités manipulées.

Les acteurs peuvent relever ou non du même espace géographique, juridique ou technique.

Les processus de certification ou de labellisation des identités sont souvent limités à un État. Les référentiels transnationaux sont encore rares tout comme les organismes capables de les faire respecter.

MYTHES ET LEGENDES DES SYSTEMES DE CLOUD

Professeur Jean-Pierre Cabanel, INP / ENSEEIHT, membre de l'IRIT
Professeur Daniel Hagimont, INP / ENSEEIHT, membre de l'IRIT

Face à l'augmentation continuelle des coûts de mise en place et de maintenance des systèmes informatiques, les entreprises externalisent de plus en plus leurs services informatiques et confient leur gestion à des entreprises spécialisées (que nous appelons fournisseurs). L'intérêt principal réside dans le fait que le client de ces fournisseurs ne paie que pour les services effectivement consommés, alors qu'une gestion de ces services par le client ne serait pas complètement amortie, en particulier lorsque les besoins du client varient. Le « Cloud Computing » se situe dans cette orientation récente.

Devant le manque de consensus sur la définition de la notion de « Cloud Computing », reprenons celle de CISCO : "Cloud Computing is an IT ressources and services that are abstracted from the underlying infrastructure and provided on-demand and at scale in a multitenant environment".

Il s'agit donc de fournir aux clients (des entreprises) des services à la demande, illusion de l'infinité des ressources et enfin d'utiliser les mêmes ressources (mutualisation) pour tous les clients.

Cette stratégie offre plusieurs avantages parmi lesquels :

- Réduction des coûts pour le client. Il n'a plus besoin de gérer sa propre infrastructure et il est facturé en fonction de l'utilisation des services du Cloud.
- Flexibilité pour le client. Il peut augmenter la capacité de son infrastructure sans investissements majeurs, les ressources du Cloud étant allouées dynamiquement à la demande.
- Moins de gaspillage. Les infrastructures gérées chez les clients sont souvent sous-utilisées, alors que l'infrastructure d'un Cloud mutualise un ensemble de ressources pour un grand nombre de clients, ce qui permet d'augmenter le taux moyen d'utilisation des ressources.

Un exemple privilégié de mesure de ce gaspillage est la consommation électrique des infrastructures.

MYTHE N° 1 :
LE CLOUD EST JUSTE CE QU'ON APPELAIT AVANT LE "TIME SHARING" : LES APPLICATIONS NE SONT PLUS HEBERGEES CHEZ SOI ET ON NE PAYE QUE CE QUE L'ON CONSOMME

Le Cloud, c'est un peu plus compliqué. Les utilisateurs potentiels d'un Cloud se regroupent en 3 catégories : administrateur du Cloud, administrateur du client et utilisateur final.

L'administrateur du Cloud est responsable de l'administration des ressources matérielles et logicielles du Cloud. Il est notamment responsable de la gestion de la capacité d'hébergement du Cloud. Le Cloud doit donc fournir à son administrateur des services d'administration lui permettant de gérer les ressources matérielles et logicielles mises à disposition des clients.

Quant à l'administrateur du client, il utilise les ressources fournies par le « Cloud « pour gérer les applications finales du client. Il n'a pas une vue globale de l'environnement du Cloud,

mais seulement des ressources mises à la disposition du client et des applications gérées avec ces ressources.

En fonction du niveau de service fourni par le Cloud, on identifie 3 scénarios d'utilisation du Cloud :

- **Infrastructure as a Service (IaaS)** : Il s'agit du niveau le plus bas. Le Cloud fournit des ressources matérielles à ses clients (capacité de traitement, de stockage ...). Ces ressources matérielles peuvent être fournies directement au client (l'unité d'allocation est alors généralement une machine équipée d'un système d'exploitation) ou être virtualisées (l'unité d'allocation est alors généralement une machine virtuelle, plusieurs machines virtuelles pouvant s'exécuter sur une même machine physique) pour une gestion plus fine des ressources physiques. Pour ce niveau, le Cloud fournit un ensemble d'API permettant à l'administrateur du client d'utiliser un ensemble de ressources. L'administrateur du client a alors la responsabilité d'utiliser ces ressources (machines physiques ou virtuelles) pour y installer et gérer les applications utilisées par le client.
- **Platform as a Service (PaaS) :** Il s'agit d'un niveau intermédiaire dans lequel le Cloud ne fournit pas que des machines et leurs systèmes d'exploitation, mais également des logiciels appelés plateformes applicatives. Ces plateformes sont des environnements d'exécution pour les applications finales comme par exemple : les serveurs d'applications dans une architecture JEE. Ces plateformes applicatives sont maintenues par l'administrateur du Cloud, mais l'administrateur du client a la charge d'administrer les applications finales du client sur ces plateformes applicatives.
- **Software as a Service (SaaS)** : Il s'agit du niveau le plus haut dans lequel le Cloud fournit directement les applications finales à ses clients. L'administrateur du Cloud administre les applications finales et le rôle de l'administrateur du client est quasiment nul. Il est important de souligner qu'un Cloud de niveau SaaS peut être implanté par un acteur en s'appuyant sur un Cloud de niveau PaaS géré par un autre acteur, lui même implanté sur un Cloud IaaS.

MYTHE N° 2 : LE CLOUD COMPUTING EST UNE REVOLUTION TECHNOLOGIQUE

On peut penser que le « Cloud Computing » est une révolution technologique, mais non, c'est une orientation vers un mode de gestion des infrastructures informatiques des entreprises.

En adoptant cette orientation, on retrouve tout les problèmes classiquement adressés dans les infrastructures actuelles, et notamment :

- **La tolérance aux pannes**. Un service géré dans un Cloud soit tolérer les pannes dans le sens où il faut assurer la cohérence de l'état du service en cas de panne ainsi que sa disponibilité pour les usagers. La disponibilité peut être plus difficile à assurer du fait que les services sont déportés dans le Cloud et qu'une indisponibilité de la connexion entre le client et le Cloud peut lourdement affecter la disponibilité du service.
- **La sécurité.** Un service géré dans un Cloud doit résister à des utilisations malveillantes. La sécurité peut être délicate à assurer du fait que le Cloud peut héberger des applications pour le compte de différents utilisateurs (ce qui n'est pas le cas pour une infrastructure interne à l'entreprise cliente). De plus, l'utilisation d'un service

nécessite une communication entre le client et le Cloud, ce qui peut constituer un talon d'Achille pour la sécurité.

- **L'interopérabilité et la portabilité.** Les clients des « Clouds » auront vite envie de pouvoir migrer des services d'un Cloud à un autre, ce qui nécessitera l'établissement de standards permettant de tels échanges.

Un problème apparaît toutefois plus crucial dans le domaine du Cloud Computing. Comme on l'a vu précédemment, l'organisation d'un Cloud implique deux administrateurs : l'administrateur du Cloud et l'administrateur du client. L'administrateur du Cloud doit déployer des logiciels (systèmes d'exploitation, machines virtuelles, plateformes applicatives ou logiciels pour l'utilisateur final) sur des machines physiques et les gérer à l'exécution (migration, répartition de la charge) afin d'assurer la qualité de service à ses clients.

L'administrateur du client doit effectuer les mêmes tâches d'administration dans le cas des scenarios PaaS et IaaS. Ces tâches d'administration ne peuvent être effectuées manuellement et une tendance générale est de fournir des environnements d'administration autonomes visant à automatiser au maximum ces tâches (on parle également plus généralement « d'autonomic computing ». Ces environnements d'administration autonome fournissent des formalismes permettant de décrire les actions à effectuer pour déployer des applications et les reconfigurer dynamiquement pour prendre en compte les conditions à l'exécution.

Il existe principalement trois types de système de Cloud et les problèmes de sécurité sont différents suivant la structure utilisée.

1. **Les systèmes privés** propres à un grand compte, avec si nécessaire quelques sous-traitants
2. **Les systèmes partagés** par plusieurs grands comptes
3. **Les systèmes publics**, ouverts à tout le monde

Un système de type Cloud se décompose en plusieurs parties :

- Des postes clients indépendants
- Un système de communication entre le poste client et le système.
- Des bâtiments qui abritent les ordinateurs Cloud
- Des ordinateurs, systèmes d'exploitation et logiciels du Cloud

Chacun des ces éléments est un des maillons de la chaine sécuritaire du système et impacte sur les paramètres suivants :

- Confidentialité
- Authentification
- Déni de service
- Pollution, destruction

La problématique de la sécurité d'un système de Cloud relève d'une tache ardue, et les protections envisagées vont diminuer la potentialité de généralisation d'utilisation de Cloud multiples pour un même client.

De manière induite, la problématique juridique est, elle aussi, très difficile : Qui va être responsable des aléas direct ou indirect qui surviendront ? Comment obtenir la réalité sur les causes des situations ?

Il y a quelques années, les constructeurs de « main frame », DEC, BULL, IBM etc., exploitaient des systèmes identiques au Cloud avec sur le plan sécuritaire plusieurs différences essentielles :

- Très souvent, les clients du point central, appartenaient à une même entité juridique: une banque, une industrie etc.
- Les systèmes de communications utilisés n'étaient pas l'Internet, ils permettaient un contrôle suffisant : lignes et réseaux spécifiques et propriétaires.
- La protection des ressources et la recherche des causes d'aléas étaient simplifiées, une seule entité juridique cliente et des systèmes de communication propriétaires des fournisseurs de « Main Frame » ou centre de ressources informatiques.

La nouvelle approche, modifie l'environnement précédemment présenté : clients avec des entités juridiques multiples, même si ces clients sont connus et identifiables à priori, et utilisation de moyens de communication ouverts et incontrôlables : l'Internet.

MYTHE N° 3 : LE CLOUD PRIVE D'UN GRAND COMPTE EST COMPLETEMENT SECURISE

Dans les systèmes privés propriétaires d'un grand compte, ce type d'utilisation (très proche des PKI intra entreprise), le système est installé sur le site de l'entreprise et les risques sécuritaires sont minimisés. Ils relèvent de la protection des communications dans l'entreprise (internationales) et du contrôle des personnes et des systèmes dédiés au Cloud. Le responsable vis-à-vis des utilisateurs est alors le service informatique qui gère les services de Cloud. Sommes-nous face à un système qui possède un haut niveau de sécurité ?

Et bien cela n'est pas si clair, il est encore nécessaire de contrôler, les chemins utilisés par l'information afin que des copies illicites ne soient réalisées, de s'assurer de la pérennité du fournisseur du service, afin de ne pas perdre de l'information et ainsi désorganiser l'entreprise, contrôler les communications, etc.

Avec les systèmes réservés à plusieurs grands comptes, nous sommes en présence de la structure la plus exposée aux problèmes sécuritaires. En effet le site physique du Cloud n'est pas sous contrôle de l'entreprise mais contient des informations confidentielles de plusieurs entreprises.

MYTHE N° 4 : LES INFORMATIONS STOCKEES SUR UN CLOUD PARTAGE SONT PROTEGEES, PAR CONTRAT, DES VIRUS, VERS ET AUTRES ATTAQUES

Les postes clients du système Cloud, utilisent sûrement des supports magnétiques amovibles, (il existe très peu d'application fermée) ou bien le poste client est utilisé pour d'autres travaux, ou dans le cas pire, le poste client est connecté à l'Internet de temps en temps.

Pensez-vous alors que les filtres anti virus du Cloud vont protéger les informations des entreprises clientes ? Et bien non ! En réalité ces filtres possèdent une efficacité toute relative et cela conduit au risque de pollution du Cloud par les virus et autres programmes malveillants positionnés par un client et ainsi polluer ou détruire des informations des entreprises clientes du Cloud

Vous imaginez peut-être, que les données des entreprises peuvent être séparées physiquement sur des machines différentes avec des accès réseaux différents ? Et bien non ! La réalité économique de ces systèmes oblige à mettre en commun les ressources afin de diminuer les coûts pour les clients.

Un fournisseur de systèmes de Cloud peut-il garantir par contrat la non destruction ou pollution des données stockées ? Les notions de virus et vers sont elles assimilées aux forces

majeures : nature, guerre etc. ? La pérennité du fournisseur est-elle prise en compte par des clauses spécifiques ? Il semble que si l'on désire garder des coûts acceptables de service de Cloud, il soit très difficile de garantir de telles contraintes.

Pensez vous qu'il est possible, de détecter le client responsable d'une pollution ? Quelles sont les responsabilités partagées du Cloud et du client pollueur ?

Dans un environnement semi ouvert (les clients sont connus), la technique actuelle ne permet pas de protéger de la pollution un site de Cloud, de plus, cette dernière, peut être engendrée par un poste client, qui ne connait pas obligatoirement son propre état de pollution. Il est donc très difficile de remonter au client initial, et les autres clients du Cloud sont alors en droit de se retourner vers le propriétaire du Cloud dans le cas de pollution de leurs données.

De plus des postes clients peuvent eux-mêmes être pollués, par un Cloud pollué par un autre client. Cela montre l'interaction informatique entre des entreprises qui ne se connaissent peut être pas,

Peut être pensez vous que si vous participez à un Cloud, le fournisseur vous garantit un cloisonnement informatique étanche ? Et bien non ! Votre entreprise (vos postes connectés au Cloud) devient une partie de la toile tissée par le Cloud et votre informatique est alors assujettie aux aléas d'autres entreprises.

C'est un des problèmes très important lié au système de type Cloud.

MYTHE N° 5 :
SI VOUS QUITTEZ VOTRE FOURNISSEUR, VOTRE CONTRAT GARANTIT LA CONFIDENTIALITE ET LA RESTITUTION DE VOS INFORMATIONS ET LEUR DESTRUCTION

En dehors des problèmes de confidentialité et d'authentification relatifs aux communications électroniques entre plusieurs sites, les informations (confidentielles ou non) des clients sont stockées chez un tiers. Il se pose alors le problème de la confiance dans le tiers par rapport aux problèmes suivants :

- Accès à des informations de clients par des employés du tiers (espionnage).
- Pénétration du site par autrui qui est ou non un client. (usurpation d'identité)

Même si les informations sont chiffrées sur les machines du Cloud, le chiffrement est propriétaire (algorithme et clef) du Cloud et pas de chaque client. Un chiffrement propre à chaque client avec des clefs différentes pour chaque envoi, minimise les risques d'indiscrétion, mais complique la gestion du Cloud et ouvre la porte à d'autres problèmes.

Comment pensez-vous accorder votre confiance à un fournisseur de service de Cloud ? Quel niveau d'informations confidentielles êtes-vous prêt à confier à autrui ? Pensez vous que par contrat le fournisseur de Cloud va vous garantir la non divulgation en interne, ou par accès extérieur, des informations stockées ?

Ces questions montrent la difficulté d'accorder sa confiance à un fournisseur de service de Cloud, que vous ne contrôlez pas.

Vous pouvez aussi penser à changer de fournisseur de Cloud ou vous pouvez vous retrouver face à la disparition de votre fournisseur.

Alors se pose la question de la récupération de vos données et de l'effacement des informations des supports magnétiques utilisés. Pensez-vous que par contrat, votre fournisseur va vous garantir l'effacement de vos informations, c'est-à-dire la destruction des

supports magnétiques ? Il semble peu vraisemblable que vous obteniez cette clause dans votre contrat.

Les systèmes ouverts au public ne peuvent correspondre au monde industriel, y compris aux PME/PMI. Les dangers sont très importants, ils correspondent à ceux relatifs au réseau internet. Aucun contrat ne pourra garantir la sécurité des informations, donc ils ne peuvent être utilisés que pour des informations ou traitement non confidentiels.

Comme les puissances de calcul, les volumes de stockage, les prix des logiciels continuent de s'améliorer, on peut se demander si le grand public nécessite ce type d'offre.

MYTHE N° 6 :
AVEC UN SERVICE DE CLOUD, JE N'AI PLUS BESOIN DE ME PREOCCUPER DE MA SECURITE ET DE LA DISPONIBILITE DES SERVICES, ET MON CONTRAT COUVRIRA LES RISQUES INFORMATIQUES ENGENDRES

Comme tout problème de sécurité, la problématique de l'utilisation de systèmes de type Cloud peut être formalisée par les deux idées antinomiques suivantes :

D'un coté les diminutions de coût engendrées par la mise en commun et la meilleure utilisation des ressources informatiques et, d'un autre coté une augmentation importante des risques d'espionnage, pollution etc. dans le monde informatique.

Avec un service de Cloud Computing, les problèmes de sécurité sont très fortement amplifiés : destruction, pollution, confidentialité etc., et la disponibilité des ressources est assujettie au fonctionnement du réseau. Il est plus facile de sécuriser des informations dans son entreprise que sur un système non propriétaire partagé et utilisable à travers un réseau.

Il est clair, que pour des entreprises stratégiques de taille importante, la notion de Cloud ne peut exister que dans le périmètre de l'entreprise, le Cloud est physiquement installé sur un des sites et les clients appartiennent à un même environnement. C'est une vieille utilisation, même si l'exploitation des calculateurs est confiée à un tiers qui peut être le fournisseur de système Cloud.

Pour des entreprises (PME-PMI) stratégiques, un vrai problème se pose, et l'analyse entre la perte financière engendrée par la copie (espionnage ou destruction) de document, et le gain obtenu par la diminution des coûts journaliers de l'informatique, est très difficile à évaluer et dépend de nombreux facteurs.

L'utilisation des systèmes de Cloud ouverts et gérés par des tiers devient alors limitée à des applications dont le niveau de confidentialité est faible, dans le monde industriel, la dernière molécule, le dernier programme etc. ne se partage pas, et les informations relatives à la comptabilité client sont protégées.

L'utilisation de système de type Cloud pose le problème de la confiance vis-à-vis du fournisseur du Cloud, mais aussi vis-à-vis de ses clients, il manque un gendarme.

Pensez-vous vraiment confier vos informations confidentielles à un tiers, et pensez vous que votre contrat couvrira les risques informatiques engendrés ? L'informatique évolue, les types d'attaques aussi, et un contrat signé à une date, ne peut envisager les évolutions dans les années suivantes.

QUELQUES PLATEFORMES EXISTANTES

Plusieurs plateformes ont émergé dans le domaine du Cloud Computing. Parmi les plus connues, nous pouvons citer :

- **Amazon Elastic Compute Cloud** (EC2) : il s'agit d'une plateforme de type IaaS basée sur les machines virtuelles Linux. EC2 fournit une plateforme de création de machines virtuelles personalisées (AMI pour Amazon Machine Image) et d'exécution de ces machines virtuelles.
- **Google App Engine** : il s'agit d'une plateforme de type PaaS de développement et d'exécution d'applications web. Une quantité de ressources minimum est allouée par la plateforme et peut évoluer en fonction des demandes de l'application.
- **Microsoft Live Mesh** : il s'agit d'une plateforme de type SaaS de stockage d'applications et de données. Elle assure la disponibilité et la synchronisation des données entre tous les équipements du client.

Ces quelques exemples montrent l'implication des grands acteurs. Si le Cloud Computing est plus une orientation stratégique et architecturale qu'une révolution technologique, il est clair que cette orientation risque de bouleverser les infrastructures informatiques de nos entreprises.

MYTHES ET LEGENDES DES SERVICES DE CLOUD

Jean-Marc Grémy, Cabestan Consultants

MYTHE N° 1 : CELA FAIT DEJA 30 ANS QUE NOUS FAISONS DU CLOUD COMPUTING !

Non ! La définition des services de Cloud Computing est complètement en opposition avec cette idée. Depuis 30 ans nous externalisons la fonction Informatique chez des tiers (les tant redoutés contrat de *Facility Management* des années 90) ou nous optons pour l'hébergement de systèmes dans des Datacenter. Dans le premier cas on mutualise les ressources humaines, dans le second cas les infrastructures physiques (bâtiment, énergie, accès télécoms…). Mais en aucun cas nous avons mutualisé sur la même machine des applications, des systèmes d'exploitation divers appartenant soit au prestataire de Cloud dans le cas du IaaS soit au client final dans le cadre du PaaS.

Peut-être le seul cas rencontré jusqu'ici est celui de l'hébergement des sites Web institutionnels des entreprises. Ils étaient hébergés, souvent pour des questions de couts, sur une machine physique avec des instances du service Web. Ainsi une même machine pouvait supporter plusieurs sites web de différentes entités juridiques. Dans ce contexte l'hébergeur garantissait l'exploitation du système, la disponibilité des infrastructures d'accès (souvent le seul réseau Internet) ainsi que la sauvegarde des données applicatives.

La définition[37] du Cloud impose l'idée du partage de ressources et de la colocation de systèmes. A elle seule cette définition exclue les modèles que nous avions construit jusque là. Une machine, un service, un propriétaire.

Le Cloud Computing a ceci de particulier qu'il propose à travers ces différentes architectures[38] une évolutivité des implémentations : de la machine dédiée (hardware) à l'application en passant par des OS dédiés, des bases de données dédiées… sur des machines partagées. Le service suivant la même logique : exploitation du hardware uniquement jusqu'à l'exploitation de l'application et ses données en passant par l'exploitation unique d'une instance de l'OS.

Pour comprendre les évolutions et les possibilités de la technologie, projetons-nous en avant pour en voir l'évolution. Si nous repartons de l'idée de payer en fonction des besoins (i.e. *pay as you grow*) ne pourrions nous pas imaginer que cette seule assertion prédit la fin des serveurs informatiques dans nos Datacenter privés ? L'idée serait que finalement nous pourrions ne plus avoir de systèmes mais uniquement des unités d'œuvre de calcul chez un opérateur de service. En fonction des besoins, du moment de notre activité, de sa saisonnalité, nous aurions plus ou moins de capacité de calcul. L'institut d'étude IDC prédit un marché mondial du Cloud Computing en 2013 à une valeur de $45mds ; le prix d'une machine virtuelle étant inférieur à $1 chez certain opérateur, le nombre possible de machines avec $45mds est vertigineux.

[37] *NIST : National Institute of Standards and Technology. Agence du Department of Commerce Américain.*

[38] *Voir* Mythes et Légendes des systèmes de Cloud

Pour mettre en perspective les définitions des architectures de Cloud, et pour donner quelques repères au lecteur, nous pouvons illustrer la définition que nous avons donnée avec les offres[39] suivantes :

- Software aaS (SalesForce, GoogleApps...)
- Platform aaS (Force.com, Google App Eng, Microsoft Azur...)
- Infrastructure aaS (Amazon EC2, Microsoft Azur...)

Alors si les constructeurs de serveurs vont se positionner, qu'en est-il des opérateurs télécoms et Internet ? Leur légitimité est tout aussi importante que les constructeurs, si ces derniers ont la puissance de calcul, les opérateurs disposent du transport. Mariage de raison ou prise de pouvoir ? L'histoire le dira…

Si on ne sait pas qui sera demain le grand gagnant de cette « nouvelle vague », une chose est sûre, cela fait 30 ans que l'on se prépare à l'arrivée du Cloud.

MYTHE N° 2 : LE CLOUD COMPUTING C'EST UTILISER DES INFRASTRUCTURES VIRTUALISEES.

Oui, c'est le principe fondateur ! Quand Harry rencontre Sally, ou quand la technologie rend possible des choses qui ne l'étaient pas ou très peu autrefois. Mais qui dit "virtualisation" ne dit pas nécessairement "éditeur unique". Il existe aujourd'hui plusieurs offres sur lesquelles l'entreprise peut s'appuyer pour bâtir son propre Cloud Privé. Les critères de choix sont multiples : évolutivité (élasticité pour certain), sécurité, exploitabilité, interopérabilité…

La différence essentielle avec la virtualisation proposée par les grands systèmes, depuis maintenant plusieurs années, réside dans le fait que l'on peut toujours cloisonner des instances de systèmes d'exploitation, mais ces derniers peuvent être de nature différente : Windows™, Linux™, Mac OS™…

Cette définition de la virtualisation et son association aux offres de Cloud Computing sont essentielles. C'est en partie pour ce point que le Mythe n°1 est en opposition avec l'idée d'une existence ancienne du Cloud. La virtualisation est le moteur économique et technique du Cloud. Elle représente à elle seule l'idée du Cloud. Les instances applicatives sont mutualisées sur des équipements physiques communs. Sans ce partage de ressources techniques, il n'y a pas de Cloud.

La dimension économique de la virtualisation est avant tout liée à la capacité de la technologie à proposer une agilité de l'entreprise à pouvoir déployer à la demande son informatique : des serveurs à la demande aux postes de travail à la demande l'ensemble de la chaîne technique peut-être virtualisé. L'avantage de la virtualisation est la capacité qu'elle offre de permettre une instanciation rapide et facile d'une machine (au sens système d'exploitation). Dans certains cas de figure cette idée, poussée à son extrême, permet de mettre en place des plans de contingence informatique jusque là réservés aux grandes entreprises. Comment ? Redémarrer sur un autre site physique le serveur logique qui aura été préalablement sauvegardé. Dans des temps record de restitution.

Mais attention à ne pas faire trop de raccourci ou définir les services de la virtualisation, sa souplesse, son évolutivité et sa sécurité à la seule offre d'un éditeur, fut'il le « *best-of-breed* ». Ne pas recréer un « frigidaire » de la virtualisation.

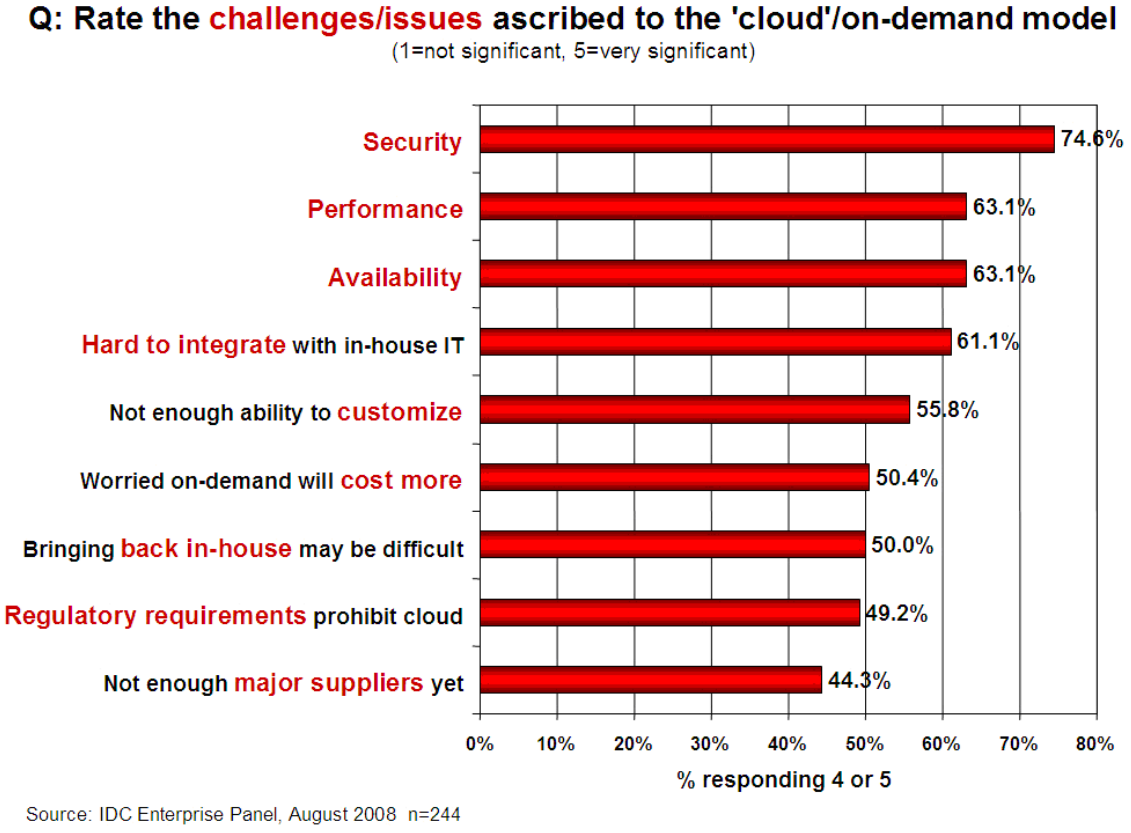
[39] *Les produits commerciaux énoncés restent la propriété de leurs ayants droit, cette liste ne saurait être exhaustive en termes de définition d'offre et d'appellation.*

MYTHE N° 3 :
LES OFFRES DE SERVICES DU CLOUD COMPUTING NE PROPOSENT PAS DE SECURITE LOGIQUE

Nous n'aborderons pas dans ces pages la question de la sécurité physique. On présume, peut-être à tord, qu'elle fait partie des fondations des offres de services ; notamment pour la couverture des risques.

Pour faire écho à ce point et pour conserver une vision impartiale de tout constructeur/offreur de service, nous appuierons notre développement de la sécurité des offres de Cloud sur les travaux communs : de la *Cloud Security Alliance*[40], de l'*European Networks and Information Security Agency*[41] ainsi que sur les premiers travaux de *l'Open Datacenter alliance*[42].

Cela étant posé, revenons à la sécurité logique. Pour développer ce point, quelques chiffres issus d'une étude publiée en 2008 par le cabinet d'étude IDC :



Sur le podium des préoccupations du panel ressort la sécurité à la première et troisième place. On pourrait, dans une certaine mesure, associer la performance à la sécurité mais nous ne développerons pas ce point ici.

[40] *CSA : www.csa.org.*
[41] *ENISA : www.enisa.europa.eu*
[42] *Open Datacenter Alliance : www.opendatacenteralliance.org.*

Quelle différence peut faire l'interviewé entre sécurité et disponibilité ? Dans les critères fondamentaux de la sécurité, on a l'habitude de discerner la **disponibilité**, de la **confidentialité** et de l'**intégrité**. Donc dans cette étude, l'aversion au risque de perte des services est telle que cette préoccupation ressort telle quelle. Dont acte. Nous reviendrons sur ce point dans le mythe suivant.

La sécurité, l'intégrité des données et leur confidentialité sont donc la préoccupation majeure. Par habitude, nous pouvons même penser que par sécurité, le panel devait penser au seul critère de confidentialité.

MYTHE N° 4 :
SI JE CHANGE DE PRESTATAIRE DE CLOUD, JE NE POURRAI PAS RECUPERER LES INFORMATIONS QUE JE LUI AI CONFIEES

Il est évident que les données confiées sont récupérables. Mais attention, là encore la plus grande prudence est à observer quant aux capacités réelles de les récupérer. L'entreprise doit tout d'abord considérer deux points :

- le volume de ses données stockées. A lui seul ce paramètre constitue l'élément de la faisabilité, nous reviendrons dessus dans le prochain Mythe,
- la possibilité technique de l'offre de Cloud.

Cette question importante, qui fait appel à un concept sous-jacent, quelle est ma possibilité réelle de changer de prestataire ? L'idée ici est de mettre en perspective les situations dans lesquelles les entreprises auront cloudisées des penta octets de données. Comment les transférer vers un autre opérateur de cloud ? Nous considérons l'opérateur de Cloud dans le cas des offres de service de type IaaS ou PaaS. Dans le cas du SaaS, la question est plus simple et peut-être plus complexe qu'il n'y paraît. Nous reviendrons sur ce cas, ultérieurement.

Pour faire écho à cette possibilité technique, qui de toute façon doit prendre une forme quelconque, l'évolution des offres de Cloud verra peut-être arriver des opérateurs de stockage qui fourniront leur service aux opérateurs commerciaux (Paas ou SaaS). De telle sorte que les données n'aient plus à être « techniquement récupérées ».

MYTHE N° 4 BIS :
QUAND JE DEMANDE UNE SUPPRESSION DE FICHIER, OU DE L'ENSEMBLE DE MON INFORMATION NOTAMMENT QUAND JE CHANGE DE PRESTATAIRE, LES FICHIERS ET ENREGISTREMENTS SERONT SUPPRIMES

Si la possibilité technique de récupérer ses données nous est donnée par les éléments à vérifier sur l'offre de service telle que nous l'avons abordée précédemment, le point est maintenant tout autre, quelle est la rémanence des données chez le prestataire ?

L'essence même du Cloud n'est elle pas de garantir en tout lieu (de la planète Internet), à tout moment l'accès à ces données ? Encore un point pour lequel la réponse n'est ni triviale ni définitive.

Elle n'est pas triviale, car elle dépend de l'offre de service.

MYTHE N° 5 :
LE PRESTATAIRE A UN ACCES COMPLET A MES APPLICATIONS ET MES DONNEES QU'IL HEBERGE

On attend une certification de Qualité de la sécurité dédiée aux offres de Cloud. Aurons-nous des approches de certification de la gestion de la sécurité de l'information, à l'instar des processus de certification ISO/IEC 27001 ? Le cadre normatif a développé des normes de bonnes pratiques à destination des professionnels de santé (ISO 27799), des professionnels des télécoms (ISO 27011)… Auront-ils demain une démarche identique dans le Cloud ou pouvons nous appliquer les modèles de certification existant ?

Pour fermer ce point sur la certification des services, nous rappellerons la philosophie de la démarche de certification : apporter la confiance aux tiers. Cette confiance permet aussi au prestataire de s'assurer qu'il suit bien, au-delà de l'état de l'art, les attentes et les prérequis. Cette confiance lui est donc aussi destinée.

MYTHE N° 6 :
AVEC UN SERVICE DE CLOUD COMPUTING JE N'AI PLUS BESOIN DE ME PREOCCUPER DE MA SECURITE, NOTAMMENT DE LA DISPONIBILITE DES SERVICES

La question de la disponibilité est un point essentiel du Cloud. Observons-la sur deux axes :

Le premier celui de l'ubiquité des données. En effet, l'idée sous-tendue par les différentes offres de Cloud (rappel sur la définition du NIST) est que les machines virtuelles dans le cas du IaaS, les systèmes d'exploitation et applications de base dans le cas des PaaS ou des applications et leurs données dans le cas des SaaS sont en permanence disponibles, et ce, où que vous vous trouviez sur le globe.

Mais dans la réalité est-ce vrai ? Comment être sûr du respect de ce postulat ?

Si nous tenons compte des contraintes légales (lois et réglementations) dans certain cas de figures, les données doivent être stockées dans des localisations bien précises : en France, en Europe, les sites doivent être auditables. Dans ce contexte, la logique de Cloud et la disponibilité qu'il offre sont à revoir, si l'on imaginait que la disponibilité était implicitement garantie.

Le second point trop souvent ignoré est la résilience du réseau, donc cela nous ramène à la part que joueront demain les opérateurs. Mais deux écoles existent :

- L'opérateur disposant de son propre réseau est en mesure d'en assurer la continuité. Au détail prés que la quasi totalité des opérateurs utilise les services d'autres opérateurs pour améliorer la capillarité de leur réseau, les performances, la disponibilité. Dans ce cas une défaillance de l'opérateur du contrat serait potentiellement un problème
- La connexion aux services du Cloud se fait par Internet. Et dans ce cas on considère le réseau techniquement suffisamment résilient pour prendre en compte la majeure partie des problèmes à assurer tout le temps et en tout point

D'ailleurs, cette question de la disponibilité de l'information n'est pas très éloignée de celle de l'Intégrité de l'information. Un défaut d'intégrité d'une information peut avoir comme conséquence directe la perte de la disponibilité. Attention à ce point, lorsque par exemple, l'entreprise déploie des outils de cryptographie sans maîtrise de l'outil, de recouvrement voire de séquestre des clés de chiffrement… L'information est semble t'il disponible mais inaccessible par la transformation opérée par le chiffrement.

MYTHES ET LEGENDES DES TELECOMMUNICATIONS SPATIALES

Guillaume Rembert

MYTHE N° 1 : UN PROCESSEUR DE CALCUL EMBARQUE DANS UN SATELLITE EST PLUS PERFORMANT QUE CELUI DE MON ORDINATEUR

Le véhicule spatial, et, dans le cadre du sujet qui nous intéresse, le satellite de télécommunications sont des systèmes assez mal connus du grand public et font l'objet de tous les fantasmes. Parmi ceux-ci, une personne qui n'en connait pas les aspects techniques pourrait penser que les calculateurs de bord et autres technologies embarquées sont plus performants que les technologies commerciales rencontrées parmi le grand public. On prête aux satellites des aspects quelque peu magiques. Ils sont en soi une réelle prouesse humaine : nous avons réussi à arracher à la gravité et à faire tourner un objet assez vite pour qu'il ne retombe pas. Ils sont également une preuve concrète de l'accès au voyage spatial pour l'Homme.

Quelle que soit l'orbite d'un satellite, c'est à dire sa position et son mouvement relatif à la Terre, il est soumis à un environnement très rude (vide, variations de températures extrêmes, tempêtes d'électrons, vibrations pendant le lancement, etc.) qui, combiné à une très faible maintenabilité (il est assez difficile d'aller le réparer), entraine un nombre phénoménal de précautions et de validations nécessaires à la garantie du taux de fiabilité désiré par les opérateurs de satellites. Pour exemple, un acteur majeur des communications spatiales, affiche pour son réseau le taux de fiabilité record de 99,9999% pour l'année 2005 (moins d'une minute d'indisponibilité sur toute l'année)...

Il faut ensuite savoir que la durée de vie moyenne d'un satellite géostationnaire est actuellement supérieure à 15 ans. Cela peut laisser rêveur et jaloux plus d'un technicien concevant des équipements de communications terrestres, mais beaucoup moins leurs gestionnaires financiers qui sont actuellement embourbés dans un modèle économique basé sur la rente, la saturation du marché et l'hyper-consommation.

Néanmoins, la qualité a un coût, et il n'est pas que financier... Il est aussi et principalement technologique ! Le changement d'une ligne de code dans un programme, le remplacement d'un câble ou le changement d'une molécule dans la formule d'une peinture engendre un très grand nombre de tests et d'essais. Les opérateurs recherchent très souvent des technologies validées en orbite, qui ont fait la preuve de leur fonctionnement pendant un temps défini en conditions opérationnelles.

Ce secteur industriel se différencie sur de nombreux points : les formidables avancées scientifiques qu'il permet, le frisson de peur associé aux opérations de lancement et de mise à poste de tout véhicule spatial, l'échec redouté et le goût du risque. Les sommes financières qui y sont mises en jeu sont colossales et les difficultés potentielles tellement nombreuses que l'innovation technologique opérationnelle y est rendue très difficile. De nombreux projets de constellations satellitaires ayant pris de trop longues années à être développés sont arrivés trop tard vis-à-vis de leurs concurrents terrestres qui avaient déjà conquis le marché. Heureusement, les pouvoirs publics sont intervenus souvent pour soutenir ces

développements, effet d'engagement aidant, mais principalement parce que le service rendu avait une réelle valeur ajoutée pour l'Homme.

La pression financière associée à la maturité technologique (le coût d'une assurance augmente fortement lorsqu'une technologie n'est pas validée en orbite), la longue durée des cycles de développement et de validation de nouvelles solutions techniques ralentit l'évolution et l'adoption de technologies complexes. On comprend donc facilement qu'un processeur que l'on achète pour quelques euros, que l'on utilise tous les jours (dans son ordinateur par exemple), dont la fiabilité peut laisser à désirer, est bien plus performant qu'un processeur embarqué dans un satellite, dont la fiabilité est garantie. Il ne faut malgré tout pas oublier que les modèles physiques les plus poussés se basent sur l'aléa, que les conditions environnementales des systèmes ne sont jamais totalement maitrisées et que de ce fait, la garantie d'un bon fonctionnement n'est jamais absolue...

MYTHES ET LEGENDES DES MEDIA SOCIAUX

Yanis Taieb, MediaWeb Lab

La révolution internet consistait à interconnecter des millions d'individus ou entités sociales.

Mais pour que ces interconnections puissent aboutir à de réelles interactions, il fallait qu'elles soient organisées autour de sujets, de contenus que l'on puisse partager.

Or c'est justement cette dimension manquante qu'ont apportée les média sociaux en permettant à tous les internautes de créer, partager et diffuser du contenu. Grâce à ces plateformes des millions d'internautes peuvent, chaque jour, échanger de l'information, des connaissances, du savoir, partager des émotions, des sentiments et là on n'est pas dans le virtuel.

MYTHE N° 1 : LES MEDIA SOCIAUX SONT DANGEREUX POUR LES UTILISATEURS

Un certain nombre de média traditionnels semblent, par un discours réducteur, vouloir nous faire croire que ces nouveaux média sont dangereux pour les utilisateurs.

Je tiens à souligner que si les média sociaux sont dangereux, c'est surtout pour les média traditionnels avec qui ils rentrent en concurrence directe !

Au mois de novembre 2010, plusieurs jugements des Prud'hommes donnent gain de cause à différentes entreprises ayant licencié des salariés pour propos déloyaux sur Facebook. En lisant les commentaires auxquels ont donné lieu ces décisions, je prends pleinement conscience que la majorité des internautes n'a pas réalisé qu'internet n'est pas un espace virtuel et l'est encore moins depuis l'avènement du web 2.0.

Du danger imaginaire de ce nouvel environnement

Je voudrais, faire remarquer, que si les propos des salariés à l'origine de ces jugements prud'homaux avaient été tenus sur des média traditionnels, ils auraient entrainés les mêmes conséquences.

Doit-on en déduire que les média traditionnels sont également dangereux ?

Un média est, d'après sa définition « une institution ou un moyen impersonnel permettant une diffusion large et collective d'informations ou d'opinions ». Par définition, c'est donc un canal de diffusion public. Certes Facebook, comme d'autres réseaux sociaux permettent de restreindre la diffusion de ses informations. Cependant, à partir du moment où l'on accepte la diffusion de ses informations « aux amis de ses amis » ou au-delà bien sûr à tous les membres d'une communauté, on n'est plus dans une sphère privée mais dans une démarche de communication médiatique. Il convient donc de tenir compte des textes de lois régissant la prise de parole publique.

Se poser la question de savoir si ces lois sont en phase ou rentrent en contradiction avec la liberté d'expression individuelle est un autre débat.

MYTHE N° 2 :
LES MEDIA SOCIAUX SONT UN PHENOMENE DE MODE MINEUR

Non décidemment le phénomène des média sociaux n'est pas un phénomène mineur. Il n'est pas non plus limité dans l'espace que ce soit à certaines catégories de populations ou à certaines zones géographiques (sa seule réelle limite en la matière étant la nécessité d'une connexion internet). Enfin ce n'est certainement pas un phénomène de mode qui a une durée de vie éphémère.

Les média sociaux : un phénomène mineur ?

Pour atteindre 50 millions d'utilisateurs, la radio a mis 38 ans, la télévision 13 ans, internet 4 ans. Or, Facebook compte plus de 400 millions d'utilisateurs actifs après seulement 4 ans d'existence. La plateforme a rejoint Google sur le plan de l'activité avec une moyenne de 7% de la part du temps consacré par les internautes.

Il y a quelques semaines, Twitter, plateforme en vogue du web 2.0 et créée en 2006 atteignait 175 millions de membres et était évaluée 1,6 milliard de $, soit 50% au dessus de la valeur du New York Times, véritable institution des média traditionnels fondée il y a plus de 150 ans.

Pendant ce temps, deux des principales plateformes de réseaux sociaux professionnels LinkedIn et Viadeo connaissent une croissance sans précédant d'une part en termes de membres et d'autre part en termes d'activité.

La première compte plus de 70 millions de membres répartis sur plus de 200 pays et affiche une moyenne pour chaque membre de 42 pages visitées par mois.

La deuxième dénombre plus de 30 millions de membres dont la bagatelle de 500 000 entrepreneurs et dirigeants et 3 millions de Français et rassemble 145 000 groupes de discussions regroupant au total 5 millions d'internautes.

Je ne m'étendrai pas plus sur les chiffres : on ne peut que constater l'immense opportunité d'audience que proposent les média sociaux !

MYTHE N° 3 :
LES MEDIA SOCIAUX NE SONT QU'UNE TENDANCE POUR JEUNES PUBLICS

Si l'essor initial des média sociaux est à mettre à l'actif des jeunes générations, on constate d'une part l'émergence de plateformes plutôt destinées à un public plus âgé (notamment les plateformes professionnelles) et d'autre part on assiste à un effet de rattrapage du taux de pénétration des populations plus âgées, y compris sur des plateformes, plutôt tout public, comme Facebook.

Ainsi, aujourd'hui, le phénomène s'étend largement au-delà des publics jeunes. Voici quelques chiffres pour illustrer la situation et l'évolution récente : L'âge médian des membres de Linkedin se situe autour de 41 ans et celui de Viadeo autour de 36 ans. L'âge médian de ceux de Facebook est passé de 26 ans à 33 ans, dans l'année 2009. Cette même année, la plateforme a enregistré, par exemple, aux Etats-Unis, une croissance de plus de 900% de sa population de + de 55 ans, alors que la croissance moyenne s'établissait à 145%.

Cette tendance s'est propagée en 2010 sur les différents continents.

MYTHE N° 4 :
LES MEDIA SOCIAUX SONT UN PHENOMENE TYPIQUEMENT AMERICAIN OU ANGLO SAXON

Il n'aura échappé à personne que le phénomène des média sociaux est né aux Etats-Unis, tout comme, d'ailleurs, celui des sites de rencontre duquel il a puisé son inspiration.

Cependant, on constate que si son expansion a débuté dans les pays développés, elle a très rapidement atteint l'ensemble des pays en voie de développement qui aujourd'hui contribuent aussi largement à la croissance du phénomène malgré leur handicap d'équipements informatiques et de connexions internet.

Ainsi, le taux de pénétration de Facebook sur l'ensemble de la population Philippine connectée est de l'ordre de 65%, celui de la Malaisie, au dessus de 75% : des taux assez proches de ceux constatés dans la plupart des pays développés.

De la même façon, si le phénomène s'est initialement propagé dans les pays anglo-saxons, il en a largement dépassé les frontières. Un chiffre résume bien la situation : 70% des membres de Facebook ne sont pas américains. Des statistiques récentes indiquent même un taux de pénétration des réseaux sociaux plus important parmi les internautes brésiliens que chez les internautes américains, de même qu'un taux quasi équivalent ou plus important dans les pays latins (Espagne, Italie, France, Roumanie) qu'au Royaume Uni. On notera d'ailleurs aussi que certains pays latins font quasiment jeu égal avec les USA.

Or, une des caractéristiques communes de ces pays non anglophones qui ont largement assimilé le phénomène, est d'avoir toujours maintenu un lien social très fort !

MYTHE N° 5 :
LES MEDIA SOCIAUX SONT LE DERNIER ACCESSOIRE BLING BLING A LA MODE

Le lien social ? L'essor des média sociaux s'appuie largement sur un des fondements de l'humanité depuis ses origines : la vie en société qui induit la nécessité du lien social et donc du réseau social. Ainsi le réseau social a toujours existé. Ce qui change aujourd'hui, c'est sa portée : on peut désormais être relié avec des millions de personnes aux quatre coins du monde et échanger, partager avec eux, en direct ou en différé.

Mais ce qui caractérise aussi ce phénomène, c'est qu'il remet l'Homme au centre de l'action par rapport à l'Organisation. On pouvait craindre une déshumanisation de nos sociétés et l'on pourrait assister à un second souffle de l'hominisation. On comprend ainsi que ces nouveaux média sont à la croisée d'aspirations et d'enjeux vitaux pour la communauté humaine. Aussi, il serait très étonnant que leur développement ne soit pas durable.

MYTHE N° 6 :
LES MEDIA/RESEAUX SOCIAUX SONT DES OUTILS A DESTINATION DES GRANDES ENTREPRISES

Les grandes entreprises face aux média sociaux

La plupart des grandes entreprises du secteur technologique ont rapidement adopté et intégré les média sociaux dans leur stratégie.

Ce n'est pas étonnant de les retrouver précurseurs dans ce domaine car d'une part, la nature de leur activité en fait généralement des entreprises très réactives surtout vis-à-vis des nouvelles technologies et d'autre part, leur organisation et leur fonctionnement s'appuient

largement et depuis longtemps sur des principes collaboratifs qui constituent un des aspects essentiels de l'environnement du web 2.0.

Cette situation est cependant loin d'être généralisable à l'ensemble des grandes entreprises qui ne sont globalement pas très présentes sur ces nouveaux média. En effet, les grandes firmes sont lentes à s'engager car un déploiement sur les média sociaux a des impacts sur l'ensemble des fonctions vitales de l'entreprise, ce qui nécessite une parfaite coordination des différents services. De plus, ces nouveaux média induisent un degré très élevé d'interactivité de la communication auquel il s'agit de répondre par un niveau élevé de réactivité.

Or, ces deux obstacles que les grandes entreprises doivent surmonter avant de décliner leur stratégie sur les média sociaux, ne constituent pas des obstacles majeurs pour les TPE ou les PME.

Média sociaux au service des TPE et PME

Au-delà, l'environnement du web 2.0 sert particulièrement bien la stratégie de ces dernières.

Les média sociaux permettent d'abord l'accès à un coût quasiment nul à une très large audience. Je rappelle quelques données : Facebook compte 500 millions de membres, LinkedIn le premier réseau professionnel, plus de 70 millions de membres avec 50% de décideurs économiques, Viadeo en réunit près de 30 millions dont plus de 3 millions en France…

Ces média sont également très efficaces pour affiner leur positionnement, aspect aujourd'hui essentiel de la stratégie de communication d'une petite entreprise. Ils offrent des outils de segmentation très performants permettant aux entreprises de toucher plus facilement leur cœur de cible, atout primordial pour des entreprises qui s'adressent à des marchés de niche ou des nouveaux marchés avec des produits innovants.

Enfin ils constituent des outils d'information, de veille et d'inspiration sans équivalent notamment pour des structures qui ont peu de temps à consacrer à cette activité, pourtant stratégique dans un environnement de plus en plus fluctuant.

Décidemment, ces nouveaux média présentent de nombreux arguments favorables pour les TPE et PME. Mais qu'en est-il du temps à y consacrer, n'est ce pas une discipline chronophage ?

MYTHE N° 7 :
LES MEDIA/RESEAUX SOCIAUX SONT DES OUTILS CHRONOPHAGES

- Communiquer : développer sa notoriété, améliorer sa visibilité notamment sur Internet, façonner son image ;
- Vendre : prospecter, établir un lien permanent avec ses clients et prospects, engager la discussion avec eux sur ses produits, ses services ;
- Coopérer : identifier de nouveaux partenaires, maintenir le lien avec ses partenaires existants, collaborer avec eux ;
- Recruter : se mettre en relation avec des futurs collaborateurs potentiels, mieux les connaître, garder le contact;
- Anticiper : s'informer, se former, se positionner ;
- Créer : analyser, comprendre, s'inspirer…

Autant d'activités vitales au développement de l'entreprise et autant d'activités que l'on peut pratiquer sur les média/réseaux sociaux. Non ! Avec une vision pragmatique et réaliste, les média et réseaux sociaux ne sont pas des outils chronophages. Mais il s'agit bien sûr de les maîtriser, d'avoir une stratégie et de les utiliser à bon escient.

CONCLUSION

Internet, considéré depuis son apparition comme l'une des révolutions technologiques majeures du 20ème siècle n'était, jusqu'à présent, parvenu qu'à rendre obsolète l'utilisation du télécopieur.

Pourtant penser que l'impact de cette technologie resterait limité à cela, c'était oublier cette formidable capacité des hommes à assimiler les nouvelles technologies, surtout quand elles sont révolutionnaires et à développer à partir de celles-ci une multitude d'innovations créant ainsi un effet d'entrainement susceptible de générer bouleversements sur bouleversements.

L'innovation et la société humaine

Depuis la nuit des temps, l'homme n'a eu de cesse d'innover et la société humaine de s'approprier ces innovations, de les digérer, de les décortiquer, de les décliner, de les diffuser et d'innover encore.

Ces innovations engendrent leur lot d'évolutions et de changements dont l'ampleur et le rythme dépendent bien sûr de la nature même de l'innovation mais aussi de sa capacité éventuelle à accélérer les processus de développement et de diffusion d'autres innovations.

Ainsi la domestication du feu fût une innovation essentielle car elle permit, notamment, à l'homme de prendre définitivement le dessus sur l'animal et d'assurer sa survie en milieu hostile. Mais le feu a aussi été un facteur prépondérant du processus d'hominisation et donc de socialisation, qui a très largement contribué à l'accélération de l'histoire. Autre exemple prépondérant, le rail a été à l'origine de bouleversements en série qui ont fait dire à Charles Péguy : *« **Le monde a plus changé entre 1880 et 1914 que depuis les Romains.**»*

On comprend bien qu'avoir accès, qui plus est rapidement, à des ressources et des territoires inaccessibles jusqu'à présent, permettre aux personnes et aux marchandises de circuler 20 fois plus vite (pour la petite histoire, le rail a permis, au 17 ème siècle, de réduire le temps de la traversée transcontinentale de l'Amérique de 6 mois à 1 semaine) engendraient un certain nombre de changements dans le monde et ouvraient de nouvelles perspectives.

Les impacts indirects des révolutions technologiques

Mais la principale révolution du chemin de fer ne fût pas le chemin de fer lui-même mais son action indirecte sur le processus d'innovation. Le chemin de fer permit d'une part, en rapprochant les hommes d'accélérer le développement de l'innovation, de la même manière que la domestication du feu, mais il permit aussi d'accélérer la diffusion de ces innovations.

Or la découverte engendrant d'autres découvertes, l'innovation d'autres innovations, le rail a provoqué un mouvement d'entrainement de grande ampleur. Ignorer ces bouleversements ainsi que les nombreuses opportunités qu'ils généraient, aurait été, à l'époque, fatal à n'importe quelle entreprise.

Le web 2.0 et son impact sur l'innovation

Quels impacts le web 2.0 pourrait-il avoir sur le processus d'innovation ?

Non seulement les média/réseaux sociaux facilitent la communication entre tous les hommes (connectés à internet) et la rendent même immédiate, mais en plus ils fournissent des outils collaboratifs très poussés.

Non seulement les plateformes des média/réseaux sociaux permettent d'accélérer la diffusion de l'innovation mais de plus elles permettent de mieux la digérer, la décortiquer, la décliner et continuer à innover.

Nul doute que notre monde va connaître, dans les années à venir, des mutations et des bouleversements sans précédant avec de très fortes répercussions sur les entreprises et leurs marchés.

Jack Welch, PDG emblématique de General Electric a dit : *«**Lorsque la vitesse d'évolution du marché dépasse celle de l'organisation, la fin est proche.**»*

Un des plus grands défis de l'entreprise, pour rester performante aujourd'hui, est d'appréhender ces nouveaux média. Il est, ainsi, essentiel que les dirigeants soient à la fois initiateurs de ce mouvement et chef d'orchestre de son déploiement.

MYTHES ET LEGENDES DES COMMUNICATIONS UNIFIEES ET COLLABORATIVES

Jean-Denis Garo, Aastra

Le terme communications unifiées et collaboratives réunit un ensemble d'applications portées sur un ordinateur, une tablette, un smartphone. Couplées au système d'informations et de communications (Téléphonie) elles répondent à un besoin de développement des outils pour enrichir les relations entre les utilisateurs offrant divers médias synchrones et asynchrones.

Les applications les plus courantes sont : la messagerie unifiée, l'audio et vidéoconférence, la gestion de présence, le partage de documents, la messagerie instantanée (IM ou chat), le softphone, le click to call (CTI), le social web et web2.0…

MYTHE N° 1 : LES COMMUNICATIONS UNIFIEES ET COLLABORATIVES FAVORISENT LA PRODUCTIVITE.

Mettre à disposition des outils favorisant les communications, ouvrir des fenêtres d'échange entre les utilisateurs sont évidemment les objectifs des solutions de communications unifiées et collaboratives. Toutefois un déploiement mal accompagné, l'absence de formation aura l'effet contraire à celui souhaité. L'utilisateur lui-même, dans son organisation du travail, peut être son pire ennemi. L'utilisateur doit rester maître de ses outils. La gestion présence est un moyen pour lui de définir à quel moment il se déclare joignable et via quel média.

L'autre danger vient de l'introduction d'outils collaboratifs personnels dans la sphère professionnelle. On peut ici parler de prolifération, les salariés jonglant entre outils professionnels et personnels à tout instant. Un autre smartphone (privé), l'usage d'applications chat ou réseaux sociaux (si la DSI l'autorise) apportent d'autres intrusions dans le temps de travail.

A productivité il faut opposer fragmentation du travail. La multiplication d'outils de communication amène l'utilisateur à être constamment sollicité, réduisant ainsi les plages horaires dédiées au travail de fond, nécessitant concentration. Toutefois la faute n'en revient pas aux outils mais à l'usage des outils. Ces derniers doivent s'adapter à l'organisation du travail souhaitée. Nous ne recommanderons jamais assez l'accompagnement au changement, la formation aux outils et aux méthodes de travail, en un mot la communication autour du projet. Une rupture d'usage et une nouvelle façon de travailler nécessitent une réflexion préalable.

MYTHE N° 2 : LES COMMUNICATIONS UNIFIEES ET COLLABORATIVES SONT DES OUTILS DE CONTROLE (FLICAGE)

Dans ce cas précis, c'est la gestion de présence qui est souvent incriminée. Déclarer son statut, partager son calendrier, laisser des collaborateurs y inscrire des rendez-vous, communiquer sur l'ensemble des médias disponibles (N° de téléphone portable, fixe, chat, vidéoconférence…) pour être joint, accepter d'être joignable à tout moment, sont autant de

fenêtres permettant à une personne ou une organisation de suivre, contrôler l'activité d'un salarié.

C'est pourtant oublier les principes de base qui laissent à l'utilisateur l'opportunité de déclarer ou non son statut. Une entreprise peut automatiser un certain nombre de mécanismes comme lancer automatiquement le logiciel à l'ouverture d'une session sur l'ordinateur. C'est oublier aussi que ces outils sont avant tout mis à disposition des utilisateurs pour favoriser la communication, la joignabilité, et faciliter les échanges. Ce n'est pas un terminal que l'on cherche à joindre mais une personne. D'ailleurs quoique l'entreprise souhaite contrôler il ne faut pas oublier que l'utilisateur trouve toujours un moyen de contournement. Aussi l'entreprise doit-elle définir des règles applicables et acceptables, afin de répondre à son besoin légitime de management des équipes, et ainsi favoriser l'adoption d'outils améliorant sa performance. Les outils devant avant tout être contrôlés par les utilisateurs et non pas un moyen pour l'entreprise de contrôler ses salariés.

Les nouvelles générations vivent ainsi : elles déclarent déjà ce qu'elles font, pensent, où elles sont sur Facebook, Twitter L'usage est bien là. Ces générations sont toutefois réticentes à agir de même dans le cadre de l'entreprise. Mais l'utilité de ces solutions prendra vite le pas sur la méfiance.

MYTHE N° 3 :
LES COMMUNICATIONS UNIFIEES ET COLLABORATIVES REMPLACENT LES LOGICIELS DE GROUPE DE TRAVAIL (GROUPWARE OU COLLECTICIEL)

Le travail de groupe est surtout une affaire d'organisation, l'outil va permettre de favoriser ou faciliter l'échange, fluidifier l'information. La gestion de présence permet de connaître la disponibilité de quelqu'un, le partage d'agenda permet de positionner des rendez-vous, le partage de documents permet d'échanger à plusieurs sans avoir à se déplacer, la vidéo apporte une proximité, le chat une spontanéité… les médias de communications unifiées ne remplacent pas toutefois des logiciels dédiés au travail collaboratif, voire des progiciels métiers. Ces logiciels dédiés apportent des réponses à des besoins de partage de notes, de documents, de wikis et offrent la possibilité de co-rédaction. Ils requièrent aussi l'existence et la gestion de bases de connaissances

Si l'amélioration de la productivité personnelle est au premier rang des bénéfices reconnus de ce type de solutions, la productivité collective, elle, en est à ses prémices.

Les communications unifiées et collaboratives sont donc des solutions favorisant la flexibilité et l'intelligence collective mais ne sont pas encore considérées par les entreprises comme une solution dédiée au travail de groupe. L'évolution des solutions disponibles et l'intégration d'applications métiers devraient rapidement infléchir cette tendance.

MYTHE N° 4 :
LES COMMUNICATIONS UNIFIEES ET COLLABORATIVES ATTIRENT LES JEUNES (GENERATION Y) EN ENTREPRISE

Si un équipement performant attire les jeunes, comme un PC portable, ou un téléphone mobile, un véhicule pour les générations précédentes, offrir un panel de solutions unifiées et collaboratives comme la vidéo et le chat semble moins être un déclencheur que l'usage de solutions privées au travail. Ce que les jeunes aiment c'est utiliser leurs médias Facebook, MSN… pour communiquer avec leurs groupes d'amis plus qu'avoir des outils similaires pour

échanger avec leurs collègues. C'est aussi la possibilité de rester connecté avec ces mêmes groupes tout au long de la journée.

Cet usage des nouvelles technologies au sein de l'entreprise s'approche plus d'un moyen dont se dote l'entreprise pour être performant, voire adopter une démarche développement durable, ce qui rassure les jeunes prétendants mais ne sera pas un élément d'attraction. Le salaire, la localisation, les valeurs et la notoriété de l'entreprise restent en tête des critères de décision des jeunes.

L'entreprise gagnera avec ces générations une adoption facilitée aux outils/médias de dernière génération. On constate d'ailleurs déjà une accélération de l'usage d'outils tels que le « chat ». Elle gagnera aussi en image de marque (Dynamisme). Mais plus que l'outil, le télétravail, facilité par ces outils de communications unifiées et collaboratives, peut être un argument pour attirer les jeunes, leur offrant une certaine autonomie.

MYTHE N° 5 :
LA VIDEOCONFERENCE EST RESERVEE AUX GRANDES ENTREPRISES

L'usage de la vidéo au sein des entreprises est plus que jamais une réalité. Il persiste néanmoins un décalage entre les attentes des utilisateurs, les messages marketing des acteurs spécialisés et la mise en œuvre réelle de ces solutions. Réservées auparavant à certaines catégories d'utilisateurs dans l'entreprise, les solutions tendent aujourd'hui à se généraliser à la plupart des utilisateurs de l'entreprise. La vidéo étant de plus en plus considérée comme une extension du système de communication et d'information (SI), et donc comme un média complémentaire de la voix et de la data.

La vidéoconférence se démocratise, elle répond à de nouvelles attentes. En effet les solutions de vidéoconférence (salles dédiées) répondent généralement à des besoins de réunions longues, programmées, privilégiant la parole (à l'écrit), dans des salles dédiées, offrant parfois l'apparence d'une réunion virtuelle (téléprésence, co-présence physique). Désormais plus facilement utilisables, les solutions de vidéoconférence peuvent être initiées depuis un PC portable (favorisant le nomadisme ou le télétravail), et récemment à partir d'un téléviseur ou même d'un smartphone. Les solutions de vidéoconférence sur PC sont, elles, plus utilisées pour des réunions impromptues, où rapidement le partage de documents prendra le pas sur la fenêtre vidéo. Souvent utilisées pour un suivi de projet (follow-up) elles sont, du fait de leurs coûts réduits, plus accessibles aux PME. L'émergence de terminaux dédiés à la vidéo et à certaines applications offre une troisième voie. Celle de la convivialité d'un terminal vidéo HD et la possibilité de poursuivre le partage de documents sur le PC. D'autres solutions de conférence vidéo se développent comme les webconférences.

Le besoin crée donc toujours la solution. L'ensemble des solutions de vidéoconférence (salle dédiée, utilisateur PC, télétravailleur) s'interconnectant / inter-opérant pour répondre aux nouveaux usages de mobilité et aussi aux budgets des entreprises. L'appropriation de ces nouveaux médias de communication ayant profité de l'usage grand public des applications Skype ou MSN.

CONCLUSION

La plupart des technologies mises en œuvre dans un projet de communications unifiées et collaboratives existent depuis près d'une dizaine d'années, à l'image de la messagerie unifiée ou de la gestion de présence. Elles sont à présent intégrées à une suite logicielle sous forme de briques indépendantes offrant des fonctions. La DSI décidant d'offrir telle ou telle

fonction selon des profils définis dans l'entreprise (utilisateur intensif, nomade, télétravailleur, etc).

Le développement de l'usage d'applications similaires dans la sphère privée, parfois utilisées avec ou sans autorisation dans l'entreprise, amène des utilisateurs avertis, mais aussi exigeants. La difficile cohabitation des applications professionnelles et privées au sein de l'entreprise apporte son lot de problématiques nouvelles (sécurité, confidentialité, efficacité etc.).

Touchant à l'organisation du travail, amenant des nouveaux usages, provoquant de nouveaux types de relations entre les individus, créant de nouvelles règles de communications (attitude face à la caméra, stylistique du chat, syntaxe du sms) elles alimentent les mythes et légendes.

POUR EN SAVOIR PLUS

Livre blanc Collaboration Vidéo sur IP, ce qu'en pensent les décideurs IT

http://support.aastra.fr/CollaborationVideosurIp/

Livre blanc Communications Collaboratives Unifiées, ce qu'en pensent les décideurs IT

http://support.aastra.fr/ccu/

« De la ToIP aux Communications Unifiées », Collection guide, Edition crestel - 2010

MYTHES ET LEGENDES DU CALCUL INTENSIF

Jean Papadopoulo, JP ETUDES & CONSEIL

« Calcul intensif » est le terme utilisé ces dernières années pour désigner le terme anglophone de « High Performance Computing » ou HPC, ce dernier ayant lui-même évincé celui de « Supercomputing ». Historiquement, les matériels et logiciels classés dans cette catégorie étaient dédiés à des applications scientifiques et techniques, telles la mécanique des fluides, la météorologie et la climatologie, la thermodynamique, etc… Les trois caractéristiques les plus significatives du calcul intensif étaient : les performances de l'arithmétique flottante (ce qui justifie que le classement des solutions proposées se fait généralement à l'aune des opérations flottantes par seconde ou « FLOPS » consacré par le classement « TOP500 », actuellement dans la zone « petaflopique ») ; l'importance du calcul vectoriel (liée à la nature des problèmes à résoudre) ; et le débit mémoire (lié au volume des données traitées). L'évolution des matériels ces dernières années, tel que nous le décrirons dans la suite, a légèrement modifié cette définition. En effet, les mêmes systèmes permettent aujourd'hui d'aborder des applications différentes, telle la recherche de séquences génétiques qui n'utilise pas le calcul flottant, ou la fouille de données et l'informatique décisionnelle qu'on aurait plutôt tendance à classer comme application de gestion.

MYTHE N° 1 : LE CALCUL INTENSIF EST A L'INFORMATIQUE CE QUE LA F1 EST A LA VOITURE DE MR TOUTLEMONDE

Cette comparaison était tout à fait de mise pratiquement jusqu'à la fin du 20ème siècle : les ordinateurs wqui possédaient les caractéristiques voulues étaient terriblement onéreux, basés sur des architectures propriétaires et parfois « exotiques », peu compatibles entre les différents constructeurs, bénéficiant de peu de logiciels, souvent développés en interne et également chers. L'excellence dans ce domaine était gage de prestige et d'image, mais aucun des acteurs en place n'était économiquement viable et, pour tout dire, aucun n'aurait survécu sans des subventions substantielles de la part des pouvoirs publics. Par suite, les coûts de possession et d'utilisation étaient tels que peu de domaines scientifiques et techniques pouvaient justifier un retour sur investissement suffisant pour recourir au calcul intensif.

Toutefois, les choses ont véritablement commencé à changer dès le milieu des années 90, dans la brèche ouverte par l'informatique de gestion. Cette dernière a en effet atteint un haut niveau de standardisation, par le jeu d'instructions d'abord, le X86-64 s'octroyant un quasi monopole dans le domaine ; par l'architecture système multiprocesseur (SMP comme Symmetrical Multi-Processor) que l'on retrouve aujourd'hui au niveau du chip même ; au niveau du système d'exploitation enfin, Windows et Linux ayant relégué le reste dans des niches de faible diffusion. La domination de l'architecture X86-64 a mis beaucoup plus de temps à s'établir dans le calcul intensif, car la montée en puissance de ce jeu d'instruction s'est étalée sur une vingtaine d'années pour rattraper ses concurrents propriétaires les plus avancés, surtout concernant les performances de l'arithmétique flottante. De plus, la grande majorité des applications de calcul intensif requièrent plus de puissance que ne peut délivrer un seul processeur, ni même un système multiprocesseur qu'utilise avec succès l'informatique de gestion. Ainsi, les quinze dernières années ont vu l'émergence des clusters de SMP en tant

que plate-forme de prédilection pour le HPC. L'interconnexion de ces briques de grande diffusion a bénéficié du très haut niveau de standardisation dans le domaine des réseaux par l'utilisation d'InfiniBand et Ethernet. Ceci est d'autant plus vrai depuis l'adoption récente de la spécification RoCE (RDMA over Converged Ethernet) qui apporte à Ethernet le seul attribut qui lui manquait pour jouer ce rôle, à savoir une faible latence des messages. Pour compléter le tableau, l'utilisation de Linux (sans minimiser les efforts de Microsoft avec Windows HPC Server) et le standard de communication par message MPI (message Passing Interface) ont transformé les perspectives offertes aux développeurs d'applications qui ne sont plus confrontés à une multitude de plates-formes incompatibles avec tout ce que cela implique de coûts d'adaptation et maintenance de versions multiples.

Le résultat net de cette évolution est que l'industrie du calcul intensif est passée d'une période élitiste vers une standardisation poussée, la transformant ainsi d'un marché de niche en marché de grande diffusion, garant d'économies d'échelle et moteur de sa démocratisation. Et si le célébrissime TOP500 continue de susciter des luttes intenses de prestige, il ne représente aujourd'hui que le haut d'une pyramide dont la base s'étoffe et attire des utilisateurs qui n'aurait pas imaginé y recourir il y a encore quelques années.

MYTHE N° 2 :
LE CALCUL INTENSIF EST LA CHASSE GARDEE DES AMERICAINS ET DES JAPONAIS

Encore une idée reçue qui s'explique par l'histoire telle que nous l'avons esquissée ci-dessus. En effet, le modèle initial de l'industrie du calcul intensif le plaçait d'office comme une activité extrêmement onéreuse et tributaire d'aides importantes. Dans ce contexte, seuls les Etats-Unis ont eu les moyens et la volonté politique de subventionner son développement de façon suivie et relativement cohérente. Dans les années 80, le Japon avait bâti une stratégie ambitieuse dans tous les domaines de l'informatique et s'est lancé dans le développement d'ordinateurs vectoriels qui pendant un certain temps a menacé le quasi monopole américain. Avec la prise de pouvoir du modèle « cluster de SMP », basé sur l'intégration d'éléments de grande diffusion largement accessible, la barrière d'entrée dans ce domaine s'est singulièrement abaissée. Cette redistribution met l'industrie du calcul intensif à la portée de nombreux pays qui ont le savoir faire d'intégration de matériel et logiciel à grande échelle. Ainsi, selon le dernier classement TOP500, le système le plus puissant au monde est actuellement chinois. Bull, vénérable société française qui périclitait lentement, a trouvé son salut en développant des systèmes de calcul intensif. Le plus puissant ordinateur en Europe, Tera100, installé au CEA/DAM en est un exemple, et le système « Curie » acheté par le GENCI portera également les couleurs de Bull. Les années à venir verront d'autres entrants, russes, indiens ou autres encore.

Reste qu'en termes de puissance de calcul installée, les Etats-Unis sont toujours loin devant avec plus de la moitié du total général. Ceci reflète la tradition de l'utilisation de cet outil, largement explicable par le poids du passé. Mais la croissance considérable des infrastructures mises en place en Chine en si peu de temps, le rattrapage opéré par l'Europe et plus particulièrement la France avec notamment l'initiative PRACE laissent augurer un avenir plus équilibré.

MYTHE N° 3 :
SEULES LES (TRES) GRANDES ENTREPRISES OU ORGANISMES PUBLICS Y ONT ACCES

Avec la démocratisation du calcul intensif, ce mythe appartient également au passé. Nous avons mentionné précédemment l'importance du coût de possession et d'opération de l'outil

informatique pour justifier ou non son emploi. L'autre élément de taille à considérer est l'apparition de logiciels de simulation de plus en plus performants et accessibles. La simulation est devenue, pour reprendre une très belle expression d'un rapport américain, le troisième pilier de la science, avec la théorie et l'expérimentation. La modélisation permet de prévoir les performances et le comportement d'un produit avant même de l'avoir construit. On connaît ainsi les gains qu'apporte la simulation aux industries du transport ou du bâtiment, évitant les coûteux prototypes ou tests destructifs. Mais ces techniques trouvent leur voie un peu partout, même dans des PMEs où on a du mal à le deviner. De nombreuses anecdotes sont connues, telle la coopérative agricole qui a recouru à la simulation sur une plate-forme de calcul intensif pour concevoir l'emballage utilisé pour sa production de pêches…

MYTHE N° 4 : L'AVENIR DU CALCUL INTENSIF PASSE PAR L'UTILISATION DES GPGPU

La désaffection des calculateurs vectoriels au profit des architectures parallèles basées sur l'intégration d'éléments de grande diffusion a tout de même laissé un vide pour certains types d'applications qui n'arrivent à exploiter qu'une partie de la puissance théorique maximale, l'exemple classique étant les prévisions météorologiques qui ont été les derniers défenseurs des machines vectorielles. Depuis plusieurs années se pose périodiquement la question comment « augmenter » les architectures clusters pour améliorer le traitement vectoriel. Rapidement les différentes options envisagées se sont cristallisées sur l'emploi opportuniste de cartes dérivées des contrôleurs graphiques de PC qui ont été baptisées GPGPU (General Purpose Graphical Processor Unit). Cette évolution technologique apporte aujourd'hui, il est vrai, des résultats spectaculaires dans le haut de la pyramide (cf. résultats publiés dans le dernier TOP500 sur le célébrissime benchmark Linpack). Cependant, malgré les efforts intenses de la recherche, il est encore très difficile d'obtenir des améliorations équivalentes dans l'application lambda d'un utilisateur. On peut également observer le manque de standard universellement accepté, ce qui nous paraît justement aller à l'encontre de l'objectif de plates-formes de grande diffusion et de portabilité des applications.

Si la direction est clairement perçue par les principaux acteurs de l'industrie, des implémentations divergentes s'affrontent actuellement. NVIDIA, le plus populaire actuellement, propose sa solution Fermi qui est basée sur une connexion lâche (PCI Express) avec les cœurs des processeurs, ce qui implique une évaluation délicate entre les gains du temps des calculs déportés par rapport au temps perdu pour la communication entre processeurs et coprocesseurs. Consciente de la faiblesse que représente l'absence d'offre CPU, NVIDIA vient de prendre une décision radicale et audacieuse en adoptant ARM, architecture prévalente dans les applications basse consommation (téléphones, ultra-portables,…) plutôt que de chercher une source x86. AMD vient d'annoncer la sortie prochaine de sa technologie « Fusion » qui rassemble sur un seul chip CPU et GPU, dont on peut espérer justement une réduction drastique des temps de communication entre les deux. Intel, enfin, a annoncé à ISC'10 « Knights Corner », une réorientation du projet Larrabee (initialement annoncé comme processeur graphique) visant à en faire un élément clé dans les systèmes dédiés au calcul intensif. Il est clair que le concept décantera dans les années à venir, mais à notre avis, ce n'est que lorsque cette accélération sera disponible avec un couplage fort au(x) CPU(s) qu'elle pourra être considérée comme susceptible de devenir un standard pour produits de diffusion de masse. Une analogie peut être établie à ce sujet avec les opérations sur nombres flottants qui ont un certain temps été confiées à des

coprocesseurs avant de devenir partie intégrante du CPU. NVIDIA avec CUDA et AMD avec OpenCL ont pris un peu d'avance, mais l'issue de la bataille à venir est loin d'être jouée.

Une chose est certaine : l'avenir du calcul intensif est dans les processeurs hétérogènes **fortement** couplés et non à l'épiphénomène qui utilisait des composants discrets « plaqués » sur des systèmes. Le choc prévisible entre les tenants de l'architecture x86-64, jouissant d'un quasi-monopole dans les hautes performances et dans le support des développeurs de logiciels versus les primo-accédants pariant sur leur avantage dans le domaine de la performance par watt s'avère passionnant et prometteur.

MYTHE N° 5 :
LE « CLOUD COMPUTING » SERA LA SOLUTION PRIVILEGIEE POUR ABORDER LE CALCUL INTENSIF

Peut-être…. Les phénomènes de mode sont tenaces, en particulier en informatique. Depuis que la bureautique et la gestion ont commencé à être accessibles comme services (signe tangible de la maturité de l'industrie) à différents niveau (infrastructure, plate-forme, application), beaucoup prédisent que le calcul intensif suivra le même chemin. Si de nombreux arguments peuvent appuyer cette prophétie (économie d'échelle et efficacité des grands centres –en quelque sorte le retour de la célèbre loi de Grosch- ; mutualisation des prix de licences, administration, maintenance ; coopération et collaboration facilitées), les différences avec le calcul intensif subsistent. La (re)concentration des serveurs issus du « downsizing » des années 80-90 a résulté de la montée continue en puissance des microprocesseurs, ce qui a déclenché la propagation des techniques de virtualisation, un seul système étant capable de se charger de multiples tâches. Comme nous l'avons mentionné précédemment, le calcul intensif nécessite au contraire l'utilisation parallèle de plusieurs systèmes. Le parallélisme en gestion est « automatique », la charge se répartissant entre les ressources de calcul partageant la même mémoire, alors que le parallélisme entre les nœuds d'un cluster est explicite et nécessite une analyse précise garantissant la proximité des traitements et des données utilisées. A titre d'exemple, mentionnons qu'il y a quelques années certains promettaient la disparition des grands centres de calcul au profit des grilles, il n'en a rien été.

Notre conviction est que seules les tâches les moins exigeantes pourront être servies par le modèle du « Cloud Computing ». Cela conviendra vraisemblablement bien aux PMEs, et c'est déjà un progrès très notable

MYTHES ET LEGENDES DE L'OPEN-SOURCE ET DU LOGICIEL LIBRE

François Letellier François, Consultant indépendant

MYTHE N° 0 :
LE MYTHE FONDATEUR

Toute légende commence par *il était une fois*... La légende du logiciel « libre » n'échappe pas à la règle. Le mythe fondateur du logiciel libre (free software) est l'épopée de Richard Stallman (RMS), hacker de génie travaillant au MIT après être passé par Harvard, qui se trouvant en proie à des bourrages à répétition de son système d'impression Xerox, tenta d'y remédier par lui-même en améliorant le pilote. Las, ledit pilote n'est fournit qu'en binaire, le code source est jalousement gardé secret par le fournisseur. Cet incident choque profondément RMS, dont les valeurs sont celles des hackers de l'époque : amour de la technologie et du savoir, mépris de la vénalité, valorisation du partage, défiance face à l'autorité, mais sens des responsabilités. Par la suite, le terme de « hacker » sera repris et dévoyé, pour désigner des individus animés d'un désir de nuire.

Stallman fut à l'origine de nombre de piliers de la mythologie du « libre » :

- le projet GNU, visant à réimplémenter sous une forme libre un système compatible Unix – qui après ajout d'un kernel par Linus Torvald en 1991 deviendra le fondement de la famille d'OS GNU/Linux.
- Le choix du terme de « free software » pour désigner le logiciel libre, avec une forte connotation libertaire qui, selon les interlocuteurs, galvanise ou irrite.
- La création des licences « copyleftées » (GNU Public Licence, puis LGPL) qui, basées sur le droit du copyright anglo-saxon, le retournent comme un gant selon l'idée suivante : si en tant qu'auteur, j'ai tous les droits sur mon oeuvre, eh bien libre à moi de les transmettre à tous, et libre à moi d'y ajouter une condition : que ceux qui bénéficient de mon altruisme s'engagent à faire de même auprès de tiers.
- La création de la Free Software Foundation, garante de la pureté de la pensée « libriste » qui este régulièrement en justice pour faire respecter les licences libres.

A l'origine, l'aventure était émaillée de facéties typiques de l'esprit hacker : GNU est acronyme « récursif » (GNU's Not Unix), pirouette dont on peut tracer l'origine dans le style fréquemment récursif des algorithmes LISP en vogue au tournant des années 80. Les « libertés » énoncées par Stallman sont numérotées à partir de zéro – comme tout tableau indexé informatique. Copy-left est un double jeu de mots à partir du copy-right. Le terme left ayant en anglais deux sens : « laisser » et « gauche », copyleft propage l'ambiguïté entre « je laisse le droit de copier » ou « le droit d'auteur avec une sensibilité de gauche ». Au fil des années, l'épopée de RMS a pris un tournant presque religieux et RMS lui-même, cheveux et barbes longs, s'est souvent produit affublé d'un costume de « St Ignucius » en référence à GNU, et à St Ignace de Loyolla, père des jésuites et missionnaire de la contre-réforme.

Bref, le « libre » s'est forgé un système quasi mythologique dans le courant des années 80 et 90. Puisque tout héros a besoin d'un adversaire, le Méchant désigné fut Bill Gates. Parmi les innombrables « crimes » de Gates, on peut citer sa défense féroce du droit d'auteur dès les années 70, le « hold-up planétaire » (pour reprendre le titre d'un ouvrage de R. Di Cosmo)

sur l'OS des ordinateurs personnels de presque toute la planète, mais aussi les marges faramineuses de Microsoft qui en ont fait, en quelques années, un mastodonte du logiciel.

L'édifice conceptuel du Libre a atteint son apogée dans le courant des années 90 alors que des coups de canifs commençaient à l'entamer. Premier affront, le fameux système « Linux » dériva son nom de celui de ce jeune guerrier qu'était Linus Torvalds, en oubliant presque le vieux sage Stallman et son combat déjà décennal. Microsoft, après avoir endossé le costume du Méchant, a contrattaqué et mené des campagnes de propagande (FUD pour fear, insecurity and doubt selon le camp adverse) pour démontrer en vrac que le monde du Libre n'était pas fiable, pas juste, infesté de cryptocommunistes, etc. Conséquence de cette Guerre des Etoiles du logiciel, des trublions californiens ont fini, au tournant du millénaire, par contester le vocable même de « logiciel libre » pour proposer celui d' « open source ». Dans une formule, elle-même devenue mythique, Eric Raymond (ESR) se serait exclamé « show us the code! » (montrez-nous le code, ou autrement dit, arrêtez le bla bla et les discours, revenons à du concret).

Précisons à ce stade que, dans ce chapitre, nous utiliserons indifféremment les termes de « logiciel libre » ou de « logiciel open-source », au risque de faire dresser les cheveux sur la tête des puristes.

Passé 2010, des astéroïdes sont nommés *Stallman* ou *GNU*, en Catalogne une rue se voit baptisée « rue du logiciel libre »... RMS a été l'artisan d'un énorme effort de promotion d'une éthique, d'une philosophie, d'un discours, d'un arsenal juridique, presque d'un dogme.

Tout mythe est un mélange de vérité historique et de réécriture romancée de l'histoire. Ainsi en est-il du mythe zéro du logiciel Libre. Comme après la Génèse vient l'Exode, puis plus loin les livres historiques, le mythe fondateur a maintenant cédé la place à une pratique quotidienne, universelle, sécularisée, du libre et de l'open-source dont le récit détaillé serait laborieux.

Aujourd'hui, tout pousse à penser que la dynamique du partage et de l'ingénierie collaborative est une tendance naturelle dans le monde du logiciel (nous y reviendrons) et que l'époque des éditeurs 100% propriétaires fut plutôt une parenthèse historique. Ancrée dans la culture et la pratique mathématique, l'informatique ne protégeait initialement pas les programmes (pas plus que les théorèmes). En 2011, seuls les dinosaures du logiciel se retranchent encore derrière des barricades en conspuant le « libre ».

Car le libre, ou l'open-source, est en fait au centre du processus d'innovation dans les TIC.

MYTHE N° 1 : TOUS DES SUIVEURS, POINT D'INNOVATION

Linux ? Toutes les bonnes idées viennent d'UNIX. Open Office ? C'est pour ceux qui n'ont pas les moyens de payer MS Office. GIMP ? Un clone de PhotoShop en moins bien... La liste est longue des logiciels libres qui, peu ou prou, sont semblables à une offre commerciale. Au jeu des *feature-lists* (listes de fonctionnalités), les solutions libres ne sortent pas toujours gagnantes. Elles sont fréquemment soupçonnées de reprendre toutes les innovations issues de leurs prédécesseurs propriétaires.

Inversement, les projets libres PERL, PHP, mais aussi tous les logiciels d'infrastructure d'Internet, pour n'en citer qu'une poignée, sont nés, se sont développés, sont devenus des standards de fait. *IIS ? A la traîne derrière NCSA Httpd. Oracle ? Ingres était sous licence BSD quatre ans plus tôt. Mac OS X ? Un FreeBSD avec un noyau libre Mach...*

Des chercheurs ont évalué que le taux de projets « innovants » parmi les projets phares de SourceForge est équivalent au taux d'innovation dans le monde du logiciel propriétaire : entre 10% et 15%.

Innover pour innover n'est pas la panacée. GIMP ne fait peut-être guère mieux que PhotoShop. Mais ses créateurs mettent à la portée de tous une technologie de traitement d'images. Ce faisant, ils contribuent à la banalisation de cette technologie. La banalisation est le pendant de l'innovation : sans ce double mouvement, d'innovation dans un premier temps, de banalisation par la suite, les innovations ne diffuseraient pas dans la société, ne serviraient pas au plus grand nombre. Internet Explorer ou Mozilla Firefox ? Voilà deux rivaux qui, à quelques détails près, se valent ; ils rendent le même service, avec un style différent. La technologie du navigateur web est, aujourd'hui, banalisée. En conséquence, elle se répand universellement et devient un outil de base pour une foultitude d'autres applications – ou usages. On notera que si Internet Explorer reste propriétaire, il est gratuit. Lorsqu'une technologie est entièrement banalisée (« commoditisée » selon un barbarisme fréquent), son prix de marché est à peu près égal à son coût de fabrication marginal. Dans le cas du logiciel, ce coût est nul. La technologie est devenue gratuite.

Que penser alors d'un Apple, qui s'emparant des fondements open-source, et gratuits, que sont FreeBSD et Mach, assemble un Mac OS X, système d'exploitation propriétaire et... payant ? Dans cet exemple, un socle banalisé a permis à un acteur commercial de créer de la valeur ajoutée en spécialisant, en complétant, la base gratuite et ouverte. Une appropriation, en sorte, non exclusive, mais parfois regardée d'un mauvais oeil.

L'approche réductionniste consistant à comparer, projet libre contre logiciel commercial, qui innove et qui copie, est stérile. Le schéma d'ensemble, lui, met en évidence que les bases de code open-source sont de formidables courroies de transmission de l'innovation entre les acteurs – les uns commerciaux, les autres publics, certains dédiés à la recherche, d'autres mêmes étant de simples particuliers. Au niveau européen, le recours à des dynamiques open-source épargne à l'industrie des TIC le tiers de son effort de R&D – qu'elle peut investir ailleurs – simplement parce qu'elle n'a pas à réinventer la roue, ni à payer pour l'utiliser. Dans une inspiration, certains innovent – parfois en libre, parfois en propriétaire. Puis dans une expiration, la technologie est banalisée : libération de code propriétaire, apparition d'un substitut open-source à une offre commerciale, ou bien même intégration d'une technologie open-source dans un logiciel gratuit (gratuiciel, freeware) propriétaire. Observez les mentions légales dans Acrobat Reader : vous verrez combien de projets open-source y sont utilisés !

MYTHE N° 2 ET 2BIS : LES LOGICIELS OPEN-SOURCE SONT PLUS FIABLES (OU MOINS FIABLES) QUE LES LOGICIELS PROPRIETAIRES

Ainsi donc, la comparaison point à point, logiciel par logiciel, ne fournit pas de clef pour une compréhension d'ensemble du mouvement du « libre ». Il n'empêche que les arguments fusent, entre avocats et détracteurs d'un camp ou de l'autre. Au nombre de ceux-ci : la question de la sécurité...

Les partisans du modèle propriétaire préconisent une approche de « sécurité par l'obscurité » consistant à garder secret les recettes de fabrication des logiciels, donc leur code source. Ce faisant, ils prétendent compliquer la tâche d'individus malveillants. Dans un logiciel libre, prétendent-ils « n'importe qui peut insérer du code malveillant ». De plus, en cas de panne ou de problème majeur, il n'y a personne contre qui se retourner. Pas de contrat de

maintenance, pas de responsable, pas de gorge à trancher ni de possibilité au DSI d'ouvrir un parapluie pour se protéger.

La diatribe sonne bien, mais se révèle totalement erronée. La stratégie de sécurité par l'obscurité n'apporte aucune garantie : ni contre les initiés internes, personnels malveillants des producteurs de logiciel eux-mêmes, ni contre les attaquants extérieurs suffisamment déterminés (capables par exemple de désassembler et désobfusquer un code exécutable). Pire, elle empêche à des utilisateurs initiés, mais bienveillants, de s'assurer de la fiabilité des systèmes, de vérifier l'absence de chevaux de Troie et autres backdoors ou malware. Ainsi la plate-forme propriétaire Wintel (Windows sur processeur Intel) a-t-elle battu, au long de ses versions successives, des records de vulnérabilités aux virus. La société McAfee, commercialisant un anti-virus, annonçait le chiffre de 400.000 virus recensés au tournant 2008. Mentionnons Stuxnet, ver informatique ciblant la plate-forme SCADA de Siemens, sous Windows, déstinée à piloter (entre autres) des centrales nucléaires...

Outre le code malveillant, qui utilise les failles du système, la multiplication de bugs en toutes circonstances (du bogue de l'an 2000 Y2K aux ratés d'Ariane 5, détruite lors de son lancement inaugural suite à une simple négligence de calibration d'une grandeur entière) démontre que les logiciels propriétaires pâtissent d'un problème général au logiciel : ce sont des systèmes ultra complexes et les humains qui les conçoivent ne sont pas à l'abri des erreurs.

C'est précisément à la faillibilité humaine que les avocats du logiciel « open-source » prétendent remédier. Si une personne est faillible, un groupe étendu d'observateurs ayant accès au logiciel et même à son code source, multipliera par contre les chances de découvrir les bugs et de les résoudre : « aucun bug ne résiste face à une multitude d'yeux ». De plus, les projets open-source communautaires bien organisés travaillent autour d'une « base de code » centralisée en utilisant un système de gestion de versions qui trace toute modification. Nul ne peut y insérer de code, malveillant ou non, sans l'aval d'un petit nombre de gardiens du temple, que l'on appelle souvent les « committers ». Ceux-ci sont cooptés par le leader du projet.

Pourtant, « open-source » ne veut pas dire code de qualité. Si une vingtaine de milliers de logiciels libres sont matures et largement adoptés, donc a priori fiables, le reste des projets (soit des centaines de milliers) ne sont maintenus que par une poignée de développeurs, souvent un ou deux, et faiblement adoptés. Pour ceux-ci, la théorie de la multitude d'yeux ne s'applique plus.

Ainsi, dans le monde de l'open source l'évaluation de la qualité du logiciel nécessite des méthodes spécifiques. La qualité du code lui-même importe, mais aussi la taille de la communauté, le soin apporté à la gestion de la base de code et la gouvernance sous-jacente pour l'attribution des rôles dans la communauté. En fond de plan se pose la question des acteurs qui pilotent ou contribuent au projet : s'agit-il d'individus, d'universitaires, de sociétés commerciales ? Quel est leur modèle économique, leur taille, leur politique ? Les péripéties subies par MySQL après son rachat par Sun, puis MySQL et Open Office après le rachat de Sun par Oracle, doivent rappeler que même les projets soutenus par les sociétés les plus en vue ne sont pas à l'abri d'un changement de cap. Dans ce cas, les licences open-source permettent à chacun de prendre le destin de son application en main, voire à un groupe de créer un « fork » dans le projet. Il n'en va pas de même lorsqu'un éditeur propriétaire décide d'arrêter la commercialisation et le support d'un de ses produits : dans ce cas, l'utilisateur peut continuer à utiliser le logiciel – mais doit faire une croix sur le support correctif.

D'ailleurs, les utilisateurs de logiciels propriétaires se plaignent souvent de l'attitude des éditeurs, peu soucieux de traiter promptement les bugs, renvoyant leur correction à la prochaine mise à jour (parfois payante) sinon aux calendes grecques. Côté open-source, la riposte s'est organisée. Ne serait-ce qu'en France, des centaines de SSII se sont spécialisées dans les logiciels libres. Elles sont en mesure de proposer des contrats de formation, support, maintenance sur un logiciel ou un bouquet de logiciels. Dans ce cas, une « plate-forme » composite regroupant plusieurs logiciels open-source indépendants (mais inter-dépendants) est assemblée et maintenue par la SSII prestataire, pour le compte du client. Des retours d'expérience repris dans la presse ont mis en lumière la pertinence de ce mécanisme, et la satisfaction des utilisateurs – grands comptes – qui y ont recours : les temps de prise en compte et correction d'incidents peuvent se compter en heures, là où des éditeurs propriétaires se feraient tirer l'oreille pendant des mois. Outre les contrats de prestation personnalisés, des « éditeurs open source » (c'est à dire des sociétés de logiciel ayant une capacité de R&D interne et distribuant leurs logiciels en masse sous des licences open source) ne facturent pas de coût de licence, mais proposent optionnellement un ensemble de services (maintenance corrective voire évolutive) sous forme de souscription : tel est le cas de distributions Linux comme Red Hat, qui cible les grands comptes.

MYTHE N° 3 :
LES GRANDS COMPTES N'UTILISENT PAS DE LOGICIEL OPEN-SOURCE

Non les grands comptes aussi utilisent de l'open-source. Seulement voilà : ils ne le savent pas encore tous, du moins pas en haut lieu. En 2005, différentes études convergeaient pour estimer qu'à l'horizon 2010, 80% des grands comptes utiliseraient du libre pour leur infrastructure logicielle (systèmes d'exploitation, serveurs d'applications, etc). On aura compris que ce chiffre de 80% est symbolique et prudent : autant dire « tous les grands comptes » -si l'on comptabilise aussi les logiciels libres présents dans les routeurs ou embarqués dans les logiciels propriétaires (voire les téléphones sous Android !). Chose plus étonnante : un tiers des responsables interviewés en grands comptes déclaraient *ne pas* avoir recours au logiciel libre... Situation qui pourrait se résumer par la formule suivante : « Nous n'utilisons pas de logiciel libre pour notre infrastructure, nous leur préférons MySQL et Apache ! »

Historiquement, l'entrée de l'open source chez les grands comptes s'est plutôt faite par la petite porte. Les développeurs, pour leurs besoins internes, ont utilisé, souvent sans l'aval des services juridiques, des composants logiciels sous licence open source. Depuis quelques années, il faut noter que les développeurs fraîchement sortis d'écoles ou de l'université ont recours, le plus naturellement du monde, à une myriade de frameworks et d'outils de développement « libres » : la technologie Java, si présente chez les grands comptes précisément, doit entre autres son succès à toutes les librairies (de Spring à Hibernate) ou autres outils de développement (de JBoss à Eclipse) disponibles librement pour les développeurs. La « pile » LAMP (Linux/Apache/MySQL/PHP) est devenue quasiment incontournable dans les cursus de tous les informaticiens qui, de près ou de loin, touchent au web – autrement dit, tous. Le seul point noir de cette situation est le déficit persistant de formation, chez les nouveaux diplômés techniques, aux aspects juridiques du logiciel libre.

Ainsi en est-il : les grands comptes utilisent du logiciel open source. Les motivations initiales sont pécuniaires : si « libre » ne veut pas dire gratuit, l'absence de coûts de licence présente des avantages certains. A commencer par la possibilité d'essayer et de commencer à déployer des pilotes à moindre frais. Par la suite, en cas de déploiement plus massif ou pour des

applications critiques, le recours à des prestations de support, ou les coûts internes de maintenance, viendront alourdir la facture – mais graduellement. En cas de migration d'une version à la suivante, seuls les frais de conduite du changement (inévitables) seront à prévoir, et non les coûts de mise à niveau que les éditeurs aiment tant à facturer, puisqu'ils leurs assurent un revenu récurrent. Une fois adopté, les solutions libres séduisent et leurs utilisateurs déclarent les conserver principalement en raison de la souplesse qu'elles permettent dans le déploiement, l'adaptation, l'évolution.

La tendance gagne les applications métier, mais de façon plus limitée. L'explication est double : en premier lieu, les applications très spécialisées ne peuvent pas aisément regrouper une communauté large d'utilisateurs. Leur développement en « open source » trouve ses limites. D'où une seconde conséquence : les applications « métier » ont tendance à se scinder en deux : un socle technologique générique à large audience et une spécialisation fine adaptée à une seule société. Deux exemples : les « portails » d'entreprise sont désormais déployés sur des moteurs de portail, spécialisés pour les besoins du site de l'entreprise ; idem pour les applications de gestion intégrées, maintenant basées sur des socles génériques programmables, le détail des fonctionnalités étant développé spécifiquement pour chaque entreprise.

Les applications « métier » ont donc tendance à éclater en un socle technologique et une fine couche de spécialisation. Le socle se banalise, par une tendance économique naturelle qui consiste à rationaliser (donc mutualiser) le développement de tout ce qui n'apporte pas un différenciateur fort. La sur-couche devient spécifique à un seul compte. Ce mouvement vaut quelque soit le modèle de licence : l'ERP SAS est un outil générique que l'on spécialise, en faisant souvent appel à des consultants dont les journées facturées ont pour objet de permettre l'adaptation fine aux process de l'entreprise. Ainsi le socle des applications métier devient-il un composant d'infrastructure – et le mécanisme de banalisation qui s'enclenche ouvre la porte à l'open-source. On voit arriver des ERP open source. Pour ce qui est des moteurs de portail, la vague est déjà passée ! La couche métier, de son côté, est plutôt à ranger dans le développement spécifique. Pas véritablement « open source », car non partagé, mais finalement non partageable, par définition.

MYTHES ET LEGENDES DES LOGICIELS LIBRES

Jean Christophe Elineau, président du pôle AQUINETIC
Yvon Rastteter, ARTS.SOFT

MYTHE N° 1 :
LE LOGICIEL LIBRE EST GRATUIT

Un des contre-sens les plus courants dans la thématique « Logiciels Libres » consiste effectivement à dire qu'un logiciel libre est un logiciel gratuit.

Il faut savoir qu'un logiciel libre n'est pas forcément gratuit même si pour la plupart d'entre eux, c'est effectivement le cas. Ces logiciels sont alors téléchargeables sur de nombreux sites internet, spécialisés notamment. La confusion vient de fait que la langue anglaise utilise l'expression « Free Software » pour ce que nous appelons nous, « logiciel libre ». Or, en anglais, « free » peut aussi bien signifier « libre » que « gratuit ». Le terme « Free Software est donc très souvent mal interprété.

Il existe autour du logiciel libre, plusieurs modèles économiques et certains d'entre eux permettent notamment de vendre des logiciels libres (modèle de la double licence notamment ou l'éditeur peut alors proposer une version communautaire gratuite mais aussi une version professionnelle payant). C'est par exemple notamment le cas pour la solution trixbox, solution libre de téléphonie à base d'Asterisk.

Des versions payantes, destinées à des entreprises, sont commercialisées par des éditeurs, avec support technique et documentation complète. La société Red Hat, société américaine fournit par exemple son produit « Red Hat Enterprise Linux » en basant sur des services avec vente de maintenance, formations …

Vous trouverez en conclusion de la thématique, un document de l'APRIL (Association française ayant pour objet la promotion et la défense du logiciel libre) ayant pour intitulé « le logiciel libre, comment ca marche ? ». Il permet de mieux comprendre le concept que nous défendons.

MYTHE N° 2 :
LE LOGICIEL LIBRE DETRUIT LA VALEUR AJOUTEE DE L'INDUSTRIE DU LOGICIEL

La valeur ajoutée de l'industrie du logiciel porte sur la vente des progiciels d'une part et les services associés à l'adaptation, l'exploitation, la maintenance et des logiciels d'autre part. L'analyse du prix de revient d'un progiciel fait apparaître des frais importants concernant le marketing et un coût de développement réparti entre le nombre de licences vendues qui est d'autant plus faible que le nombre de licences est important.

On est dans un modèle économique qui vise à créer de la rareté alors que le coût marginal pour produire une nouvelle version du logiciel est quasiment nul.

Cette rareté créée profite à tous les acteurs de la filière : l'éditeur du progiciel et la société de service qui le revend à un client. Les marges peuvent être importantes, surtout dans les domaines ou un progiciel est dans une situation de quasi-monopole.

L'intérêt des consommateurs, particuliers ou entreprises, est de faire baisser le prix de ce progiciel. Ceci est possible lorsqu'un éditeur produit un logiciel offrant les mêmes

fonctionnalités, mais sous forme de logiciel libre. Il se rémunère alors sur le service offert à l'utilisateur ou sur le service de haut niveau offert à un intégrateur.

D'autre part, la forme de marketing viral, de bouche à oreille, effectué dans l'écosystème du logiciel libre est beaucoup moins coûteux que le marketing classique.

Tous les postes de la chaîne de valeur s'en trouvent ainsi réduits. Parler de destruction de valeur, c'est adopter le parti qui exploite la rente du système économique propriétaire.

Prendre le parti de l'utilisateur consiste à dire que, dans une économie numérique ouverte et concurrentielle, le coût d'un logiciel doit refléter sa réalité économique : la rareté ne s'applique pas puisque le coût de production marginal est quasiment nul.

Il est d'ailleurs intéressant d'observer que tous les acteurs du logiciel propriétaire s'appuient sur des briques en logiciel libre efficaces et performantes pour réduire leur coût de production. Il est donc inéluctable que la part des logiciels libres va croître dans le contexte de l'économie numérique.

MYTHE N° 3 :
UN LOGICIEL LIBRE N'EST PAS SOUMIS A UNE LICENCE

Voilà sans doute un des aspects les plus intéressants de la thématique : "Ce logiciel est libre donc il n'est pas soumis à licence". Mais non, le logiciel libre est lui aussi soumis à licence. On en dénombre entre trente et cinquante environ (selon classification). Ces licences sont beaucoup moins restrictives que les licences propriétaires mais elles permettent d'offrir un certain nombre de garanties aux créateurs de programmes.

Selon WikiPedia (l'encyclopédie libre), « Une licence libre est un contrat juridique qui confère à toute personne morale ou physique, en tout en temps et tout lieu, les quatre possibilités suivantes sur une œuvre :

- La possibilité d'utiliser l'œuvre, pour tous les usages ;
- La possibilité d'étudier l'œuvre ;
- La possibilité de redistribuer des copies de l'œuvre ;
- La possibilité de modifier l'œuvre et de publier ses modifications ».

On notera donc surtout la possibilité de modifier l'œuvre mais aussi l'obligation de publier les modifications. Le contributeur devient ainsi co-auteur. C'est en fait la pleine expression du droit d'auteur qui peut prendre ainsi une forme collective.

Parmi ces licences, on retiendra notamment la licence GNU GPL (GNU General Public licence, fixant les conditions légales de distribution des logiciels libres du projet GNU) ou bien encore la licence CeCILL (CEA CNRS INRIA Logiciel libre).

Le non respect de ces licences peut entrainer des poursuites judiciaires. Ce fut le cas en 2009 quand la Cour d'Appel de Paris qui sanctionna une société n'ayant pas respecté les principes de la licence GNU GPL.

MYTHE N° 4 :
LE LOGICIEL LIBRE N'EST PAS PROFESSIONNEL

Ou dit autrement : c'est une affaire de bidouilleurs qui travaillent en perruque en volant les heures de travail à leur employeur.

L'extension de l'utilisation de modules écrits diffusés et maintenus en logiciel libre prouve que ce n'est pas vrai. Le nombre croissant d'éditeurs propriétaires qui incorporent des

modules en "logiciel libre" dans leurs produits, voire les recomposent entièrement avec ces produits prouvent que ces produits sont professionnels.

Les éditeurs propriétaires ont intérêt à accréditer cette idée pour mieux vendre leurs produits.

Ils s'appuient sur le préjugé comme quoi quelque chose qui est gratuit n'est pas de bonne qualité et sur le sérieux et la solidité de leurs moyens pour la maintenance.

Il est vrai cependant que, dans certains domaines, les éditeurs et intégrateurs de logiciel libre n'ont pas atteint la taille suffisante pour pénétrer des marchés maîtrisés depuis des dizaines d'années par les fournisseurs propriétaires.

Les produits du logiciel libre se sont implantés dans les domaines émergents, celui par exemple des serveurs Web. Ils peinent à s'imposer dans des domaines comme la téléphonie ou les acteurs « historiques » dominent le marché depuis des dizaines d'années et où un offreur comme Cisco a acquis une monopole mondial par la vente de ses routeurs et a pu considérablement investir pour s'implanter sur la téléphonie et concurrencer les fournisseurs historiques.

C'est question de taille et de croissance pour atteindre la taille critique. Cependant atteindre une grande taille n'est pas nécessaire pour s'imposer sur le plan mondial.

C'est le cas de sociétés comme Talend, ExoPlatform. Même Redhat reste une société de petite taille par rapport aux grands. Reste l'évolution actuelle qui voit des gris éditeurs racheter des éditeurs en logiciel libre, comme MySQL par SUN puis Oracle, mais c'est une autre problématique. Ces éditeurs de logiciel libre font justement l'objet de convoitise à cause de leur professionnalisme !

MYTHE N° 5 :
UN LOGICIEL LIBRE N'EST PAS, OU EST MAL, DOCUMENTE

Autre mythe concernant les logiciels libres : nos amis, gentils programmeurs de solutions libres ne prennent pas le temps de rédiger des documentations techniques complètes, ni de les traduire.

Ce n'est absolument pas le cas et bien au contraire la plupart des logiciels libres sont aujourd'hui particulièrement bien documentés.

Prenons par exemple, les documentations concernant certains systèmes d'exploitation comme Ubuntu, Fedora ou autres... Les documentations proposées avec ces logiciels, n'ont véritablement rien à envier aux documentations fournies avec certains systèmes d'exploitation propriétaires. Des sites spécialisés sont même créés sur cette thématique (ex : http://doc.fedora-fr.org/).

Il existe aussi des projets comme Traduc.org qui « rassemble et soutient les projets d'adaptation française des documents et logiciels de l'informatique libre » en réunissant des traducteurs volontaires pour les projets libres.

Tout ce travail peut être, bien entendu protégé notamment par la Licence de documentation libre GNU, dont l'objet est de protéger la diffusion de contenu libre.

EN COMPLEMENT :

Les Rencontres Mondiales du Logiciel Libre (R.M.L.L) rassemblent chaque année les contributeurs du logiciel libre ainsi qu'un public généraliste de plus en plus nombreux. L'organisation des R.M.L.L. est attribuée par un comité rassemblant les organisateurs précédant de l'événement, à un G.U.L.L. (Groupe d'Utilisateurs de Logiciels Libres)

Créée en 2000 par l'A.B.U.L. (Association Bordelaise des Utilisateurs de Logiciels Libres (A.B.U.L.), cette manifestation a depuis 10 ans, sillonné l'hexagone. Ainsi, les éditions précédentes se sont elles donc déroulées successivement à Bordeaux (2000, 2001, 2002, 2004 et 2010), à Metz (2003), à Dijon (2005), à Vandoeuvre les Nancy (2006), à Amiens (2007), Mont de Marsan (2008) et Nantes (2009).

Pour 2011, la manifestation prendra racine dans une ville symbolique pour l'Europe, en l'occurrence Strasbourg. Mais plus intéressant encore, 2012 semble être parti pour être l'année de l'exportation de l'événement en dehors de la France pour la première fois car c'est la ville de Liège en Belgique qui a retenue l'attention du comité de sélection.

Mais intéressons nous d'un peu plus près au public qui fréquente l'événement et notamment aux pays représentés. En 2008 à Mont de Marsan, ce ne sont pas moins de quarante pays qui étaient ainsi présents pendant les cinq premiers jours du mois de juillet. : Espagne, Allemagne, Angleterre, Pays-Bas, Irlande, Suisse, Venezuela, Canada, Etats Unis, Russie, Asie et de nombreux pays Africains (et ceci malgré les conditions d'obtention des visas particulièrement difficiles). Je m'excuse par avance auprès des pays que j'oublierais dans cette liste à la Prévert.

Cette diversité permet donc des rencontres particulièrement enrichissantes mais justifie surtout l'appellation de Rencontres MONDIALES.

Document de l'**APRIL** (Association française ayant pour objet la promotion et la défense du logiciel libre)

2° PARTIE : ASPECTS SECURITE

MYTHES ET LEGENDES DE LA SECURITE DE L'INFORMATION

Gérard Peliks, CASSIDIAN
an EADS Company

LES AGRESSIONS, ÇA N'ARRIVE PAS QU'AUX AUTRES

Bien calé dans votre fauteuil, vous lisez votre messagerie, parfois vous participez aux forums sur les vulnérabilités et les menaces pouvant peser sur votre système d'information, et de temps en temps vous prenez connaissance des dernières alertes des CERT.

Oui, bien des gens n'ont pas de chance de se faire ainsi agresser. Mais pas vous ! Parmi les dizaines de milliers de logiciels malfaisants qui tournent en permanence sur les réseaux, guettant la moindre faille autour de votre PC, comment faites-vous pour toujours passer au travers ? Qu'il est merveilleux, ce sentiment de sécurité qui entoure votre Information ! Sentiment de bien-être encore accru par l'assurance que les contre-mesures que vous avez mises en œuvre, en particulier votre antivirus et votre firewall personnel vous garantissent de ne jamais être concernés par les horreurs qui se passent chez les autres !

Mais la réalité est que la sécurité de l'Information, avec laquelle vous vivez en apparence, est un mythe ! L'insécurité est l'état normal et, comme vos voisins, vous subissez aussi des agressions et parfois celles-ci passent et font des dégâts.

Le véritable danger d'ailleurs n'est pas tellement au niveau des menaces qui vous environnent mais se situe entre votre chaise et votre clavier. Le véritable danger, pesant sur votre information, c'est vous, si vous ne mesurez pas combien est dangereux le monde qui vous entoure.

MYTHE N° 1 : IL EXISTE DES HAVRES DE PAIX SUR L'INTERNET

Les virus, les vers, les chevaux de Troie, concernent les utilisateurs des PC sous Windows. Votre PC tourne sur une distribution de Linux (Ubuntu, Mandriva ?) et donc les virus ne sont pas dirigés contre vous, puisque sous Linux il n'y en a pas ? Erreur, il existe des logiciels malfaisants sous Linux aussi.

Alors, tournons nous vers les MAC puisque là au moins nous sommes tranquilles ? Erreur, il existe aussi des logiciels malfaisants dédiés aux MAC. Mais votre Smartphone n'est pas sous Windows et ce n'est pas un MAC ? Vous avez raison sur ce point mais c'est aussi un mythe qu'il n'y a pas de logiciels malfaisants pour Smartphones, et plus il y aura de PC sous Linux, plus il y aura de MAC, plus il y aura de smartphones et de eBooks, plus il y aura de virus qui les prendront pour cible. Et ce n'est pas tout.

L'imprimante de votre entreprise n'est pas plus à l'abri que le sont vos postes de travail. Une imprimante en réseau est, comme tout serveur, un nœud sur l'Intranet et comme tout nœud d'un réseau, elle est menacée dans son fonctionnement tout d'abord. Que diriez-vous si votre imprimante, dès qu'elle est alimentée, imprimait à longueur de journée, rame après rame, parce qu'elle serait victime d'une campagne de spam que vous ne pouvez arrêter qu'en payant une rançon ? Le chantage visant une entreprise est un marché qui commence à devenir florissant, et qui pourrait bien un jour se généraliser.

Votre imprimante pose de plus un problème côté confidentialité des informations qu'elle a imprimées. Non ce n'est pas parce qu'une main inavouable récupère systématiquement, avant vous, sur votre imprimante, les informations confidentielles que vous venez d'imprimer, encore que ça peut arriver. Ce n'est pas non plus que vous ne vous méfiez pas assez du spool. Votre imprimante a un disque dur dans lequel les impressions sont stockées. Et quand vous restituez votre imprimante à la société qui vous l'a louée, pour vous équiper d'une imprimante plus moderne ou mieux adaptée, vos informations résident toujours sur son disque dur. Et voilà comment, des informations confidentielles depuis longtemps stockées sur une imprimante, alors que ses utilisateurs n'en avaient pas conscience, changent de main.

On a aussi beaucoup parlé des dangers que font courir les documents de la suite Office de Microsoft, suite aux macrovirus qui présentent effectivement un réel danger. Heureusement, la transmission de documents au format PDF est la solution ? Elle ne l'est plus. Les fichiers PDF, qui peuvent être aussi contaminés, représentent aujourd'hui un des trois principaux vecteurs d'infection.

Alors vers quoi vous tourner ? Sur 360 degrés, vous êtes menacés. Il faut apprendre à vivre dangereusement et comme il n'est pas possible d'éliminer tout danger, il faut chercher à le réduire à un niveau acceptable. C'est ce qu'on appelle le risque résiduel, qu'il faut savoir accepter et gérer.

MYTHE N° 2 :
LES EXECUTABLES EN ".EXE", VOILA LE DANGER !

Au début, il y avait les virus, constitués d'instructions qui s'accolent à un programme exécutable. Le virus libère sa charge létale quand le programme, auquel il est accolé, s'exécute. Si vous ne lancez pas l'exécutable contaminé, le virus reste inactif. Et comme le virus modifie la taille de l'exécutable, en fonction du contenu et de la taille de ses instructions, la modification qui est la signature du virus, une fois connue, peut être éradiquée de l'exécutable pour le faire revenir à son état sain. C'est ainsi que procèdent les anti-virus. Contrairement à ce qu'on croit généralement, les virus ne se dupliquent pas. L'infection ne peut se répandre que si on transmet l'exécutable contaminé, par exemple en attachement à un e-mail.

Mais Il existe une autre famille de logiciels malfaisants, les vers (worms en anglais) qui eux ne sont pas attachés à un exécutable. Ils sont eux-mêmes des exécutables autonomes et ils investissent votre PC en passant, à travers le réseau, par une faille non couverte affectant un des logiciels que vous utilisez. Une fois installés chez vous, ils se dupliquent et, toujours par le réseau, se répandent un peu partout chez les autres utilisateurs. On pourrait juste vous reprocher d'être connectés !

Les vers forment une famille bien plus nombreuse et bien plus dangereuse que les virus, et c'est pourquoi, croire que n'exécuter que des fichiers ".exe", ".zip" ou autres fichiers avec du code exécutable de confiance, pour ne pas être infecté, est un mythe.

Croire que la messagerie est le seul vecteur d'infection avec les fichiers exécutables attachés aux messages que vous recevez est aussi un mythe. Le vecteur principal d'infection aujourd'hui est le Web.

Il suffit de naviguer sur des pages Web contaminées et vous récoltez des programmes malfaisants contenus dans des pages que votre navigateur télécharge avant de les interpréter. Une page Web, apparemment anodine, peut contenir beaucoup d'éléments exécutables, comme des applets Java, des ActiveX, des codes JavaScript, des Flashs … Les cybercriminels

piègent des sites, même les plus honnêtes, surtout les plus lus. C'est ce qu'on appelle l'infection "drive by download" très répandue. Aujourd'hui le Web devance la messagerie comme premier vecteur d'infection et. Les fichiers PDF viennent juste après la messagerie dans le classement des éléments dangereux.

MYTHE N° 3 : LES CYBERCRIMINELS VEULENT DETRUIRE VOTRE SYSTEME D'INFORMATION

Attaquer les systèmes d'information pour éprouver la délicieuse poussée d'adrénaline qui vient avec l'agression du système d'information d'une entreprise, si possible grande et connue, pour le détruire et en entendre ensuite parler; attaquer les réseaux pour prouver qu'après tout on n'est pas incompétent, et les plaintes que poussera l'entreprise en seront une preuve éclatante, c'est du passé et ce type d'attaques ludiques est devenu un mythe, sauf si une cyberguerre se déclenche ou si le cyberterrorisme frappe, ce qui est un autre problème.

Aujourd'hui les cybercriminels attaquent le réseau pour un motif tout aussi inavouable que pour le détruire et leurs attaques sont plus feutrées. Ils mènent leurs attaques pour gagner de l'argent facilement et sans prendre trop de risques. Il est moins périlleux en effet d'attaquer les coffres virtuels d'une banque située à 10 000 km de distance, par l'Internet, depuis un pays où la législation concernant le cybercrime est quasi inexistante, en utilisant un PC et une connexion haut débit, que d'utiliser un camion bélier, un fusil à pompe et un chalumeau, sur place.

Attaquer pour des raisons pécuniaires change les attaquants, les attaques et les cibles. Les attaquants sont souvent des groupes de cybercriminels, parfois sans compétence informatique particulière, mais utilisant des outils conviviaux qu'on trouve dans l'underground d'Internet, les "kiddies tools". Vous y trouvez même des kits "prêts à l'emploi".

Ces attaques sont silencieuses et les vecteurs d'infection, comme chevaux de Troie et bots spécialisés s'insèrent sans dégâts visibles dans les systèmes d'information des victimes ciblées. Aux virus dévastateurs succèdent les familles de chevaux de Troie, qui sont des bots, pour relayer les attaques, et des vers qui ne veulent surtout aucun mal à votre outil de travail et à vos informations, seulement à vos comptes bancaires. Bien au contraire, ils ont intérêt à ce que tout marche parfaitement chez vous. Mais tapis au fond de votre disque dur, ils observent. Les logiciels malfaisants attendent leur heure…

Et quand vous saisissez l'adresse Web de votre établissement bancaire, alors ils se réveillent et captent l'information que vous entrez : login, mot de passe, numéro de compte, date d'expiration de votre carte de crédit, tout est intercepté et envoyé au cybercriminel. Et ainsi le marché du renseignement sur les victimes potentielles est alimenté et rapporte gros. Il existe des keyloggers qui vont chercher l'information au niveau des touches du clavier que vous utilisez.

Vous pouvez certes chiffrer votre information sur votre PC, mais ce que vous tapez sur les touches de votre clavier, c'est de l'information en clair. La question hélas ne sera pas, avec la généralisation de la cybercriminalité, de savoir si vous avez ou pas un cheval de Troie dans votre système d'information, mais plutôt combien vous en avez, qui se battent en duel pour être peu nombreux à bénéficier de vos ressources informatiques.

MYTHE N° 4 :
LA SECURITE DE L'INFORMATION EST UN CENTRE DE COUT

Bien entendu s'équiper des matériels et logiciels indispensables, s'entourer d'experts sécurité compétents a un coût. Maintenir et bien gérer le système, établir des tableaux de bord conformément à sa politique de sécurité, et aux standards, exploiter les résultats des évènements, des vulnérabilités, des non-conformités n'est pas une tâche anodine et mobilise des ressources humaines et pécuniaires.

Le coût de la sécurité pèse en général sur le budget informatique, et constitue parfois, hélas pour les victimes futures, une variable d'ajustement des budgets, surtout en temps de crise.

Mais l'insécurité a-t-elle un coût ? Si une entreprise victime d'une agression qui lui a fait perdre son fichier clients, l'historique de ses commandes, ses secrets de fabrication, son image de marque, et entaché la moralité de ses dirigeants, est appelée à disparaître à court terme après une attaque réussie, le coût de l'insécurité sera supporté par l'ensemble de l'entreprise, quand celle-ci devra fermer ses portes.

Mais si vous croyez que la sécurité est trop chère… essayez l'insécurité" ☺

MYTHE N° 5 :
LES ATTAQUES VIENNENT DE L'EXTERIEUR

Le côté obscur de la force qui pèse sur votre information peut certes venir de l'extérieur où une cohorte d'individus malfaisants menace vos finances et vos ressources. Ca ce n'est pas un mythe. Mais le mythe serait de croire que les méchants sont toujours à l'extérieur.

Le firewall qui isole votre réseau en bâtissant un périmètre de sécurité autour de votre système d'information et filtre tout ce qui sort et ce qui entre conformément à votre politique de sécurité est indispensable. Mais il ne sait pas ce qui se passe dans votre Intranet.

Les systèmes d'information aujourd'hui ne sont plus des places fortes qui doivent être entourées d'un rempart imprenable. Ils se rapprochent plus de pays avec des frontières, des ports mais aussi des aéroports d'où l'on peut pénétrer sans passer par les frontières. Sans compter, pour le criminel, la possibilité d'être parachuté près d'un endroit sensible. Il faut donc sécuriser plus que le périmètre de sécurité extérieur de votre entreprise. C'est d'autant plus vrai avec les technologies sans fils, le Peer to Peer, le Cloud Computing, qui, s'ils rendent des services indiscutables, n'en ouvrent pas moins des brèches dans le périmètre de sécurité d'une entreprise. Il faut aussi mettre des contre-mesures à l'intérieur de votre réseau d'entreprise.

Les employés sont-ils des méchants quand l'occasion fait le larron ? Pas tous, bien sûr, mais il faut garder à l'esprit qu'au moins 60% des attaques réussies, ont pour origine l'intérieur de l'entreprise, ou au moins des complicités dans l'entreprise.

MYTHE N° 6 :
LE CYBERMONDE EST UN ESPACE DE NON DROIT

La multiplication des attaques, largement plus médiatisée que les peines qui pourtant frappent les attaquants qui se font prendre, peut laisser penser que le cyber monde est un espace de non-droit où les malveillants, les maîtres chanteurs, les indélicats peuvent œuvrer en toute impunité et leurs victimes se faire agresser ou plumer sans recours. Il n'en est rien.

Mais comme l'Internet ne connaît pas de frontières, il n'est pas toujours évident de déterminer quelle juridiction s'applique. Droit du sol où le serveur Web malveillant réside ?

Nationalités des agresseurs ? Nationalités des victimes ? Pays où se passe l'agression ? En France, l'article 113-2 du nouveau code pénal répond en partie à ces questions. Il s'appuie sur le principe de territorialité, établit que « *l'infraction est supposée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire* ».

Nous allons évoquer ici seulement des lois qui s'appliquent en France. N'étant pas juriste, je n'entrerai pas dans les détails. Chaque pays a ses propres lois et ses accords croisés avec d'autres pays ou communautés de pays et bien sûr les agresseurs avertis lancent de préférence leurs attaques à partir de pays où la législation est très floue et l'extradition difficile. C'est bien sûr aussi dans ces mêmes pays que sont hébergés souvent les serveurs délictueux et les maîtres des Botnets.

En France, contrairement à ce qu'on peut croire, le cybercrime est encadré. Des lois existent et la jurisprudence commence à s'étoffer. D'ailleurs, plusieurs lois datant d'avant même la généralisation de l'utilisation d'Internet sont applicables, telles la loi dites Godfrain, du 5 janvier 1985, articles L.323-1 et suivants du Nouveau Code pénal qui punit les *atteintes au système de traitement automatisé de données* et prévoit des amendes et des peines de prison même si aucune incidence directe n'a perturbé le système pénétré.

Mais le système judiciaire ne peut intervenir que si la victime ne tait pas le délit commis par l'attaquant et le préjudice subi et que si elle porte plainte.

Avec la volatilité des preuves, la difficulté de les tracer, l'anonymat facile, l'absence de frontières et une présence policière limitée, le cybermonde réunit tous les ingrédients pour être le théâtre d'un crime parfait, à moins que les victimes ne réagissent efficacement.

Si vous vous apercevez que vous avez été attaqués et avez subi des préjudices mais si vous ne portez pas plainte, l'agresseur ne sera sûrement pas inquiété. Si par contre vous portez plainte auprès de l'autorité compétente, il reste une petite chance pour que l'agresseur soit inquiété et cesse de s'attaquer à vous et aux autres. Comme avec l'Internet nous sommes tous liés, améliorer sa sécurité, c'est aussi améliorer la sécurité des autres.

Un web de signalement des infractions a été mis en place par le Ministère de l'intérieur, n'hésitez pas à l'utiliser, c'est ainsi que la vie peut devenir plus dure pour les cybercriminels :

www.internet-signalement.gouv.fr

MYTHES ET LEGENDES DES RISQUES DE CYBERGUERRE SUR LES INFRASTRUCTURES VITALES

Franck Franchin, FRANCE TELECOM

MYTHE N° 1 : LES SYSTEMES CRITIQUES SONT PROTEGES DES ATTAQUES GRACE A LEUR REDONDANCE

Dans de nombreux secteurs d'activité industrielle, 2 ou 3 fournisseurs se partagent désormais le marché des systèmes de supervision, de commande et de contrôle (les fameux SCADA), sous forme d'un duopole ou d'un oligopole. Cela entraine que la redondance des systèmes à caractère critique est souvent assurée par le même logiciel ou le même matériel, simplement dupliqués, afin de permettre une redondance à froid ou à chaud.

Que se passe-t-il donc si un système est attaqué ? On peut scénariser une attaque en cinq phases :

- Phase préparatoire de reconnaissance, infiltration et renseignement – ouverture des accès nécessaires à l'attaque
- Phase d'attaque
- Découverte de l'attaque par la victime
- Mesure de défense
- Forensique et post-mortem

Lorsque l'attaque est découverte, la victime peut adopter plusieurs stratégies : arrêter totalement le système et/ou le processus concerné ou basculer sur le système de secours. Grande question : est-ce que le système de secours a été compromis ?

Dans un avion, les commandes de vols vitales sont doublées, via des technologies différentes : câbles électriques, fibres optiques, circuits hydrauliques et passent par des chemins physiques différents. Il existe aussi des modes dégradés lorsque la redondance des systèmes est trop complexe ou trop couteuse à implémenter.

Avec un système informatique, comment s'assurer d'une vraie redondance quand le système d'exploitation est du même fournisseur, voire de la même version, sans même parler du même logiciel métier. Comment être sûr que le système de secours est vraiment 'isofonctionnel' (et donc mis à jour comme le système 'en production') ?

Si on prend comme référence la fameuse affaire Stuxnet, la préconisation de Siemens une fois l'attaque connue fut... de ne surtout toucher à rien et surtout de ne pas changer le mot de passe qui était codé en dur dans les programmes ! Le remède risquait d'être plus grave que la maladie. Rappelons qu'on parle pourtant de systèmes à plusieurs millions d'euros qui régulent et pilotent des centrales nucléaires, des usines chimiques et autres activités à risque.

Il y a donc redondance et redondance. Quand on implémente la redondance de deux baies de disques durs amenées à stocker des données très sensibles, on utilise des processus logiques et physiques de redondance à froid et à chaud (les fameux disques durs hot plug ou les modes de stockage de type RAID) mais on s'assure aussi que les disques durs eux-mêmes ne proviennent pas du même fabricant pour chaque baie. Et si ce n'est pas possible, on prend des lots fabriqués à des dates différentes pour ne pas risquer un même défaut de fabrication.

Il est beaucoup plus difficile d'appliquer cette saine philosophie dans le monde informatique des logiciels.

Un exemple très simple : imaginez que vous soyez journaliste, que votre outil critique soit votre traitement de texte et que vos missions nécessitent une disponibilité de votre outil à 100%. La solution pour s'affranchir des failles ou des attaques informatiques consisterait à avoir un ordinateur PC sous Windows et un autre ordinateur Apple sous MacOS. Au niveau logiciel, vous pourriez avoir un OpenOffice d'un côté et un Microsoft Word de l'autre. Cela fonctionnerait très bien tant que le journal pour lequel vous travaillez n'ait pas choisi d'implémenter des macros spécifiques Word qui n'existent pas sous OpenOffice. La solution serait alors d'être iso-outil et d'avoir Word sur les deux machines. Sauf que Word sous Windows et Word sous MacOS ne sont pas totalement iso-fontionnels, voire compatibles (selon l'éditeur, cela serait corrigé dans la version 2012). La seule solution définitive serait alors d'avoir deux ordinateurs PC avec Word sous Windows, l'un sous Windows Seven, l'autre sous Windows XP, par exemple. En espérant que les macros se comportent exactement de la même manière sous les deux systèmes exploitation.

Hélas, le choix est encore plus limité pour les systèmes de supervision, de commande et de contrôle en milieu industriel de type SCADA. La solution retenue pour la redondance est donc très souvent une copie synchronisée du système en production, avec bascule des données, voire des données de session. La meilleure façon d'avoir deux systèmes aux vulnérabilités strictement identiques.

Cela signifie que la meilleure redondance reste souvent la décision et l'arbitrage humain. Encore faut-il que l'attaque ait été décelée à temps. Dans l'exemple précédent de Stuxnet, l'attaque modifiait certains paramètres bien particuliers de processus industriels très complexes. Seules les victimes savent aujourd'hui réellement le temps qu'a duré l'attaque avant qu'elles ne s'en soient aperçu. Certaines centrifugeuses iraniennes ont eu des baisses de rendement inexpliquées bien avant qu'on évoque du bout des lèvres l'éventualité de Stuxnet…

MYTHE N° 2 : INTERNET EST UNE INFRASTRUCTURE CRITIQUE PRIMORDIALE

Lorsqu'on se demande si l'Internet est une infrastructure critique primordiale, la grande question à se poser est sans aucun doute : *peut-on vivre sans* ?

Bien évidemment, l'Internet a pris une si grande importance dans nos vies professionnelles ou personnelles quotidiennes, qu'il est difficile d'imaginer devoir ou pouvoir s'en passer. Tout comme il semble impensable qu'une économie ou qu'un État puisse fonctionner sans lui.

D'ailleurs, l'Histoire récente des conflits politiques ou militaires entre certains pays de l'ancien Bloc de l'Est nous rappelle que l'attaque des réseaux et des services de communication fait bien partie de la doctrine militaire et des actions de désorganisation propres à la préparation de toute velléité plus ou moins belliqueuse.

Toutefois, une simple taxinomie des services vraiment vitaux au fonctionnement d'un État, c'est à dire à sa capacité à assurer ses fonctions régaliennes, nous oblige à négliger quelque peu le grand Internet. Rappelons ici quelles sont les grandes fonctions régaliennes d'une démocratie :

- Frapper la monnaie (et gérer et protéger la devise du pays)
- Définir le droit et rendre la justice

- Assurer la sécurité du territoire et des citoyens

Au niveau du citoyen, de l'être humain, les besoins réellement vitaux sont :

- S'alimenter (eau et nourriture)
- Accéder aux soins nécessaires (médecine générale, petite et grosse chirurgie, médicaments)
- Disposer d'un hébergement convenable (chauffage, lieux d'aisance)

Le lecteur notera d'ailleurs qu'une certaine partie de l'Humanité n'a pas la chance de se poser ces questions car elle ne dispose pas, sur une base quotidienne, de ce niveau de base que nous considérons comme 'vital'…

La question est donc de savoir dans les six points précédents quels seraient les impacts d'une indisponibilité d'Internet, que ce soit suite à des attaques physiques ou logiques ou que ce soit par défaillance du réseau énergétique.

En terme de sécurité des personnes et des biens, les services de l'État (police, gendarmerie, pompiers, armées) disposent des moyens de communication nécessaires, même si certains services ont succombé aux charmes de la VoIP. Habitués aux situations de crise, ils savent mettre en place des réseaux de secours si nécessaire. Le risque résiderait éventuellement sur les incompatibilités de certains réseaux entre eux.

En terme de distribution de l'électricité et de l'eau courante, certains systèmes de supervision et de contrôle sont connectés via l'Internet. Cela peut donc poser problème. Toutefois, les fonctions critiques peuvent être assurées soient de manière autonome, soient à travers des réseaux qu'on peut qualifier de privatifs.

En terme de distribution d'eau potable et de nourriture, il est vrai que les échanges commerciaux et logistiques sont désormais basés sur des procédures automatisées de type EDI/XML et que la plupart des réseaux de négoce passent par l'Internet, sous VPN ou non. Toutefois, il serait assez facile de passer en mode dégradé, à partir du moment où les parties prenantes disposeraient des moyens de communication adéquats et que les carburants, nécessaires au transport routier, ne viendraient pas à manquer. Ces contraintes sont assez bien identifiées et prises en compte dans la plupart des plans de crises étatiques.

Restent les services de santé au sens large. Leur criticité et leurs vulnérabilités sont très variables. Toutefois, à partir du moment où l'accès à l'énergie (chauffage et électricité) est maintenu et que les communications d'urgence sont assurées, les prestations d'urgence peuvent être maintenues dans leur très grande majorité, de manière indépendant d'Internet.

Au risque de surprendre, le seul impact réellement majeur me semble être celui pouvant toucher la distribution d'argent liquide et le paiement par carte. Il convient de ne pas minimiser cet aspect qui pourrait être risque de grand désordre, voire de panique, pour les populations civiles. La plupart d'entre nous, dans nombre de pays occidentaux, ont l'habitude de ne pas avoir plus de 100 euros d'argent liquide sur eux, ce qui serait insuffisant en cas de crise impactant le réseau bancaire pendant plus d'une semaine.

Pour conclure, mon propos n'est pas de minorer les impacts graves et évidents qu'aurait une défaillance d'Internet sur notre économie mais de la relativiser sur notre vie quotidienne. Il ne s'agirait pas d'une crise humaine à grande échelle. Une grève des transports routiers ou une grève du raffinage de carburant serait bien plus grave et coûteuse.

MYTHE N° 3 :
NOUS AURONS UN PEARL-HABOR DIGITAL DANS LES DIX PROCHAINES ANNEES

Cette phrase est extraite d'une audition d'expert devant le Sénat américain en 1998. Déjà en 1993, John Arquilla et David Ronfeld faisaient trembler les Etats-Unis en annonçant la cyberguerre prochaine.

Que s'est-il passé depuis ? Des événements bien plus graves qu'un Pearl Harbor numérique: l'affaire Madoff, la crise des surprimes, le dépôt de bilan virtuel des PIGs, la Corée du Nord qui joue avec le feu. Qu'en penser ?

Tout d'abord, il y a une grande différence en terme de doctrines et d'impacts entre un Pearl-Habor numérique et une cyberguerre (voir Mythe N°5).

Les ardents défenseurs de ce mythe ont avancé plusieurs arguments au fil des ans. Dans un premier temps, il y a 10-15 ans environ, le monde devait redouter qu'une bande de méchants génies de l'informatique, ultralibertaires, altermondialistes, pirates ou terroristes, s'en prenne à nos infrastructures vitales : transport, hôpitaux, centrales nucléaires, trafic aérien, etc.

Aujourd'hui, ce sont des Etats qui cyber-combattent de manière directe ou indirecte (Russie-Georgie, Russes-Estonie) ou des Etats contre des entreprises (Chinois/Chine contre Google).

Le problème est probablement ailleurs. Les Etats-Unis vont dépenser entre 50 et 75 milliards de dollars pendant la période 2010-2015 pour leur doctrine de cyberguerre. Une manne inespérée pour les Boeing, Northrop, Lockheed et autre Thalès. Des rapports alarmistes fleurissent dans les différents cercles de lobbying européens et américains, tous financés directement ou indirectement par des tierces parties qui ont des intérêts à cette cyberprogagande.

Nous sommes dans le domaine du fantasme, quelque fois entretenu par des journalistes en manque d'un bon papier. Les réseaux du Pentagone sont attaqués des centaines de fois par jour et si on en croit Siemens, seule une petite vingtaine de systèmes Scada ont été concernés par Stuxnet et de toute façon sans impact particulier (sic).

A ce jour, le seul Pearl-Harbor réellement numérique fut probablement WikiLeaks. Et tous les moyens financiers, juridiques, diplomatiques, policiers et militaires des Etats concernés n'ont pu y mettre réellement fin, à l'heure où j'écris cette phrase (Décembre 2010).

MYTHE N° 4 :
LE CYBER-TERRORISME EST UNE MENACE IMPORTANTE

Quand on lit la presse ou les documents gouvernementaux d'origine anglo-saxonne, et particulièrement en provenance des Etats-Unis, on frémit à la simple allusion de la possible éventualité d'un acte de cyber-terrorisme. A la défense de nos amis américains, il y aura toujours un avant et un après 9/11. Il est difficile pour nous européens de

comprendre vraiment à quel point cette tragédie les a touchés au plus profond de leurs âmes et de leurs certitudes. Il convient donc de comprendre que leurs réactions étatiques, qui nous paraissent parfois endémiques ou disproportionnées, sont tout à fait normales, et légitimes, dans leur esprit.

Cela étant dit et reconnu, quel est le risque réel d'une menace cyber-terroriste ? Au risque de surprendre, je dirais pratiquement aucun. Non pas que je souhaite minimiser ce risque ou cette menace, mais simplement parce que je suis convaincu que les-dits terroristes disposent de moyens bien plus efficaces (si le lecteur me permet cette expression) pour arriver à leurs fins.

Le Dr. Dorothy Denning a donné en 2007 la définition suivante pour le cyber-terrorisme :

"...the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objections. Further, ***to qualify as cyberterrorism, an attack should result in violence against persons or property, or at the least cause enough harm to generate fear****. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples."*

La notion de 'génération de terreur' est très importante dans la doctrine de la plupart des terroristes. Je me permettrais de rajouter à la définition précédente que l'acte terroriste doit être en soit un acte de communication, qui marque les esprits, qui permet de faire les gros titres des médias pendant plusieurs jours, plusieurs semaines.

La plupart des réseaux terroristes ont deux objectifs principaux :

- Développer leur réseau de soutien et assurer le financement de leurs activités
- Creuser le fossé culturel, politique, émotionnel entre leurs partisans (ce que j'appelle les identitaires) et le reste du monde (les oppresseurs et les victimes potentielles...)

On est très proche de l'esprit des sectes.

Dans cet esprit, tout acte terroriste doit répondre de manière directe ou indirecte à ces objectifs.

Une erreur courante consiste à croire que les terroristes sont des gens irrationnels. Bien au contraire, un terroriste agit en général de manière très pragmatique et très logique. Simplement, c'est sa logique propre que nous avons du mal à comprendre, en particulier car nous refusons son mode de pensée. Un terroriste pense toujours que son action est légitime par rapport à son référentiel de pensée et/ou de croyance. Il n'a pas à justifier ses crimes car il ne se considère pas comme un criminel. Selon ses propres référentiels, c'est lui qui est la victime, le martyr, le héros.

Les organisations terroristes sont de grands utilisateurs du cyberespace. Tout d'abord, ils ont rapidement pris conscience de l'énorme capacité d'Internet, de cet espace de 'liberté de pensée et d'expression', comme outil de propagande, de recrutement et de financement (directement ou indirectement via la cybercriminalité). On a pu découvrir

dans certaines affaires que ces organisations maîtrisaient parfaitement les outils et les méthodes d'anonymisation, d'offuscation, de déni de service distribué (DDoS) et de chiffrement. On sait aussi que les plus importantes d'entre elles ont mis en place depuis plusieurs années des cellules spécialisées, à l'image de nos armées.

Ces organisations ont donc tout à fait les capacités techniques, financières et logistiques pour mener avec succès des actions et des attaques dans le cyber-espace. Quand on voit qu'une poignée de script-kiddies, défenseurs des idées libertaires de WikiLeaks, ont pu mettre à mal pendant des heures des sites bancaires comme PostFinance.ch ou Paypal, on peut aisément imaginer ce que des terroristes déterminés pourraient faire pour nuire à des intérêts vitaux des Etats cibles. Et pourtant, aucune attaque cyber-terroriste importante n'a été révélée à ce jour.

J'oserais plusieurs explications possibles.

Tout d'abord, en reprenant la définition ci-dessus, quels seraient les points d'emploi d'un acte cyber-terroriste qui concernerait les infrastructures vitales et qui serait générateur d'extrême violence et/ou d'extrême terreur. Quelques exemples viennent immédiatement à l'esprit : hacking d'un réseau de distribution d'eau, d'une centrale nucléaire, d'un réseau de contrôle ferroviaire. Mon sentiment est que le résultat serait bien faible par rapport aux moyens engagés grâce aux contrôles, aux régulations et au facteur humain qui, pour une fois, serait à notre avantage. Si on veut s'attaquer à un réseau d'eau, il est bien plus facile d'introduire des produits nocifs en aval des systèmes de capteurs, d'analyse et de protection…Si on veut mettre en danger une centrale nucléaire, il est bien plus facile de le faire de l'intérieur, voire de l'attaquer avec un commando suicide. Les récentes attaques de bases ultra-sécurisées en Afghanistan en donnent un triste exemple. Bref, le coût d'opportunité serait disproportionné par rapport à d'autres attaques possibles.

Ce n'est clairement pas un objectif prioritaire actuel des organisations terroristes alors qu'elles disposent d'armées de martyrs prêts à se faire sauter pour leur cause (je refuse d'utiliser le terme de Kamikaze par respect vis à vis de ces héros japonais).

Toutefois, mon analyse des doctrines terroristes actuelles me conduit à suggérer un risque différent : celui d'une attaque cyber-terroriste de nos infrastructures vitales comme partie d'un plan d'action coordonné plus global. Par exemple :

- Pour 'fixer' les organisations gouvernementales
- Pour désorganiser l'Etat et les populations
- Pour amplifier l'acte terroriste 'physique' principal.

Ce livre n'a cependant point le propos de définir ni de proposer des scénarios d'attaques terroristes et c'est pourquoi je n'irai pas plus loin dans les détails.

Gageons que les plus hautes autorités sont conscientes de ces risques et que des scénarios, des exercices et des plans de crise sont déjà opérationnels.

MYTHE N° 5 :
LA GUERRE DE TROIE N'AURA PAS LIEU

Au contraire des raisonnements présentés dans les 4 mythes précédents, je serai hélas bien moins optimiste pour ce Mythe N°5.

Toutes les armées et les gouvernements du monde se préparent depuis presque 10 ans à la guerre cybernétique. La question n'est pas de savoir désormais *pourquoi* ou *comment* mais *quand*.

Récemment, début 2010, Mike McConnell, ancien directeur de la NSA, avançait même que les Etats-Unis étaient en train de perdre cette fameuse cyberguerre.

D'ailleurs, sémantiquement parlant, cette Guerre de Troie numérique a déjà eu lieu. Quand le Hezbollah a piraté les flux vidéos des drones israéliens, ou quand des russes ont attaqué les réseaux bancaires et media de l'Estonie, c'étaient des actes de cyberguerre ou de cyberguerilla. Sans parler du détournement du trafic de l'Internet mondial pendant 18 minutes via la Chine, suite à une 'erreur' malencontreuse de China Telecom.

Il est intéressant de noter qu'en matière de cyberguerre, certains pays ont mis en place des unités opérationnelles offensives avant même de parler leur propre politique de défense.

Pour les experts en sécurité, ce qui fait froid dans le dos, ce n'est pas tant la débauche de moyens militaires ou privés qui semblent se préparer au pire, mais plutôt les discours de certains politiques qui clament haut et fort que leurs pays sont bien protégés et à l'abri de toute cyberattaque.

Il est bien connu que la meilleure façon de minimiser ses faiblesses, c'est de les clamer haut et fort publiquement en les considérant comme des forces !

MYTHES ET LEGENDES DES VULNERABILITES LOGICIELLES

Nicolas Ruff, EADS Innovation Works

MYTHE N° 1 :
TROUVER DES VULNERABILITES , C'EST COMPLIQUE (RESERVE AUX EXPERTS)

Dans le domaine des failles de sécurité, il y a bien deux compétences disjointes (souvent détenues par des personnes différentes d'ailleurs): la découverte des failles, et la transformation des failles en attaques (appelée *exploitation* ou simplement *exploit* dans le jargon).

Si la deuxième compétence reste et restera réservée aux experts techniques, il est au contraire à la portée de n'importe qui de découvrir des failles.

Vous avez reçu un document endommagé qui fait "planter" Word ? Vous avez peut-être entre les mains une bombe !

Vous avez rempli un formulaire en ligne et le serveur vous a retourné un message incompréhensible car vous avez un guillemet simple (') dans votre nom de famille ou dans votre mot de passe ? Vous avez peut-être trouvé un moyen de compromettre à distance le serveur !

En pratique, quiconque a pratiqué l'audit de sécurité pendant quelques années a forcément découvert des vulnérabilités dans des dizaines de logiciels pourtant largement utilisés. Il y a un fossé entre le sentiment de sécurité des utilisateurs (souvent béats devant la technologie), et la sécurité effective de leurs applications.

COROLAIRE: UN LOGICIEL QUI N'A AUCUNE VULNERABILITE CONNUE EST "SUR"

Archifaux ! Un logiciel qui n'a aucune vulnérabilité connue n'a jamais été audité sérieusement et/ou son éditeur n'a pas de processus sérieux de gestion des vulnérabilités (ce qui inclut correction et communication).

MYTHE N° 2 :
MAINTENANT QUE LA SECURITE EST DEVENUE UN ENJEU IMPORTANT POUR LES EDITEURS, LE NOMBRE DE VULNERABILITES VA DIMINUER

Il est certain que la sécurité informatique n'a jamais bénéficié d'autant de couverture médiatique (n'allons pas jusqu'à dire de moyens :). Pourtant le nombre de nouvelles vulnérabilités ne baisse pas - il a même plutôt tendance à augmenter !

La raison ? C'est que la plupart des "gros" logiciels que nous utilisons actuellement a été développée il y a fort longtemps, dans un monde très différent du nôtre. Un monde où les quelques personnes interconnectées l'étaient via RNIS, et où la principale menace était la disquette. Pour des raisons de coût et de compatibilité, ces logiciels ne sont pas prêts d'être réécrits.

Et en ce qui concerne les nouveaux logiciels qui sont développés actuellement ? Ils le sont par des stagiaires ou des sous-traitants *offshore*, qui reproduisent exactement les mêmes erreurs qu'il y a 30 ans !

MYTHE N° 3 :
TOUT LE MONDE EST TRES CONCERNE PAR LA DECOUVERTE DE VULNERABILITES CRITIQUES

On pourrait penser que la découverte d'une vulnérabilité critique dans un logiciel est un évènement sérieux qui va impliquer toutes les parties prenantes.

Pourtant l'utilisateur (ou le client, s'il ne s'agit pas d'un logiciel gratuit) ne peut pour ainsi dire rien faire : il doit attendre le correctif de l'éditeur.

L'éditeur quant à lui dispose de ressources et de connaissances en sécurité limitées (c'est pour cela que ses produits sont vulnérables ;). Il va donc au choix : minimiser la portée de la découverte, intégrer le correctif dans une future maintenance, ou proposer un correctif spécifique (parfois payant) au client.

Quant aux autres utilisateurs du logiciel, ils sont rarement prévenus : les éditeurs n'aiment pas trop qu'on parle de leurs failles sur la place publique.

Et ceci dans le meilleur des cas, car parfois l'auditeur (ou son client) sont poursuivis en justice par l'éditeur du logiciel pour violation de licence !

MYTHE N° 4 :
CORRIGER LES VULNERABILITES AMELIORE LA SECURITE DES SYSTEMES

Cela pourrait être vrai dans un monde où tous les systèmes sont mis à jour en temps réel. Malheureusement la plupart des systèmes du monde "réel" sont mis à jour entre 24h et … jamais !

Ceci est particulièrement vrai dans le domaine des systèmes embarqués (sans parler de SCADA). On peut considérer par exemple que l'énorme majorité des téléphones portables n'est pas mise à jour après sa commercialisation. Un téléphone sous Android restera donc vulnérable à toute faille affectant le noyau Linux et/ou le navigateur Chrome après sa sortie.

A contrario, il faut souvent moins de 24h à un attaquant motivé pour produire une attaque à partir d'un correctif de sécurité. Sans parler de l'auteur initial de la découverte, qui est libre de l'exploiter à loisir tant que le correctif n'est pas disponible, ce qui prend parfois des années !

Ce problème a déjà été retourné dans tous les sens - et il n'admet pas de solution satisfaisante pour toutes les parties. Il est impossible de ne pas mettre au courant les clients des failles sans en informer également les pirates.

MYTHE N° 5 :
IL EXISTERA UN JOUR DES LOGICIELS GRAND PUBLIC INVULNERABLES

Est-ce que nos enfants (ou nos petits-enfants) pourront utiliser un jour un "système de traitement automatisé de données" (quel qu'il soit) en toute fiabilité ? Probablement pas. D'ailleurs c'est plutôt l'inverse qui est en train de se produire: aujourd'hui, la "panne informatique" est invoquée pour justifier à peu près toutes les erreurs et tous les dysfonctionnements.

La réduction des coûts à outrance, la déqualification des métiers techniques comme l'ingénierie logicielle, la course à l'immédiateté (et la culture du "patch" qui l'accompagne) ont tendance à diminuer la qualité de la production logicielle.

A titre anecdotique, on peut citer l'exemple des jeux vidéo dont la version vendue en magasin est non fonctionnelle - les éditeurs ayant mis à profit le temps de pressage et de

distribution des CD-ROM pour finir le développement du logiciel, et fournir le tout sous forme d'un patch à télécharger.

Sans parler évidemment des vulnérabilités qui sont introduites volontairement par l'éditeur (aussi appelées backdoors), souvent dans le but de faciliter le support client … Vous avez oublié votre mot de passe de 30 caractères ? Pas de problème, le technicien saura vous dépanner !

On peut donc conclure sur une note positive en affirmant que la recherche de vulnérabilités logicielles a de beaux jours devant elle !

MYTHES ET LEGENDES DES VERS, VIRUS ET TROJANS

David Grout, McAfee

MYTHE N° 1 :
LES EDITEURS D'ANTIVIRUS ECRIVENT EUX-MEMES LES CODES MALVEILLANTS:

Dès que je suis arrivé dans ce domaine en 2003 ce fut la première remarque de l'un de mes clients… « Mais c'est vous qui générez tous ces codes pour vous mettre en valeur à travers vos protections et nous vendre vos solutions ». Vaste question, que d'interrogations, serait-ce possible ?… Une investigation devenait alors nécessaire. Après quelques recherches sur l'Internet je me rendis compte que les vers les plus répandus de cette époque l'étaient en fait à travers des codes générés par des scripts Kiddies (nous en reparlerons dans un prochain mythe). 7 années plus tard en 2010 l'ensemble de mes interrogations sur le sujet est levé et sans ambiguïtés, en effet les laboratoires d'un éditeur de sécurité reçoivent en moyenne 1000 nouveaux codes malveillants par heure.

On comprend aisément deux choses, les éditeurs de sécurité n'ont pas besoin de se faire de la publicité, le mal est réel, et de plus le volume est si considérable que les entreprises d'aujourd'hui n'auraient même pas la capacité humaine de générer tous ces codes.

Pour conclure, il est sur qu'aujourd'hui l'écriture de codes de malveillants n'est pas fait par les éditeurs de sécurité, ils ont déjà un travail herculéen à les contrecarrer.

MYTHE N° 2 :
LES CODES MALVEILLANTS SONT ENFANTINS A GENERER :

Cette phrase est la citation préférée de tous les « geeks » en élaboration de codes malveillants, autrefois appelés les scripts kiddies terme qui était au départ plutôt péjoratif dans la communauté mais que j'emploierai plus pour englober les personnes et les utilitaires permettant à n'importe quelle personne de générer par lui-même un code malveillant.

Malheureusement nous sommes passés depuis quelques années dans une autre dimension de la sécurité et de la malveillance, car aujourd'hui l'argent est le vecteur premier de reconnaissance. Finie l'époque ou l'on souhaitait juste défigurer un site Internet et y mettre son nom pour, comme disent les enfants, montrer que « l'on est cap de le faire ». Aujourd'hui même si ce type d'attaque existe toujours, il est aisément contré par des dispositifs de sécurité de « base » comme les antivirus, firewall.

Depuis quelques années la génération de codes malveillants se complexifie et est le fruit d'équipes complètes de personnes présentant des compétences multiples et très pointues dans différents domaines. Il existe même à ce jour des entreprises dédiées à l'écriture de codes malveillants (avec un SAV oui oui !!!), nous sommes passés de la reconnaissance d'un nom à la reconnaissance financière.

Les dernières attaques en dates appelées aussi APT (Advanced Persistent Threats) telles que Aurora ; Stuxnet le démontrent. Le code malveillant est devenu aujourd'hui une chose extrêmement complexe motivée par le plus vieux moteur du monde : l'Argent. Il ne faut pas oublier aussi l'utilisation de cette menace, ou de cette arme qu'est le code malveillant à un niveau étatique. Aujourd'hui la démobilisation d'un pays par un malware serait-elle possible : Die Hard 4 est-il si loin de nous ?….

MYTHE N° 3 :
C'EST SUR LES PC SOUS WINDOWS QUE LES VIRUS ATTAQUENT

Un mythe qui nous tient, je dirais même qui nous colle … Et oui les virus attaquent Windows mais pas seulement. Le concept aujourd'hui d'une attaque malware est de gagner de l'argent, alors pourquoi Windows ? Tout simplement parce que la part de marché de cet OS est la plus conséquente donc potentiellement les cibles offertes par Windows sont les plus nombreuses.

Mais aujourd'hui avec l'évolution et l'ouverture des plateformes on voit des virus sur MAC, sur Linux et encore plus aujourd'hui sur IOS (Apple OS). Une chose est sûre : la seule motivation et le seul vecteur est l'argent, alors plus un OS est utilisé par des populations sensibles en entreprises plus ces OS seront visés. Il y a fort à parier que 2011 sera l'année du mobile et ce dans tous les sens du terme.

Dernier élément qui casse définitivement ce mythe, parmi les attaques ciblées à des fins financières mais aussi politiques, les malwares visent aussi des OS inconnu du grand public : SCADA avec l'attaque Stuxnet en est un.

Donc pour conclure, aucun OS n'est à l'abri et au vu du peu de couverture que les entreprises consacrent à des environnements « non standards » comme Linux ou MAC, il est sûr que si j'étais un hacker, mon choix de cible primaire serait vite fait …

MYTHE N° 4 :
UNE MISE A JOUR DE LA BASE ANTIVIRALE PAR SEMAINE ET JE SUIS TRANQUILLE

Commençons par quelques chiffres : En 2003 l'éditeur pour lequel je travaille annonçait que nous franchissions la barre mythique des 200 000 souches virales couvertes par les signatures antivirales. Aujourd'hui ce chiffre est atteint tous les 4 jours… Oui, oui vous lisez bien, aujourd'hui une base de signatures couvre 42 millions de souches et augmente en moyenne de 50 000 échantillons par jour.

Alors oui, on peut se mettre à jour toute les semaines le risque n'est que de 350 000 infections potentielles. Aujourd'hui il est clair que le niveau de mise à jour se doit d'être continu. Cependant les éditeurs sont confrontés à une problématique que n'ont pas les hackers, le risque de "faux positif". En effet, un faux positif, ou une détection erronée d'un fichier sain, peut avoir des conséquences désastreuses, c'est pour cela que les firmes antivirus sont contraintes à des tests de qualifications et qualités multiples avant la publication de leurs signatures.

La solution aujourd'hui est complexe mais le marché va vers la sécurité à travers des signatures pour une base validée et testée à laquelle s'ajoute une approche « In the Cloud » ou en temps réel en cas de suspicion forte sur un fichier, même si celui-ci n'est pas détecté par la signature classique. Mais il faut retenir que même si ce type de protection tend vers une couverture complète, elle ne reste néanmoins qu'une protection réactive. L'avenir de la protection se situe aujourd'hui dans la pro activité et surtout la prédictibilité, un énorme challenge …

En attendant mettez vous à jour antivirale le plus souvent possible, voici un mythe qui n'en n'est pas un !

MYTHE N° 5 :
IL NE SE PASSE RIEN DE SPECIAL SUR MA MACHINE C'EST DONC QUE TOUT VA BIEN

Une veille croyance du monde de l'informatique est que si rien ne se passe d'étrange c'est que tout va bien … Je dirais que cela n'est pas faux dans 95% des cas, mais que se passe t'il dans les 5% restant ?

Vous allez vous dire, mais il est parano celui là ? Il voit des malwares partout ! Vous n'avez pas tort, mais aujourd'hui il existe une catégorie de malware encore mal perçue par les utilisateurs, les Trojans (ou chevaux de Troie) qui veulent récupérer de l'argent de manière silencieuse.

Le concept n'est plus comme dans le cas de virus massif, de faire tomber une machine (ex : conficker) ou de créer un réseau de robots qui ciblera des sites web pour les faire tomber, mais un concept vraiment différent. L'idée globale est pour l'assaillant de venir s'inviter sur le poste de sa cible sans que celle-ci s'en aperçoive, à travers l'utilisation de rootkits par exemple.

Ensuite le jeu est de faire évoluer son code de manière sensible afin de ne jamais alerter les outils de protections locaux, puis une fois le virus installé et actif , d'ouvrir une porte entre la machine attaquée et l'Internet (Backdoor). Lorsque ces étapes sont réalisées alors l'assaillant commence à lancer des commandes et à récupérer de l'information : captures d'écran, fichiers sensibles … et ceci en petits morceaux afin de ne jamais éveiller le doute…

Si vous venez de lancer votre gestionnaire de tâches, votre "regedit" et que vous recherchez des traces c'est que vous aussi vous êtes devenu paranoïaque…

Mais si il ne se passe rien sur votre machine, alors peut-être qu'il ne se passe réellement rien ?…

MYTHES ET LEGENDES DU CHIFFREMENT

Gérard Peliks, CASSIDIAN
an EADS Company

Celui à qui vous dites votre secret devient maître de votre liberté
La Rochefoucault - 1650

QUELQUES MOTS A MAITRISER QUAND ON PARLE DE CRYPTOLOGIE

La cryptologie, science des messages cachés, se divise en deux disciplines antagonistes, la cryptographie et la cryptanalyse.

La cryptographie est l'art de transformer un message en clair, en un message incompréhensible. Pour cela le message en clair est traité par un algorithme (un programme) et une clé de chiffrement (un ensemble de bits). La cryptographie est aussi l'art, connaissant l'algorithme et une clé, de retrouver le message en clair à partir du message caché. On parle de "chiffrer" et de "déchiffrer" le message. C'est le chiffre de défense : on cache l'information sauf à celui qui est en droit d'en prendre connaissance.

Mais si on connait le message chiffré sans connaitre la clé pour déchiffrer le message, il est parfois, par calcul, quand même possible d'obtenir le message en clair. C'est la cryptanalyse. On parle alors de "décrypter" le message chiffré. C'est le chiffre d'attaque : on essaie de récupérer un message chiffré alors qu'on n'en est pas le destinataire.

Ceci étant posé, que signifie "crypter" un message ? Cela ne signifie rien et le mot crypter est à bannir du vocabulaire de la cryptologie.

La cryptologie à l'ère numérique est un combat entre les cryptographes qui élaborent des algorithmes toujours plus difficilement cassables, et qui se basent sur des clés toujours plus longues, et les cryptanalystes qui élaborent des méthodes toujours plus efficaces pour retrouver le message en clair sans utiliser la clé.

Par exemple, à l'aire pré-numérique, Scherbius qui avait conçu la première machine Enigma dans les années 1920 était un cryptographe. Les Anglais du Bletchley Parc, durant la seconde guerre mondiale, qui décryptaient les messages, que les Allemands chiffraient avec cette machine, étaient des cryptanalystes.

MYTHE N°1 : LE SECRET DU CHIFFREMENT EST DANS L'ALGORITHME

Non, contrairement à ce qu'on pense généralement, le programme de traitement (l'algorithme) qui transforme, en utilisant une clé de chiffrement, un fichier en clair en un fichier chiffré, n'est ni confidentiel défense, ni même un secret industriel, tout du moins dans un contexte où ce principe a été compris.

Le secret réside dans une clé qui sert à chiffrer un fichier, cas de la signature électronique ou du chiffrement symétrique, ou à déchiffrer ce fichier, cas du chiffrement asymétrique.

Kerckhoffs, à la fin du 19eme siècle avait déjà énoncé ce principe : "le secret du chiffrement ne doit résider que sur le secret de la clé". L'algorithme peut être public.

Et mieux, si l'algorithme est un standard comme par exemple l'AES ou le RSA, une communauté importante d'experts peut essayer de le casser, signale ses failles qui sont alors corrigées, et avec le temps, le code d'implémentation de cet algorithme ne présente plus de vulnérabilité évidente, connue.

Si le code d'implémentation de l'algorithme de chiffrement est jalousement gardé, alors seuls ceux qui ont le droit d'en connaître, donc un nombre infime d'experts par rapport à ceux qui composent la communauté sur le net, peuvent corriger d'éventuelles erreurs. De plus, quand les experts qui connaissent les méandres d'un algorithme confidentiel ne sont plus disponibles, la connaissance a disparue et la maintenance ne peut plus se faire.

Avec un algorithme public, c'est au niveau de la clé que le secret réside. L'algorithme utilise diverses parties de la clé pour effectuer les transformations qui aboutissent au chiffrement ou au déchiffrement du message. Sans la connaissance de la clé, il est difficile de savoir comment se comporte l'algorithme, donc il est difficile, à partir du message chiffré, de reconstituer le message en clair.

Il existe néanmoins des chiffrements qui reposent sur le secret de l'algorithme. Mais ni Kerckhoffs, ni les cryptologues d'aujourd'hui ne trouvent que c'est une bonne idée et conseillent d'utiliser plutôt les algorithmes standards et éprouvés, et de plus soutenus par la communauté du chiffre.

MYTHE N° 2 :
ON CHIFFRE AVEC SA CLE PRIVEE

Mythe ou réalité, cela dépend.

Pour comprendre ce qui suit et pourquoi le chiffrement qui utilise une clé privée est un mythe, cela nécessite des explications sur les deux méthodes de chiffrement. Le chiffrement symétrique et le chiffrement asymétrique.

Dans le chiffrement symétrique, on chiffre une information en utilisant une clé et un algorithme de chiffrement symétrique tels que le 3DES ou l'AES. On déchiffre avec le même algorithme et la même clé. La clé de chiffrement, dite "clé secrète", est la même que la clé de déchiffrement, c'est pourquoi ce type de chiffrement est dit symétrique. En utilisant la même clé, un coup on chiffre, un coup on déchiffre.

Mais un problème se pose. Celui qui chiffre génère la clé de chiffrement symétrique (la clé secrète), mais comment celui qui va déchiffrer, si ce n'est pas la même personne que celui qui a chiffré, va-t-il entrer en possession de cette clé, qui doit bien sûr rester secrète pendant le transfert ? L'autre gros problème est la multiplication des clés secrètes si on se met à chiffrer et déchiffrer entre un nombre élevé de destinataires. Le chiffrement symétrique est pratique et de plus très rapide, mais suite à la difficulté de transmettre la clé et suite à la multiplication des clés qu'il impose, il est difficilement utilisable en l'état.

Le chiffrement asymétrique met en jeu deux clés mathématiquement liées. Une clé privée qui est un secret et une clé publique dont tout le monde peut prendre connaissance. Quand on chiffre avec un algorithme de chiffrement asymétrique comme le RSA, et avec une des deux clés, on déchiffre avec le même algorithme et avec l'autre clé. Dernier postulat : connaissant la clé publique, il est évidemment très difficile de retrouver la clé privée correspondante.

Vous conservez votre clé privée, de manière idéale sur un token USB ou une carte à puce protégée par un code PIN, et vous donnez à tous ceux qui en ont besoin votre clé publique correspondante, ou alors vous dites où aller la chercher.

Avec quoi chiffrez-vous votre information pour la garder confidentielle ? Avec votre clé privée ? Non bien sûr, réfléchissez. Si vous chiffrez avec votre clé privée, tous ceux qui ont votre clé publique pourront déchiffrer votre information, donc il aura été inutile de la chiffrer et la confidentialité espérée ne sera qu'illusoire.

Mais tout de même, une signature RSA est le chiffrement par la clé privée d'une information. Ici le but n'est pas la confidentialité, mais l'authentification: tout porteur de la clé publique doit pouvoir déchiffrer cette information pour l'authentifier comme venant du porteur, unique, de la clé privée.

MYTHE N° 3 : ON CHIFFRE AVEC UNE CLE PUBLIQUE

Nous avons vu que ce n'est pas avec votre clé privée que vous chiffrez votre information, sinon tout le monde pourrait la déchiffrer.

Alors si ce n'est pas avec votre clé privée, c'est forcément avec l'autre clé, votre clé publique ? Et bien non ! Si vous chiffriez avec votre clé publique, comme personne d'autre que vous n'est censé posséder votre clé privée, pour déchiffrer, à moins que vous chiffrez vos informations pour, seulement vous-même les déchiffrer, ce ne peut être avec votre clé publique. Alors si ce n'est avec votre clé publique, ce pourrait être avec la clé publique de celui à qui vous voulez envoyer votre information chiffrée ?

En effet, comme vous trouvez cette clé publique dans le certificat de celui à qui vous voulez envoyer l'information chiffrée, et comme ce certificat est signé par une autorité de confiance, vous êtes sûr que c'est vraiment la clé publique de votre correspondant, car lui seul possède la clé privée correspondante avec laquelle il va déchiffrer l'information que vous avez chiffrée. Donc tout va bien et c'est comme ça qu'il faut faire ?

Et bien non !

Le chiffrement asymétrique présente un gros handicap : il est cent à mille fois plus lent que le chiffrement symétrique. Cela est du à ses algorithmes qui sont plus complexes. Si déchiffrer une vidéo prend 5 minutes en chiffrement symétrique et plusieurs heures en chiffrement asymétrique, vous aurez vite choisi quel chiffrement vous désirez utiliser.

Ce n'est donc pas non plus avec la clé publique de votre destinataire que vous allez chiffrer votre information, mais avec une clé secrète symétrique que vous générez. Et cette clé secrète, vous la chiffrez avec la clé publique de votre destinataire. Vous lui envoyez cette clé de chiffrement symétrique ainsi chiffrée. La clé de chiffrement symétrique reste confidentielle durant le transfert puisqu'elle ne peut être déchiffrée que par le destinataire qui seul possède sa clé privée. Avec sa clé privée le destinataire déchiffre la clé secrète, et avec cette clé secrète, il déchiffre l'information qui avait été chiffrée avec cette même clé secrète, par chiffrement symétrique.

En résumé, ce n'est pas avec une clé publique qu'on chiffre une information, mais avec une clé secrète symétrique. La clé publique ne servant ici qu'à chiffrer la clé secrète, par chiffrement asymétrique, et la clé secrète sera ensuite déchiffrée par la clé privée du destinataire.

MYTHE N° 4 :
LE CHIFFREMENT QUANTIQUE, ARME ABSOLUE, DES AUJOURD'HUI

Basé non plus sur des calculs mathématiques mais sur la physique des particules, le chiffrement quantique causera une rupture technologique, dans le monde des cryptographes et des cryptanalystes, c'est dire que leur combat va prendre une dimension nouvelle.

Le calcul quantique permet d'effectuer en parallèle une énorme quantité d'opérations qui s'opérait en série avec les calculateurs classiques. Les ordinateurs vont pouvoir résoudre rapidement les problèmes quasiment insurmontables avec les moyens conventionnels tels que la décomposition d'un grand nombre en facteurs premiers, base du RSA, ou le problème du logarithme discret, base du chiffrement par courbes elliptiques.

Nous n'entrons pas ici dans les détails, mais retenez que le cassage de clés par force brute, c'est-à-dire la recherche de toutes les combinaisons possibles de clés pour arriver à retrouver un message en clair à partir d'un message chiffré, deviendra possible, dans un temps acceptable.

Mais aujourd'hui les ordinateurs quantiques ont un gros défaut : ils n'existent pas, sauf dans les romans de science fiction ou alors à titre expérimental, ils en sont à leurs premiers balbutiements dans des laboratoires de recherche.

Les cryptographes ont ainsi encore des années de tranquillité devant eux. De plus, ils peuvent utiliser la mécanique quantique, et nous ne parlons plus d'ordinateurs quantiques, pour échanger une clé de chiffrement de manière sûre, ce qui était jusque là le gros problème à résoudre pour le chiffrement symétrique.

La mécanique quantique dit qu'un photon tourne autour d'un axe qui est orienté dans une direction qu'on peut lui imposer en jouant sur un champ magnétique. On connait d'autre part la probabilité que ce photon traverse ou pas un filtre à particules, en fonction de l'angle que fait ce filtre par rapport à l'orientation de l'axe du spin du photon qui essaie de le traverser.

Et merveille des merveilles, pour un cryptographe, si une tierce personne observe le spin d'un photon, son orientation est modifiée. Celui qui reçoit la clé s'aperçoit d'une incohérence avec ce que devait être l'état du photon quand celui-ci a été envoyé.

Cette propriété est utilisée pour échanger la clé de chiffrement de manière sûre, car si un espion entre dans la boucle et observe, la clé envoyée est invalidée et on en essaie une autre.

Le calculateur quantique qui résout les problèmes difficilement traités par les ordinateurs actuels et qui cassent les clés dont la taille rendait jusqu'ici ce cassage impossible ou trop coûteux en temps et en ressources est encore un mythe qui va durer quelque temps avant de devenir réalité.

Par contre l'échange sécurisé de clés de chiffrement, qui utilise la mécanique quantique, a dès aujourd'hui des applications, en particulier dans le domaine des télécoms.

MYTHE N° 5 :
LE CHIFFREMENT SEUL MOYEN D'ASSURER LA CONFIDENTIALITE

Une façon d'assurer la confidentialité d'une information est de la chiffrer. Mais il existe un autre moyen, plus pernicieux : cacher cette information, dans son contenant. C'est la science de la stéganographie, aussi vieille que la cryptologie, sinon plus.

Avec la stéganographie, l'information à cacher est en clair (ou chiffrée), mais on ne se doute pas de sa présence. Un exemple physique simple est l'utilisation de l'encre sympathique qui

rend invisible un message, sauf quand on chauffe son support. Plus technique, des micropoints peuvent dissimuler une information en la rendant microscopique.

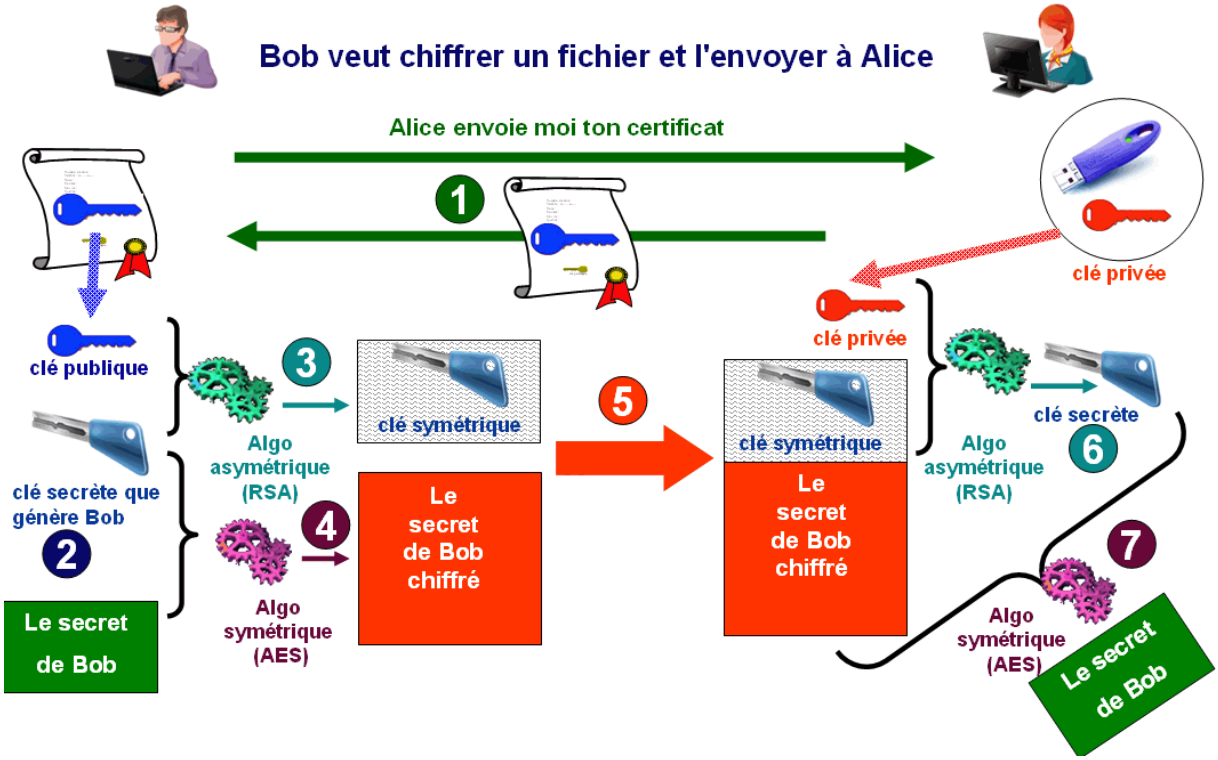
Autre exemple, dans une vidéo de vacances, suivant que vous portiez un chapeau de paille ou un béret basque, ça peut signifier quelque chose à quelqu'un que vous avez mis au parfum de la vraie signification de votre couvre-chef, mais pas pour le commun des mortels.

Une application numérique de la stéganographie est de jouer sur le dernier bit de chaque pixel d'une image, pour cacher un message dans l'ensemble de ces bits. L'œil ne remarque pas les modifications de teintes ou de niveaux de gris de l'image, mais avec le programme approprié, l'image révèle ses messages cachés.

Face à un message chiffré, le cryptanalyste pensera que le message dissimule un secret et a donc de la valeur et il tentera de le décrypter. L'avantage de la stéganographie est que si le message est simplement invisible dans son support visible, qu'il soit chiffré ou en clair, personne n'aura l'idée d'aller le chercher sauf son destinataire qui saura que, dans un fichier anodin, se trouve le message secret.

LES MECANISMES DU CHIFFREMENT

Principe [43] :



Bob chiffre un fichier et l'envoie à Alice. Les exemples sur le chiffrement font toujours intervenir Bob et Alice. Dans la réalité, se sont-ils connus vraiment et échangés des informations chiffrées ? Peut-être est-ce aussi un mythe ☺ ?

[43] *Crédit Pictogrammes Aastra*

Comme l'a dit Albert Einstein « il faut rendre les choses complexes aussi simples que possible mais il ne faut pas les rendre plus simples que possible ». Il est sûr que la crypto est complexe, ça ce n'est pas un mythe.

Allons y ensemble, je vous guide dans l'utilisation des diverses clés et algorithmes divers qui interviennent dans l'échange d'un fichier chiffré.

Bob demande à Alice son certificat. Alice le lui envoie. Bob vérifie le certificat d'Alice, qui est l'autorité qui l'a signé, ses dates de validité, et s'il l'accepte en tire la clé publique d'Alice, pour l'utiliser dans un algorithme asymétrique, comme le RSA.

Bob génère une clé secrète avec laquelle il chiffrera son message confidentiel par un algorithme de chiffrement symétrique, comme l'AES.

Avec la clé publique d'Alice, Bob chiffre sa clé secrète qu'il vient de générer, en utilisant un chiffrement asymétrique, comme le RSA.

Avec sa clé secrète, Bob chiffre son message, en utilisant un chiffrement symétrique, comme l'AES.

Bob envoie à Alice, le message qui a été chiffré par sa clé secrète et un algorithme symétrique comme l'AES, et joint sa clé secrète qui a été chiffrée par la clé publique d'Alice et un algorithme asymétrique comme le RSA.

Avec sa clé privée contenue dans son token USB, Alice déchiffre la clé secrète, générée par Bob et chiffrée avec la clé publique d'Alice.

Et avec cette clé secrète et un algorithme symétrique, comme l'AES, Alice déchiffre le message envoyé par Bob.

La clé secrète intervenant dans le chiffrement symétrique utilisée pour chiffrer et déchiffrer le message secret a ainsi été envoyée par Bob à Alice en toute sécurité.

MYTHES ET LEGENDES DES MATHEMATIQUES DE LA CRYPTOGRAPHIE

Eric Bourre, CASSIDIAN
an EADS Company

MYTHE N°1 :
LES FAILLES CRYPTOLOGIQUES SONT DUES A DES MATHEMATIQUES PAS ASSEZ SOLIDES

Penser que des failles cryptologiques seraient dues à des problèmes mathématiques est une idée fausse.

POUR LA CRYPTOGRAPHIE A CLE SECRETE (SYMETRIQUE) :

Les algorithmes de chiffrement utilisés aujourd'hui sont l'AES ou le 3DES. L'AES n'a pour l'instant pas été cassé et la recherche exhaustive (force brute) demeure la seule solution pour retrouver la clé de chiffrement.

Les standards sont conçus de manière à ce que les attaques classiques, comme la cryptanalyse linéaire ou différentielle, soient très difficiles voir impossibles à réaliser.

Si l'on considère l'attaque par force brute pour trouver la clé secrète comme la seule possible, il faut essayer toutes les possibilités.

Si la clé utilisée est de longueur 256 bits, il faudra essayer 2^{256} combinaisons (soit environ 1 million de milliard de milliard de milliard de milliard de milliard de milliard de milliard de milliard de combinaisons), ce qui représente un nombre qui dépassera toujours la puissance de calcul qui peut être mise en place. Cela équivaudrait pratiquement à compter un à un tous les atomes qu'on estime composer l'univers (environ 2^{270} atomes) ! Cela rend en fait inconcevable le déchiffrement. Nous verrons toutefois dans le mythe n°4 pourquoi ce niveau de sécurité est la plupart du temps interdit.

POUR LA CRYPTOGRAPHIE A CLE PUBLIQUE (ASYMETRIQUE) :

Elle se base sur des fonctions à sens unique.

Les fonctions à sens uniques sont des fonctions difficilement inversibles à moins d'en connaître la brèche, la brèche étant la clé privée. C'est à dire qu'un message chiffré sera difficilement déchiffrable si l'on ne connaît pas la clé privée, correspondant à la clé publique qui l'a chiffré.

Bien sûr le terme "difficilement déchiffrable" s'exprime et se quantifie de façon mathématique. En cryptologie, ces problèmes 'difficilement déchiffrables" sont de complexité exponentielle par rapport à la taille des clés.

Pour RSA doubler la taille d'une clé ne rend pas le problème 2 fois plus difficile mais plus de 1000 fois plus difficile à résoudre. Il serait possible de choisir des clés assez grandes pour rendre toute attaque vaine.

Mais alors pourquoi ne choisissons-nous pas des tailles de clés plus grande?

Cela est du au fait que le temps de déchiffrement (ou de signature) augmente plus que linéairement en fonction de la taille de la clé. Ainsi doubler la taille des clés rend le déchiffrement/ signature entre 6 et 7 fois plus lent, donc 6 à 7 fois plus coûteux !!

Plus la taille de la clé est grande, plus le coût associé aux opérations cryptographiques sera grand.

Le tout est donc de trouver un juste milieu entre la sécurité nécessaire (qui dépend des puissances machines existantes) et son coût. Il existe des recommandations liées à la taille de clés pour un algorithme de chiffrement choisi (jusqu'en 2010 : 1024 bits, jusqu'en 2030 : 2048, puis ensuite 3072). Cela est valable, tant que l'on ne trouve pas de meilleur algorithme de déchiffrement que le RSA.

Pour résumer, les failles des systèmes cryptographiques tiennent donc à :

- des failles sur les protocoles, ou algorithmes mis en place (ex : le WEP) ;
- des données, en entrée des problèmes trop faibles, comme des tailles de clés trop faibles ;
- des langages de programmation, faille systèmes ;
- des composants physiques ou logiciels qui utilisent des clés (rayonnement des cartes à puce....).

Mais les problèmes mathématiques eux sont solides.

MYTHE N°2 :
ON ME DIT QUE L'ALGORITHME RSA SE CASSE DEUX FOIS PLUS FACILEMENT, NOUS DEVONS ALORS DOUBLER LA TAILLE DES CLEFS

Comme je l'ai indiqué dans le mythe précédent, la complexité du problème RSA n'est pas linéaire en fonction d'une taille de clé.

Si l'on double la taille de la clé RSA, on rend l'attaque par force brute plus de 1000 fois plus longue pour aboutir. De façon pratique, si on trouvait un algorithme qui casse RSA deux fois plus rapidement, il suffirait de choisir des clés avec seulement quelques bits supplémentaires.

L'INRIA en 2009 a réussi à casser une clé RSA de 768 bits. Pour casser une clé d'environ 1536 bits, l'INRIA aurait besoin d'une puissance de calcul 1000 fois supérieure (sachant que cet institut possédait déjà des supercalculateurs calculant en parallèle pour réaliser ce cassage). La croissance de la difficulté de cassage de clé augmente beaucoup plus vite que la taille des clés. Nous pouvons aujourd'hui penser que les clés de taille 2048 bits ont de beaux jours devant elles.

MYTHE N°3 :
LA MONTEE EN PUISSANCE DE CALCUL PERMETTRA DE RESOUDRE DES PROBLEMES COMPLEXES

Penchons nous sur la loi de Moore un instant.

Elle stipule que la puissance machine double chaque année (on a constaté qu'elle doublait réellement tous les 18 mois). Cela veut dire que la puissance machine augmente de façon exponentielle. On pourrait alors penser que ces améliorations pourraient résoudre des problèmes complexes (solutions exponentielles). Toutefois cette loi ne peut durer car la croissance exponentielle s'essouffle inévitablement très rapidement. En fait ce qui va bloquer ce développement est le fait que le coût des chaînes de production, permettant de créer les processeurs plus puissant, est lui aussi exponentiel (à tel point que même des géants comme IBM et Siemens, pourtant concurrents, ont dû grouper leurs investissements pour arriver à suivre le mouvement). On est donc proche de la fin de la loi de Moore.

Sauf une découverte d'autres lois physiques comme l'utilisation du calcul quantique pourrait permettre à la loi de Moore de se vérifier durablement. Mais rien n'est plus hypothétique car le calcul quantique réclamerait apparemment une énergie exponentielle pour être mise en application. Sans découverte physique majeure, il y aura toujours des tailles de clés intouchables face à toute puissance de calcul que l'homme pourra mettre en place.

MYTHES ET LEGENDES DES TECHNOLOGIES QUANTIQUES DE L'INFORMATION

Grégoire Ribordy, ID Quantique SA

Au niveau fondamental la nature suit les lois de la physique quantique. Au niveau fondamental, la théorie de l'information doit donc être une théorique quantique de l'information.
David Deutsch

MYTHE N°1 : LE FUTUR DES TIC EST QUANTIQUE

Le développement fulgurant des TIC au cours des quatre dernières décennies a été rendu possible par la loi de Moore. Ce principe, énoncé en 1965 par Gordon Moore, un des fondateurs d'Intel, stipule que le nombre de transistors que peut incorporer un circuit intégré double tous les dix-huit mois (lors du premier énoncé de cette loi, Moore parlait de 12 mois). Cette loi a pour corollaire que la puissance de calcul à disposition à coût fixe double elle aussi tous les 18 mois. Alors que le circuit Intel 4004, le premier microprocesseur commercialisé par Intel et lancé en 1971, contenait approximativement 2300 transistors, les puces les plus récentes en comprennent plusieurs milliards. C'est cette augmentation exponentielle qui a permis le développement des applications des TIC qui ont transformé la société dans laquelle nous vivons.

Pour que la loi de Moore soit vérifiée, l'industrie des semi-conducteurs a dû faire face au défi de réduire la taille des transistors. Pour ce faire, les techniques de photolithographie, qui permettent « d'imprimer » sur des galettes de Silicium les circuits électroniques ont été affinées progressivement de façon à augmenter leur résolution et la finesse des composants fabriqués. En 1971, l'épaisseur de la grille d'un transistor du microprocesseur Intel 4004 mesurait environ 10um (1/10 de l'épaisseur d'un cheveu). Quarante ans plus tard, l'épaisseur de cette même grille a été réduite par un facteur de plus de 1000 et approche les 5nm (1nm est un milliardième de mètre), ce qui correspond à environ une vingtaine d'atomes de silicium. Avec de telles dimensions, on n'est plus très loin du domaine où les lois de la physique quantique commencent à jouer un rôle et à modifier le comportement de la matière, empêchant les transistors de fonctionner.

La physique quantique est un ensemble de théorie physique décrivant le monde microscopique et introduit au début du 20^{e} siècle. Elle marque une rupture avec la physique dite classique, qui comprend l'ensemble des principes physiques admis au 19^{e} siècle. Au cours des dernières décennies de ce siècle, les techniques expérimentales ont suffisamment progressé pour mettre en évidence des différences entre les prédictions théoriques et les résultats de mesure. Des physiciens, comme Max Planck, Albert Einstein ou Niels Bohr se sont donc vus contraints d'introduire une nouvelle théorie, la physique quantique, pour modéliser ces expériences. Cette nouvelle physique décrit le comportement des atomes et des particules élémentaires, mais ne s'applique pas au monde macroscopique où la validité des lois de la physique classique reste incontestée.

Une des prédictions qui découle de cette physique quantique est l'effet tunnel. Ce phénomène rend compte de la possibilité au niveau microscopique pour les particules de

traverser des barrières, si celles-ci sont suffisamment fines. C'est cet effet qui empêcherait de faire fonctionner un transistor dont la taille serait réduite abusivement. Les électrons auraient en effet la possibilité de traverser les barrières du transistor, qui aurait donc des fuites.

Le fait que la fabrication des transistors risque de se heurter à un « mur quantique », à cause de l'effet tunnel et plus généralement de l'influence des lois quantiques, amène certains à prédire la fin de la loi de Moore. Il faut noter ici que d'autres facteurs, tel que l'augmentation du coût des installations de fabrication avec la miniaturisation des composants, ou encore la difficulté à dissiper la chaleur générée dans les puces, qui augmente aussi avec leur densification, pourraient aussi contribuer à mettre un terme à la progression de Moore. Les plus optimistes remarquent que la fin de la loi Moore a déjà été prédite à de multiples reprises par le passé, mais que les limites ont toujours pu être dépassées.

Une des approches proposée pour dépasser ce mur quantique consiste à réaliser un ordinateur quantique. Le développement d'un tel ordinateur vise à utiliser les lois de la physique quantique pour accélérer le traitement de l'information plutôt que d'être limité par ces lois. S'il est déjà établi qu'un ordinateur quantique permettrait de résoudre certains problèmes de façons plus efficaces qu'un ordinateur conventionnel, en l'état des connaissances actuelles il ne semble pas que ce soit un outil universel. Il serait donc plus adéquat de parler de calculateur ou de co-processeur quantique.

En résumé, s'il est certain que la physique quantique aura un impact sur la conception des puces du futur et qu'elle offre des pistes intéressantes pour l'amélioration des performances des ordinateurs dans certains domaines, il est difficile de prédire dans quelle mesure ses lois seront vraiment utilisées dans les TIC de demain.

MYTHE N°2 :
UN ORDINATEUR QUANTIQUE PERMET DE CASSER LES TECHNIQUES ACTUELLES DE CHIFFREMENT ASYMETRIQUE

C'est à la fois vrai et faux. Nous avons vu au mythe précédent que les lois de la physique quantique imposent des limites à la miniaturisation des composants électroniques. Or depuis le milieu des années 80, des physiciens ont proposé de tenter de tirer profit de ces lois, en développant un ordinateur quantique, pour réaliser certaines tâches de façon plus efficace qu'avec un ordinateur conventionnel.

A ce jour, aucun ordinateur quantique complet n'a été démontré, du moins dans le monde de la recherche publique. L'absence de matériel n'a pas empêché les théoriciens de réfléchir au logiciel. Un certain nombre d'algorithmes quantiques visant à tirer profit des capacités d'un tel ordinateur a ainsi été proposé au cours des vingt dernières années. Certains de ces algorithmes ont un impact drastique dans le domaine du chiffrement. On citera ainsi l'algorithme de Shor, proposé en 1994 par Peter Shor, alors chercheur aux Bell Labs. Cet algorithme permet de factoriser un nombre entier, c'est à dire de trouver les nombres premiers dont le produit est égal à ce nombre entier, de façon efficace.

Bien qu'anodin pour le commun des mortels, le problème de la factorisation joue un rôle important dans le domaine du chiffrement. On a vu au Mythe N°3 du chapitre sur le chiffrement, qu'il est possible de chiffrer un message au moyen de la clé publique du destinataire de ce message, de façon à ce que lui seul soit en position de le déchiffrer grâce à sa clé privée correspondante. Ce type de chiffrement est basé sur des objets mathématiques appelés fonctions à sens unique qui sont faciles à calculer, mais difficiles à inverser à moins d'en connaître la brèche. Le chiffrement au moyen de la clé publique se fait en calculant la

fonction. Le déchiffrement avec la clé privée équivaut à inverser cette fonction en connaissant sa brèche. Finalement, un adversaire qui souhaiterait décrypter le message – c'est à dire qu'il ne disposerait pas de la clé privée – se voit contraint à inverser cette fonction sans pouvoir utiliser la brèche. La fonction à sens unique utilisée par un des algorithmes de chiffrement asymétrique le plus répandu, l'algorithme RSA, est la multiplication des nombres entiers. Une feuille de papier et un crayon suffisent à calculer le produit de 2357 par 4201 en quelques minutes. Factoriser 9901757, c'est à dire trouver les deux entiers dont le produit donne ce nombre, est en revanche beaucoup plus gourmand en ressources.

Or, l'algorithme de Shor permet, au moyen d'un ordinateur quantique de factoriser efficacement des nombres entiers de grande taille. S'il était possible d'assembler un ordinateur quantique, il serait donc possible d'utiliser cet algorithme pour casser l'algorithme RSA et donc déchiffrer des transmissions sécurisées par ce procédé.

Comment se fait-il qu'un ordinateur quantique permette une telle prouesse, impossible au moyen d'un ordinateur conventionnel ? Une démonstration rigoureuse requerrait bien évidemment des notions avancées de physique quantique. Il est toutefois possible de proposer une explication intuitive. Une des caractéristiques de la physique quantique est le principe de superposition. Il est possible de préparer un système quantique dans une superposition de deux états A et B. Un tel système se trouve à la fois dans l'état A et dans l'état B. Au moment d'une mesure, on force le système à décider dans quel état il se trouve et on obtient le résultat A ou B, mais pas les deux. Au moment de la rédaction de cet article, je me trouve à Genève. La physique classique ne m'autorise à me trouver qu'en un seul endroit à la fois. En revanche, si j'étais un « être quantique », je pourrais me trouver dans une superposition spatiale et être localisé à la fois à Genève et à Paris. Ce principe de superposition n'est pas vraiment intuitif, mais il faut l'accepter. En informatique, on peut le mettre à profit, tel que l'a démontré Shor, pour accélérer certaines tâches. Imaginons un problème dont la résolution au moyen d'un ordinateur conventionnel nécessite d'effectuer un calcul sur toutes les données possibles constituées de n bits. Il en existe 2^n, ce qui implique, si n vaut 10, de réaliser le calcul 1024 fois. Pour résoudre le même problème avec un ordinateur quantique en exploitant le principe de superposition, on peut tout d'abord préparer une superposition de toutes les données possibles : 1er bit en superposition de 0 et 1, 2^{e} bit en superposition de 0 et 1, … et ainsi de suite jusqu'au n^{e} bit. Il suffit ensuite d'effectuer le calcul une seule fois pour explorer tout l'espace des données et obtenir le bon résultat. Il est bien évident que cette explication est simplifiée à l'extrême, mais son esprit est correct.

On a vu que la sécurité du procédé asymétrique RSA est mise à mal par un ordinateur quantique permettant d'implémenter l'algorithme de Shor. Qu'en est-il des autres procédés asymétriques ? Bien que basés sur des problèmes mathématiques différents, certains procédés sont mathématiquement équivalents à celui du RSA. On peut par exemple citer le procédé des courbes elliptiques. Ils sont donc évidemment aussi vulnérables à un adversaire disposant d'un ordinateur quantique.

Est-ce à dire que la sécurité de tous les algorithmes asymétriques sera annihilée par le développement d'un ordinateur quantique ? Il n'est pas possible de répondre à cette question. Il existe en effet au moins un algorithme asymétrique, l'algorithme dit de McEliece, dont la résistance à l'algorithme de Shor a été démontrée. On ne peut toutefois pas exclure la découverte future d'un algorithme, classique ou quantique, permettant de le « casser ».

En résumé, un ordinateur quantique, s'il existait, permettrait de casser les procédés de chiffrement asymétriques les plus usités grâce à l'algorithme de Shor. Il a toutefois été

démontré récemment que cet algorithme est inopérant contre au moins un procédé asymétrique. La sécurité de ce procédé n'a toutefois pas été formellement démontrée, mais il n'existe pour l'instant aucune vulnérabilité connue. Cette situation peut néanmoins évoluer rapidement.

MYTHE N°3 :
UN ORDINATEUR QUANTIQUE PERMET DE CASSER LES TECHNIQUES ACTUELLES DE CHIFFREMENT SYMETRIQUE

On a vu au mythe précédent qu'il existe un algorithme pour ordinateur quantique permettant de résoudre les problèmes mathématiques sur lesquels sont basés certains des procédés de chiffrement asymétrique les plus usités. Qu'en est-il de l'impact de cet ordinateur quantique sur les procédés symétriques ?

Les procédés symétriques n'étant pas basés sur des fonctions à sens unique, l'algorithme n'est d'aucune utilité dans ce cas. Il existe toutefois un second algorithme, celui de Grover, qui a un impact sur ces procédés. Cet algorithme a été inventé en 1996 par Lov Grover, lui aussi chercheur aux Bell Labs. Il permet d'effectuer une recherche dans une base de données non triée de façon plus efficace qu'avec le meilleur algorithme fonctionnant sur un ordinateur conventionnel.

Bien que ce problème n'ait en apparence pas grand chose à voir avec la cryptographie, il est possible d'utiliser l'algorithme de Grover pour attaquer les procédés de chiffrement symétrique. L'impact de cet algorithme est de diviser la longueur de la clé par deux.

La résistance d'un procédé de chiffrement symétrique peut être caractérisée par la longueur de la clé qu'il utilise. Intuitivement, plus la clé est longue, plus il en existe de différentes. Il faudra ainsi plus de temps à une personne essayant de décrypter une communication en essayant toutes les clés. Comme les ordinateurs travaillent en mode binaire, on définit cette longueur de clé en nombres de bits. L'agence nationale de sécurité des systèmes d'information recommande l'utilisation d'une clé de 128 bits. Une telle sécurité est évidemment atteinte avec le procédé de chiffrement le plus utilisé actuellement, l'Advanced Encryption Standard (AES), qui fonctionne avec trois longueurs de clé : 128 bits, 192 bits ou 256 bits.

Bien que suffisante actuellement, une longueur de clé de 128 bits ne serait plus adéquate si un adversaire avait à sa disposition un ordinateur quantique permettant d'utiliser l'algorithme de Grover. La longueur de clé effective serait en effet réduite à 64 bits, taille considérée comme nettement insuffisante. C'est une des raisons pour laquelle le procédé AES a été standardisé avec plusieurs longueurs de clé, dont une de 256 bits. Celle-ci est en effet surdimensionnée si l'on considère uniquement les ordinateurs classiques.

En résumé, un ordinateur quantique affaiblit les procédés de chiffrement symétrique, mais de façon moins dramatique qu'il ne le fait pour les procédés asymétriques. Pour contrer une telle attaque, il suffit de doubler la longueur de la clé utilisée, ce qui est faisable dès aujourd'hui.

MYTHE N°4 :
UN ORDINATEUR QUANTIQUE N'EXISTE PAS ENCORE. JE N'AI DONC AUCUNS SOUCIS A ME FAIRE.

En considérant les résultats scientifiques publiés, il semble possible de conclure qu'un ordinateur quantique suffisant pour résoudre un problème impossible avec un ordinateur

classique n'existe pas encore. Des moyens financiers importants sont toutefois investis et des progrès constants réalisés. Des réalisations de « portes » quantiques, le composant élémentaire d'un ordinateur quantique, ont été démontrées par plusieurs groupes dans le monde. Ces « portes » sont basées sur différentes technologies, sans qu'il ne soit pour l'heure clair de savoir laquelle se révélera être la plus pratique. Plusieurs de ces « portes » quantiques ont même été couplées pour réaliser des enchaînements simples d'opérations.

Il n'en reste pas moins que ces prototypes, du moins ceux réalisés dans le domaine de la recherche publique, ne constituent pas une menace aujourd'hui. Est-ce donc à dire qu'il est inutile de se faire des soucis actuellement ?

Tout dépend de la durée de vie des communications devant être protégées. L'interception d'un message et son décryptage ne doivent pas nécessairement être simultanés. Il est en effet possible pour un adversaire d'enregistrer des données chiffrées puis d'attendre qu'un ordinateur quantique soit disponible pour les décrypter. Le seul critère est évidemment que les données aient encore une valeur et ne soient pas encore tombées dans le domaine public au moment où il devient possible de les décrypter. Ce n'est pas le cas des informations échangées par le commun des mortels, mais il existe des applications qui requièrent une protection de longue durée. On peut penser ici par exemple aux communications militaires et gouvernementales, ou encore aux données médicales personnelles.

Il convient ici encore de préciser que lorsque l'on parle d'ordinateur quantique, il ne faut pas imaginer un PC installé sous un bureau, mais plutôt un coprocesseur spécialisé couplé à un ordinateur conventionnel, le coprocesseur se concentrant sur certaines tâches bien définies. Il faut aussi noter que le nombre d'algorithmes quantiques offrant des performances supérieures à leur contrepartie classique est relativement limité, environ une quinzaine. Les détracteurs de l'ordinateur quantique ne se privent pas de le rappeler. Ce nombre est certes limité, mais certains de ces algorithmes quantiques ont un impact drastique dans des domaines importants.

MYTHE N°5 :
LA CRYPTOGRAPHIE QUANTIQUE PERMET DE TRANSMETTRE DES INFORMATIONS AVEC UNE CONFIDENTIALITE ABSOLUE

Non, la cryptographie quantique ne permet pas de transmettre des informations avec une confidentialité absolue. Elle permet en revanche d'échanger une séquence de bits aléatoires et de vérifier s'ils ont été interceptés ou non.

On peut utiliser une image pour tenter d'expliquer le principe de cette technologie. Un canal de communication, c'est un peu comme une partie de tennis. L'émetteur de l'information prend une balle de tennis, y inscrit le message et l'envoie à son partenaire. Celui-ci attrape la balle et lit le message. Le risque, c'est qu'un troisième joueur soit placé entre les deux premiers et se munisse d'un filet à papillon. Il pourrait ainsi intercepter les balles et lire les messages, avant de les transmettre plus loin.

Avec la cryptographie quantique, c'est un peu comme si on remplaçait les balles de tennis par des bulles de savon. Si quelqu'un tente de les intercepter, elles éclatent et la communication est interrompue, générant ainsi une alarme.

Il est évident que personne n'utilise des balles de tennis pour transmettre des messages. Dans tous les systèmes de communication, il y a toutefois toujours un support physique qui transporte l'information. Dans les réseaux à haut débit moderne, les données voyagent sous la forme d'impulsions lumineuses guidées par des fibres optiques. Ces impulsions lumineuses

sont intenses et sont constituées de millions de grains de lumière, appelés photons. Pour intercepter les communications sur un tel réseau, il est possible d'extraire quelques pourcents de la lumière sans perturber les autres photons. C'est par exemple possible en courbant légèrement la fibre optique de façon à induire des fuites. On recueille ainsi l'intégralité des communications.

L'idée de la cryptographie quantique est de remplacer ces impulsions intenses par des impulsions élémentaires constituées d'un seul grain de lumière. Un photon est un objet décrit par les lois de la physique quantique. Celle-ci stipule qu'il n'est en général pas possible de procéder à une mesure sur un système sans le perturber. Il s'agit du principe d'incertitude d'Heisenberg. Par analogie, il n'est pas possible de toucher une bulle de savon sans la faire éclater. Il s'agit ici d'une explication simplifiée du principe de la cryptographie quantique. Il n'en reste pas moins que cette technologie exploite les lois de la physique quantique pour mettre en évidence une interception de communications.

Toutefois, il est important de réaliser que cette détection d'une interception a lieu à posteriori. Cette technologie n'empêche pas l'espionnage, mais elle le révèle. Il serait ainsi inapproprié de l'utiliser pour échanger des données confidentielles. Il vaut mieux l'utiliser pour transmettre une séquence de bits aléatoires puis vérifié s'ils ont été interceptés ou non. Si ce n'est pas le cas, on peut établir que la séquence n'est connue que par l'émetteur et le récepteur. Elle peut donc être utilisée comme clé de chiffrement avec un procédé symétrique.

Plutôt que de parler de cryptographie quantique, il vaut mieux ainsi dénommer cette technologie distribution quantique de clés. Il faut aussi insister sur le fait que cette technologie ne vise pas à remplacer tous les procédés de cryptographie conventionnelle. Il s'agit plutôt d'une primitive supplémentaire permettant d'échanger une clé symétrique et donc de compléter l'arsenal des procédés conventionnels. Une des forces de la distribution quantique de clés est que sa sécurité ne repose que sur les lois de la physique quantique, sans aucune hypothèse mathématique. Elle peut ainsi être démontrée de façon rigoureuse.

MYTHE N°6 :
LA CRYPTOGRAPHIE QUANTIQUE, ARME ABSOLUE

La sécurité de la cryptographie quantique peut se démontrer de façon rigoureuse à partir des lois de la physique quantique. Elle est bien évidemment basée sur une hypothèse – la physique quantique est correcte – mais celle-ci est étayée par plus d'un demi-siècle de recherches théoriques et expérimentales. La physique quantique est une des théories physiques dont les prédictions ont été vérifiées avec la plus grande précision.

En comparaison, la sécurité des principaux procédés de chiffrement asymétrique repose sur deux hypothèses. Premièrement, les fonctions à sens unique sont vraiment à sens unique. On ne connaît actuellement pas d'approches permettant d'inverser les fonctions à sens unique de façon efficace, mais il n'existe aucune preuve formelle qu'une telle approche ne puisse être découverte. Si c'était le cas, la sécurité de ces procédés serait réduite à néant.

La seconde hypothèse a déjà été discutée. Ces procédés asymétriques sont vulnérables à l'ordinateur quantique et il faut donc supposer qu'un tel calculateur n'existe pas. C'est probablement vrai aujourd'hui, mais combien de temps cela le restera t'il ?

La sécurité de la cryptographie quantique n'étant basée sur aucune hypothèse technologique, elle est idéale pour compléter l'arsenal des procédés conventionnels de façon à protéger des informations dont la durée de vie est longue et dépasse quelques années.

Toutefois, la cryptographie quantique n'a t'elle pas été cassée ? Certains résultats scientifiques récents rapportés de façon erronée ou tronquée dans la presse grand public pourraient le laisser croire. Toutefois, ces résultats ne rapportent que l'exploitation de failles dans certaines implémentations de systèmes de cryptographie quantique. Ce n'est donc pas la cryptographie quantique qui est cassée, mais une réalisation particulière. Ces recherches ont montré qu'il est parfois possible de tirer parti d'imperfection pratique des composants utilisés dans un système pour le rendre vulnérable. Ce qui est en cause, c'est une mauvaise implémentation, mais le principe de la cryptographie quantique reste fondamentalement sûr. Il est bien évident que les systèmes de cryptographie conventionnelle peuvent eux aussi être vulnérables à des imperfections d'implémentation.

En résumé, la sécurité de la cryptographie quantique repose sur une base – la validité de la physique quantique - complètement différente de celle des techniques conventionnelles – inexistence des ordinateurs quantiques et robustesse de certains problèmes mathématiques. En ce sens, on peut considérer avec raison qu'elle représente un saut… quantique. De là à justifier le qualificatif d'arme absolue, il y a certainement un pas qu'il vaut mieux ne pas franchir. Il ne faut d'ailleurs pas oublier les limitations de cette technologie qui requière une connexion par fibre optique de bout en bout et dont la portée n'excède actuellement pas les 250 kilomètres.

MYTHE N°7 :
LES TECHNOLOGIES QUANTIQUES EN SONT ENCORE AU STADE DU LABORATOIRE

Il faut tout d'abord s'entendre par ce qu'on appelle technologie quantique. Le laser, et son oscillation lumineuse collective, est prédit par la physique quantique et a été démontré pour la première fois il y a plus de 50 ans. Aujourd'hui, il s'agit évidemment d'un composant banal que l'on trouve même dans les applications grand public. Un laser n'est toutefois pas purement quantique, car il s'agit d'une manifestation macroscopique d'un phénomène quantique. Une telle source lumineuse produit des millions de grains de lumière, ou photons, qui se comportent selon les lois de la physique classique.

Ce qui est nouveau, c'est de travailler au niveau d'un système quantique élémentaire – un seul photon, un seul atome, une seule particule – et de lui associer une valeur binaire pour réaliser des tâches jusque là impossibles. Il s'agit d'applications de la théorie quantique de l'information. Evidemment, ces technologies sont beaucoup moins mûres que le laser.

Il est ainsi probable qu'aucun ordinateur quantique complet n'ait encore été développé dans le monde de la recherche publique. Des composants élémentaires, des « portes » quantiques, ont été développés au moyen de différentes technologies, mais il reste difficile des les assembler pour réaliser l'équivalent d'un processeur quantique. Le problème principal est lié à la décohérence, c'est à dire la perte de leurs propriétés quantiques par ces bits quantiques – on parle de qubits. Cette décohérence est causée par une interaction des qubits avec l'environnement qui les parasite. Pour réaliser un ordinateur quantique, il est donc important de pouvoir isoler les qubits de l'environnement pendant les opérations. Cette isolation doit toutefois être contrôlable, car il faut pouvoir la déclencher initialement – pour saisir les données du problème – et après les opérations – pour lire le résultat du calcul. La difficulté réside donc la mise au point de techniques d'isolation que l'on peut enclencher et déclencher à volonté.

Il ne faut toutefois pas conclure des difficultés liées au développement de l'ordinateur quantique que toutes les technologies issues de la théorie quantique de l'information en sont encore au stade du laboratoire. Il existe en effet des produits de cryptographie quantique qui

permettent de sécuriser des communications sur un réseau optique. La première application publique remonte à 2007 où cette technologie a été déployée pour sécuriser un réseau utilisé par le département des technologies de l'information du Canton de Genève, en Suisse, pour le dépouillement des résultats d'élections. Des applications dans le secteur gouvernemental et financier commencent aussi à émerger. Les technologies actuelles permettent de sécuriser des liens d'une portée d'une centaine de kilomètres. Les systèmes de cryptographie quantique sont couplés à des boîtiers de chiffrement auxquels ils fournissent des clés de chiffrement.

Une autre application de la physique quantique est la génération d'aléas. La physique quantique étant intrinsèquement aléatoire – elle ne prédit pas le résultat exact d'une mesure, mais la probabilité d'obtenir un résultat parmi un ensemble – il est naturel de l'utiliser pour produire des nombres aléatoires. Il faut rappeler que la physique classique, quant à elle, est fondamentalement déterministe. Si l'on connaît l'état d'un système au temps initial, on peut prédire son évolution. Il n'est donc pas possible d'utiliser un processus de physique classique pour produire du hasard. Un ordinateur en particulier ne peut pas produire du hasard sans l'ajout d'un périphérique dédié à cette tâche. Les nombres aléatoires sont toutefois fort utiles dans de nombreuses applications. On citera à titre d'exemple la génération de mots de passe ou de clé de chiffrement. Des générateurs quantiques d'aléas existent depuis plus d'une dizaine d'année. Bien qu'il en existe plusieurs types, leur principe général est le suivant : des photons sont envoyés un par un sur un miroir semi-réfléchissant ; selon la physique quantique, chaque photon décide de façon aléatoire et indépendante s'il sera réfléchi ou transmis par le miroir ; il suffit de placer un détecteur de photons derrière chacune des deux sorties du miroir et de leurs associer une valeur binaire pour produire des bits aléatoires. Un de ces générateurs est disponible commercialement pour une somme de l'ordre de 1000 euros. Il a d'ailleurs été adopté par une grande partie des opérateurs des plateformes de jeu et loteries en ligne pour tirer au hasard les nombres gagnants ou brasser les cartes virtuelles de poker.

MYTHES ET LEGENDES DE LA SIGNATURE ELECTRONIQUE

Gérard Peliks, CASSIDIAN
an EADS Company

LA SIGNATURE ELECTRONIQUE, CE QU'ELLE N'EST PAS

Avec la généralisation des accès par l'Internet et la dématérialisation des documents, un jour viendra où la signature électronique va reléguer la signature papier au rang de curiosité du passé.

Aujourd'hui cette technologie, qui authentifie un document et en prouve l'intégrité, est mal connue, et dans le vécu quotidien, on utilise la signature électronique sans trop se poser de questions ou si on s'en pose, on apporte souvent de mauvaises réponses. C'est en particulier le cas sur l'utilité du certificat, objet de bien d'interprétations erronées.

Comme la signature manuscrite, la signature électronique permet à celui qui consulte un document signé d'authentifier le signataire. Mais la signature électronique, c'est encore autre chose.

Non, la signature électronique n'est pas la copie d'une petite partie d'un écran contenant une signature manuscrite, qu'on aurait coupée puis collée au bas d'un document Word. Cette manipulation s'appelle simplement du traitement d'image et n'a aucune valeur car on peut après tout placer ainsi n'importe quelle signature sur n'importe quel document. Il est alors trompeur d'établir une relation entre le document et la signature, même si celle-ci était, en toute honnêteté, déjà dans le document initial scanné.

La signature électronique n'est pas d'avantage ce que vous saisissez en apposant votre paraphe sur une tablette digitale et qui ajoute directement votre signature manuscrite au document que vous signez, comme un contrat de location de voiture, par exemple. Cela s'appelle la signature numérique et fait l'objet de lois spécifiques.

La signature électronique consiste en un petit fichier chiffré, accolé à un document, qui prouve en faisant appel à divers algorithmes et clés de chiffrement que le document a bien pour origine celui qui l'a signé (authenticité) et n'a pas été modifié depuis sa signature (intégrité). Le destinataire, par son logiciel de traitement du document signé, ou manuellement, peut en vérifier l'authenticité et l'intégrité. De plus, le signataire ne pourra pas prétendre ne pas avoir eu connaissance de son document signé (non répudiation).

Nous évoquons dans ce document les mythes et les légendes qui tournent autour de la signature électronique, et nous apportons des réponses. A la fin du document, vous trouverez des explications techniques plus détaillées sur les mécanismes qui interviennent dans l'établissement d'une signature électronique et sur la vérification du document signé.

MYTHE N° 1 : ON SIGNE PAR SON CERTIFICAT ELECTRONIQUE

Un certificat électronique ne sert en aucun cas à signer un document qu'on émet. Il intervient dans la vérification de la signature d'un document qu'on reçoit ou qu'on consulte.

Votre certificat personnel ne vous est d'aucune utilité pour signer un document ou pour vérifier la signature d'un document que vous recevez. Pour effectuer cette vérification, vous avez besoin, non pas de votre certificat mais du certificat de celui qui a signé le document.

En annexe, vous trouverez des explications techniques qui vous permettront de mieux saisir les mécanismes.

Un certificat prouve que quelqu'un, qui en est le propriétaire, possède aussi une clé de chiffrement privée qui lui est propre et qu'il a utilisée pour signer son document. Grace à ce certificat le destinataire du document pourra vérifier que ce document a bien été signé par celui dont il a le certificat.

Un certificat contient une clé, dite "clé publique", mathématiquement liée à une deuxième clé, dite "clé privée".

Si vous chiffrez un élément du document avec votre clé privée, cet élément ne pourra être déchiffré qu'avec votre clé publique correspondante, qui se trouve dans votre certificat que vous remettez au destinataire du document. Inutile de prendre des précautions pour transférer votre certificat, celui-ci ne contient aucune donnée confidentielle.

Votre certificat est lui-même signé par une autorité de confiance, qui utilise bien sûr le même mécanisme, pour prouver que la clé publique trouvée dans le certificat est bien la vôtre, c'est-à-dire correspond bien à la clé privée que vous possédez et avec laquelle vous avez signé le document.

Vous signez votre document avec votre clé privée, le destinataire de votre document signé vérifie votre signature avec votre clé publique.

L'élément chiffré puis déchiffré qui a servi à établir qui a signé le document est une "empreinte", ou anglais un "hash" et en bon français un "condensat".

On ne signe donc pas avec un certificat électronique, ni avec la clé publique qu'on trouve dans le certificat, mais avec sa clé privée.

MYTHE N° 2 :
LE CERTIFICAT EST CONFIDENTIEL ET IL FAUT LE PROTEGER

Non, un certificat n'est pas confidentiel, c'est un fichier tout à fait visible et public, destiné à être lu et utilisé par n'importe qui. Le certificat ne contient aucune donnée confidentielle, tout son contenu est en clair, mis à part l'élément chiffré dont nous avons parlé au mythe no 1.

Le certificat est par contre, lui-même, signé électroniquement par une autorité de confiance qui en atteste l'authenticité et l'intégrité. Si vous modifiez ne serait-ce qu'une virgule dans le certificat, cette modification apparaîtra au logiciel de traitement du certificat comme n'étant plus signé par l'autorité de confiance que ce certificat indique.

Le certificat contient une clé de chiffrement publique, qui correspond à la clé privée possédée également par le propriétaire du certificat. Comme le nom des clés l'indique, la clé publique trouvée dans le certificat est publique et donc n'est pas confidentielle.

Seule la clé privée correspondant à la clé publique est confidentielle, et son propriétaire ne doit jamais la dévoiler. La clé privée n'est bien évidemment pas dans le certificat mais, dans le cas idéal, sur un support amovible, tel qu'un token USB protégé par un code PIN.

Le certificat est lui-même signé par une autorité de confiance qui a chiffré un élément du certificat (l'empreinte du certificat qui est l'élément dont nous avons parlé au mythe no 1).

Vous possédez le certificat de l'autorité de confiance, contenant sa clé publique (attention, c'est un deuxième certificat, celui de l'autorité de confiance).

L'empreinte chiffrée du certificat peut être alors déchiffrée, par vous, à l'aide de la clé publique de l'autorité de confiance et ainsi vous êtes sûr de l'authenticité et de l'intégrité du certificat qui est attestée par l'autorité de confiance.

Mais si ne possédez pas le certificat de l'autorité de confiance ? Alors vous ne pouvez pas vérifier la validité (authenticité et intégrité) du certificat que cette autorité a signé. Rassurez-vous, vos logiciels connaissent déjà les certificats de nombreuses autorités de confiance, et ceux qui vérifient les signatures électroniques, savent vous demander d'ajouter, aux certificats des autorités que vous connaissez déjà, le certificat de telle autorité de confiance, et vous indiquent en général d'où le télécharger.

MYTHE N° 3 : UNE SIGNATURE ELECTRONIQUE EN VAUT UNE AUTRE

Bien entendu, nous ne parlons pas ici de l'identité de celui qui signe. Il est sûr qu'un document signé par un notaire ou par une autorité officielle a plus de valeur devant la loi qu'un document signé par un inconnu. Nous parlons ici de la validité d'une signature, qui que soit le signataire. En d'autres termes nous parlons de l'adéquation entre le signataire et sa signature.

Il existe différents niveaux de confiance pour les signatures parce qu'il existe différents niveaux de confiance pour les certificats. Tout dépend qui en établit la validité et comment les certificats ont été obtenus.

Il y a également différents niveaux de confiance à accorder aux certificats suivant les algorithmes de chiffrement et de calcul d'empreinte utilisés et la longueur des clés de chiffrement. L'algorithme de calcul d'empreinte recommandé aujourd'hui est le SHA2 et la longueur des clés pour le chiffrement asymétrique RSA est de 2048 bits.

La première chose qu'on regarde dans un certificat est l'autorité de confiance qui l'a signé. Si le destinataire a confiance en cette autorité, le certificat peut être utilisé pour en tirer la clé publique qu'il contient afin de vérifier qui a signé le document. Si le destinataire ne fait pas confiance en l'autorité qui a signé le certificat, il ne fera pas confiance en la signature du document.

Les autorités de confiance n'ont de sens que par la confiance qu'elles inspirent à leurs clients qui achètent leurs certificats (et avec chaque certificat la clé privée qui correspond à la clé publique que le certificat contient.

Cette confiance peut être accordée par exemple aux certificats signés par une autorité de confiance de même nationalité que le destinataire du document signé, ou alors à une autorité de confiance reconnue par beaucoup d'état comme Verisign qui est une autorité américaine.

Et surtout, il est important de connaître comment un certificat a été décerné à son propriétaire. Le certificat et la clé privée ont pu être achetés par courriel, à travers l'Internet, juste en fournissant une adresse et en le payant. A l'autre bout de l'échelle, le certificat, et sa clé privée associée ont pu être décernés par une autorité de confiance qui convoque l'utilisateur et s'assure de son authenticité, avant de lui remettre sa clé privée et le certificat qui contient sa clé publique.

On distingue plusieurs classes de certificats. Un certificat s'il est obtenu sans formalités, pourvu qu'on le paye, est un certificat qui n'est pas de la même classe qu'un certificat obtenu après déplacement et authentification forte de l'utilisateur. En France, seuls les documents

signés et vérifiés avec des certificats à partir d'une certaine classe ont même valeur juridique que les documents qui présentent une signature manuscrite.

MYTHE N° 4 :
SIGNER, C'EST CHIFFRER ET CHIFFRER C'EST SIGNER

Non, signer n'est pas chiffrer. Il y a des documents signés et des documents chiffrés. Il y a aussi des documents à la fois signés et chiffrés. En fait la signature et le chiffrement sont deux fonctions différentes avec des buts différents. Le chiffrement assure la confidentialité alors que la signature assure l'authenticité et l'intégrité du document sur laquelle elle porte. Un document peut être signé mais être en clair.

La signature du document, d'un point de vue technique fait appel à un calcul d'empreinte, puis cette empreinte est chiffrée par chiffrement asymétrique. De même la vérification de la signature du document fait appel aussi au chiffrement asymétrique pour déchiffrer l'empreinte avec la clé publique correspondant à la clé privée.

Mais seule l'empreinte du document est chiffrée ou déchiffrée, le document lui peut ne pas être chiffré. La signature électronique n'assure pas la confidentialité du document.

A l'opposé, rien ne prouve qu'un document chiffré l'ait été par son propriétaire et qu'il n'ait pas été modifié par une tierce personne.

MYTHE N° 5 :
UNE SIGNATURE ELECTRONIQUE, C'EST POUR LA VIE

La signature n'est vérifiable que durant la période de validité du certificat.

Outre la clé publique, le certificat contient la date à partir de laquelle il commence à être valable et la date à partir de laquelle il ne sera plus valable. Comme le certificat est lui-même signé par une autorité de confiance, si on falsifie ces dates, cela se remarque. Les logiciels de vérification des signatures tiennent compte de ces dates.

Il existe également des listes de révocation de certificats. Si le certificat du signataire a été révoqué, le logiciel de traitement de signature électronique refusera de considérer la signature du document comme valable, même si le certificat est encore dans ses dates de validité.

Une signature électronique n'est donc vérifiable, par logiciel, que durant la période de validité du certificat qui possède la clé publique avec laquelle on le vérifie.

Mais si le document a été signé alors que le certificat pour vérifier la signature était encore valable ? Bien entendu, même quand le certificat a expiré ou a été révoqué, la signature peut être tout de même recevable par un être humain qui prend de la hauteur par rapport à un logiciel de traitement de signatures électroniques, qui agit mais n'interprète pas.

C'est le même cas qui se pose si un contrat a été signé par un employé qui était dans une entreprise au moment de la signature, et l'a quittée depuis.

LES MECANISMES DE LA SIGNATURE ELECTRONIQUE

Pour comprendre le mécanisme de la signature électronique, il faut connaître deux mécanismes qui sont le calcul d'empreinte et le chiffrement asymétrique.

Le calcul d'empreinte consiste à calculer, à partir d'une chaine de caractères de longueur quelconque, un ensemble de bits (l'empreinte) dont le nombre fixe est déterminé par l'algorithme de calcul d'empreinte. C'est par exemple 128 bits pour le MD5 et 160 bits pour

le SHA1. Si la chaine de caractère de longueur variable subit la moindre modification, son empreinte produite sera différente. Un document est donc caractérisé par son empreinte.

Le chiffrement asymétrique fait intervenir deux clés. L'une pour chiffrer, l'autre pour déchiffrer. L'une des clés est privée et doit être gardée secrète par son propriétaire, l'autre est publique et son propriétaire peut la donner à tout le monde. Cette clé publique est placée dans un certificat électronique qui atteste qu'elle correspond bien à la clé privée détenue par le propriétaire des deux clés.

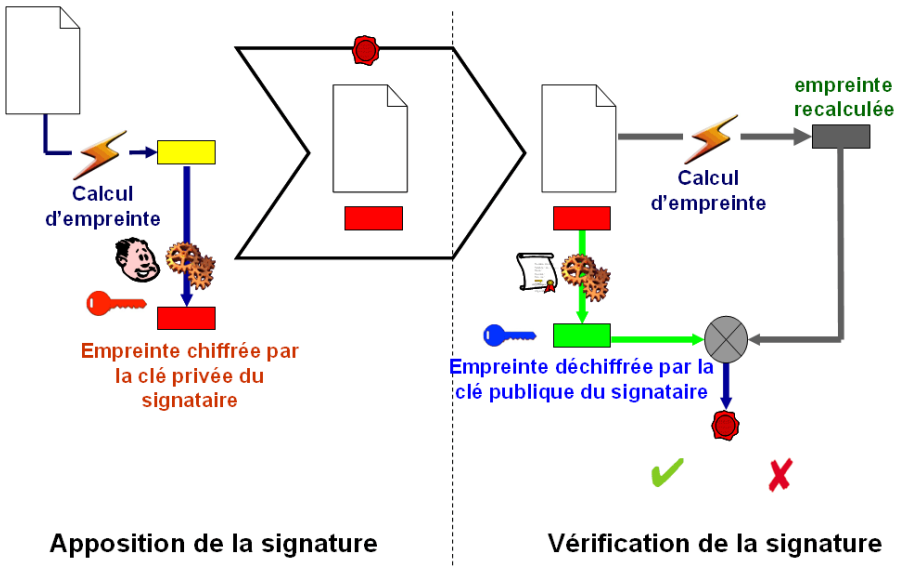
La clé publique est contenue dans un certificat qui est signé par une autorité de confiance. Bien entendu, connaissant la clé publique, il n'est pas possible d'en déduire la clé privée. Quand on chiffre avec l'une des clés, on ne peut déchiffrer qu'avec l'autre. Dans la signature électronique, c'est la clé privée qui est utilisée pour chiffrer et la clé publique pour déchiffrer. Dans le chiffrement asymétrique d'un document, c'est l'inverse.

Le signataire calcule l'empreinte du document à signer et la chiffre avec sa clé privée. Il joint l'empreinte chiffrée au document qui est alors signé.

Ceux qui vérifient la signature du document ont besoin de la clé publique de celui qui l'a signé, donc du certificat qui la contient. Ils déchiffrent grâce à la clé publique l'empreinte chiffrée. Ils recalculent, à partir du document reçu, l'empreinte de ce document. Si l'empreinte déchiffrée est la même que l'empreinte recalculée, la signature est prouvée.

Le document est authentique car son empreinte n'a pu être chiffrée que par celui qui détient la clé privée. Le document signé est intègre puisque le calcul de l'empreinte du document signé est identique au calcul d'empreinte du document avant sa signature.

Principe :



Terminons cette exploration en soulignant un arrêt de la Cour de Cassation qui par un arrêt du 30 septembre 2010 rappelle les formes impératives que doit revêtir un échange électronique pour acquérir une force probatoire et une valeur juridique donnant ainsi son importance à cette technologie : " Sans signature électronique garantissant identité du signataire et intégrité du message, le courriel n'a pas plus de valeur juridique qu'une lettre anonyme faite de collages de caractères découpés dans les journaux".

MYTHES ET LEGENDES DU MANAGEMENT DES EVENEMENTS ET DE L'INFORMATION DE SECURITE

Gérard Gaudin, Consultant indépendant, initiateur du Club R2GS

Le management des évènements et de l'information de sécurité (appelé dans le monde anglo-saxon SIEM – Security Information and Event Management) est un domaine constituant un sous-ensemble de la GOS (Gestion Opérationnelle de la Sécurité), ou de la LID (Lutte Informatique Défensive), ce dernier terme étant couramment utilisé dans les milieux gouvernementaux et de la Défense Nationale.

MYTHE N° 1 : LE SIEM, C'EST DE LA GESTION DE LOGS

Le domaine SIEM (Security Information and Event Management), dont l'existence date du début des années 2000 et a été ainsi dénommé par un grand cabinet de conseil en stratégie anglo-saxon, a été fortement assimilé à l'origine à la gestion d'évènements de sécurité en temps réel. Or, le pourvoyeur d'informations pour la détection et la mise en évidence d'évènements de sécurité s'est avéré être naturellement l'ensemble des logs disponibles sur le système d'information des entreprises et des organisations, du fait de leur organisation structurée et de leur orientation « changement d'état ». Mais progressivement avec la maturation du domaine sont apparus des besoins de sources d'informations plus diversifiées, telles des données de contrôle de conformité et d'intégrité, des données issues des scanneurs de vulnérabilités, des données issus des systèmes d'administration réseau et système, ou des données d'identification ou issues des référentiels système. Les outils initiaux d'analyse et de corrélation de logs sont de ce fait en train d'évoluer vers des outils traitant plus largement des informations : logs, données issues des systèmes d'administration réseau et système (incidents de type dysfonctionnement et charges notamment), données relatives aux vulnérabilités ou aux non-conformités des systèmes ou applications, ou fichiers de description des paramètres de configuration des systèmes sous surveillance. On peut ainsi considérer à ce sujet que plus de la moitié des sources utiles sont de nature différente des logs.

MYTHE N° 2 : LES ASPECTS TECHNIQUES SONT PREDOMINANTS

Le domaine SIEM a très vite été identifié essentiellement aux outils de gestion de logs, sous l'influence puissante des éditeurs de ces outils. La suite logique a été une focalisation quasi exclusive des organisations lançant des projets sur les aspects techniques, au détriment de la mise en place des liens avec les moyens en matière de gouvernance sécurité que sont le suivi des points de repère du SMSI (Système de Management de la Sécurité de l'Information) et la mesure des risques résiduels principaux pesant sur les systèmes d'information. Cette situation, qui a consisté ainsi à se priver de la raison d'être et de la finalité réelle de ces outils (le « Check » et le « Act » du modèle PDCA couramment utilisé en qualité et en sécurité), a conduit à des difficultés de justification de la pertinence des investissements consentis, les effets essentiels de levier de progrès n'étant ni perçus ni mis en valeur ; d'où l'apparition dans la précédente décennie de nombreux échecs et désillusions. Tirant les leçons de ces fausses pistes et de ces approches « bottom-up » erronées, nombre d'organisations ont entamé

depuis peu (notamment sous l'impulsion du Club R2GS créé en 2009 en France) des démarches radicalement opposées, pouvant être définies comme des démarches globales d'entreprise de type « top-down » et s'articulant sur les 3 axes phares suivants :

- Appui sur les 2 piliers de base que sont les risques principaux pesant sur le SI de l'organisation (incidents les plus fréquents ou les plus graves) et son SMSI, pour définir des objectifs naturels de surveillance et de détection,
- Appui sur un ensemble de modèles et processus (dont un modèle de classification des évènements de sécurité, un référentiel d'indicateurs et un référentiel de plans de réaction), permettant de décliner finement les politiques d'assurance sécurité de l'organisation,
- Accent sur la promotion auprès de l'organisation sécurité et IT de la démarche SIEM et des modèles et processus associés.

MYTHE N° 3 : LE SIEM EST UNIQUEMENT UNE AFFAIRE DE SPECIALISTES

Le domaine SIEM est un domaine réputé difficile d'accès, où les risques d'échec sont réels comme il a été indiqué précédemment. Les équipes opérant dans ce domaine, en premier lieu des équipes de terrain opérationnelles ayant pour mission de défendre l'entreprise contre toute attaque externe ou interne, doivent maîtriser les différents types et méthodes d'attaque ainsi que les outils les soutenant dans leur tâche. Mais dans cette lutte quotidienne et de tous les instants, les autres acteurs de l'entreprise ou de l'organisation ont un rôle pouvant souvent être clé. Il s'agit :

- Des managers des diverses entités de l'organisation qui doivent transmettre les enjeux de certains comportements humains en terme de risques pour l'activité,
- Des responsables du SI qui doivent veiller à ce que la sécurité soit une composante majeure des nouveaux projets et de la production et de l'exploitation des réseaux et systèmes,
- Des managers de haut niveau qui doivent créer une culture sécurité de manière similaire à ce qui a été généralement fait dans le passé avec la qualité.

Dans cet effort de plus en plus nécessaire bien que de priorité variable selon le secteur d'activité concerné, les facteurs comportementaux prennent une part de plus en plus prépondérante, dans un contexte où les vulnérabilités de nature technique disposent aujourd'hui des outils adéquats pour pouvoir être maîtrisées. Cette attention impérative au facteur humain ne peut que conduire à la diffusion progressive des thèmes SIEM au sein des grandes organisations les plus exposées. Les vols d'informations tant stratégiques qu'à caractère personnel sont là pour nous rappeler, notamment quand ils font les unes de la presse, que les politiques de sécurité doivent marcher main dans la main avec les politiques de ressources humaines sur cette question hautement symbolique de l'éthique envers son employeur. Ces aspects seront de plus en plus cruciaux dans un monde hyperconcurrentiel ou souvent dominé par l'avidité où tout se monnaye. Dans les fuites ou les vols d'informations sensibles, les collusions volontaires ou involontaires d'employés sont en effet présentes dans plus de 60 % des cas de sinistres, selon certaines études et certains chiffres pouvant être considérés comme fiables.

MYTHES ET LEGENDES DU PCA / PRA[44]

Bruno Hamon, MIRCA

Construire un PCA c'est conduire un projet d'entreprise, transversal et multidisciplinaire.

Son ardent objectif consiste à préparer l'entreprise à faire face à un sinistre, pour assurer sa survie. La construction du PCA impose la production d'un plan d'actions détaillé sur ce qu'il faudra faire si le sinistre survient.

Construire le PCA, revient donc à adapter l'organisation d'une entreprise pour atteindre l'objectif de continuité, lui-même orienté vers la satisfaction de ses clients.

Pour réussir cet ambitieux projet, vous devez déjouer les pièges et les mythes qui sont nombreux et dont certains ont la vie dure.

MYTHE N° 1 : JE N'AI BESOIN DE PERSONNE POUR CONSTRUIRE MON PCA

En aucun cas !

Comme tout projet transverse, vous devez susciter l'adhésion de tous. Il faut mobiliser dès la construction du PCA la direction générale, seule autorité pour le légitimer. Cette adhésion, c'est celle que l'Entreprise attend de ses collaborateurs au moment du sinistre. Dès le projet de mise en place du PCA, vous devez communiquer vos objectifs de résultats et de délais.

Il faut éviter les cathédrales technologiques et les effets tunnels tout comme il est nécessaire de fixer des objectifs atteignables. Redémarrer toutes vos activités sous 2 heures, ce n'est pas un objectif réaliste, et c'est rarement ce dont vous avez besoin. Le PCA dans l'entreprise, c'est l'affaire de tous

MYTHE N° 2 : JE VAIS D'ABORD TRAITER L'INFORMATION DANS MON PCA

Surtout pas

Il faut tout d'abord mobiliser vos directions Métier, seules compétentes pour définir les objectifs opérationnels à atteindre au moment du redémarrage, et en déduire les moyens et les outils nécessaires. Ce n'est qu'après que vous pourrez mobiliser vos fonctions support, dont la fonction informatique, en répondant précisément aux besoins des directions Métier.

Il n'y a pas de belle infrastructure technique : il n'y a que celle qui répond aux besoins des opérationnels métier, dans les délais et là où elle est attendue.

MYTHE N° 3 : JE N'AI PAS BESOIN DE TESTER MON PCA

Grave erreur !

Dans un PCA, il n'y a ni héros, ni exploit personnel, ni improvisation subtile de dernière minute.

[44] *Plan de Continuité d'Activité / Plan de Reprise d'Activité*

Les improvisations de dernière minute sont rarement géniales.

Quand votre PCA est défini, documenté, et que tous ont été entraînés à son exécution, il faut alors mobiliser toute l'Entreprise sur l'objectif des tests du PCA.

Seuls ces tests permettent d'établir avec certitude que votre PCA est opérationnel.

Pour les deux volets du PCA souvent désignés par le PCO (Plan de Continuité Opérationnel qui traite l'angle Métier) et le PCI (Plan de Continuité Informatique qui lui traite de la partie technique), il est fortement recommandé de procéder régulièrement à des « tests unitaires » (une seule procédure) mais aussi réaliser des « tests de bout en bout » (enchainement de l'ensemble des procédures)

MYTHE N° 4 : UN PCA, ÇA COUTE LES YEUX DE LA TETE

Fausse idée !

La mise en place d'un PCA est une nécessité que l'on rend accessible en ajustant la démarche aux enjeux d'une entreprise tout en faisant preuve de pragmatisme et du souci de la maîtrise de l'investissement.

Par conséquent, un projet PCA doit être adapté au contexte de l'entreprise qu'il va toucher ; la prévention doit être privilégiée, dans certain cas l'externalisation du secours peut également permettre à l'entreprise de ne se concentrer que sur son cœur de métier. Par ailleurs, on a pu constater ces dernières années que les coûts des solutions techniques avaient drastiquement baissé ; dans certain cas la solution technique peut répondre aux chocs extrêmes mais aussi aux problèmes de disponibilité du quotidien. Enfin, notons qu'un PCA peut commencer par une simple clé USB !

MYTHE N° 5 : UN PCA EST UN PROJET SANS RETOUR D'INVESTISSEMENT

Autre fausse idée !

Décider de mettre en place un PCA ressemble, à peu de choses près, à la signature d'un contrat d'assurance.

De fait, la question à se poser alors n'est pas tant « Avons-nous besoin d'un PCA ? » que

« Jusqu'à quel point avons-nous besoin de définir les mesures de continuité d'activité de notre organisation ».

Cette approche spécifique privilégie donc l'adéquation des mesures aux enjeux d'une entreprise et doit garantir un retour sur investissement par construction.

Dans tous les cas de figure, les bénéfices attendus doivent s'ajuster aux risques encourus.

MYTHE N° 6 : UN PCA N'EST BON QUE POUR LES GRANDS COMPTES

Encore une idée fausse!

Une PME reste plus sensible aux risques de choc extrême car elle réside souvent sur un seul et même site. Autrement dit, son bassin commercial est souvent régional et son assise financière demeure plus fragile. Très rares sont les cas où les PME peuvent compter à la fois sur le recouvrement des fonctions-clés mais également sur une concentration de leurs ressources vitales.

Par conséquent, une PME peut moins se permettre de laisser les sinistres décider de son avenir en comparaison avec ses principaux et gros concurrents qui eux sont généralement assis sur plusieurs sites/continents ou adossés à des groupes/investisseurs puissants.

Dans tous les cas, il est important de bien calibrer l'organisation de crise et le dispositif du PCA.

Ces deux aspects doivent être aussi souples et agiles que la PME.

MYTHE N° 7 : MON PCA EST ACHEVE ET TESTE : LE TRAVAIL EST TERMINE

Malheureusement non, il ne fait que continuer !

La vie de l'Entreprise continue, et vous devez adapter les processus de décision de l'Entreprise pour qu'ils « pensent PCA » : un nouvel embauché, un nouveau client, un nouveau fournisseur, un nouveau produit, un nouveau contrat, un nouveau règlement, un nouveau site de production, une nouvelle agence commerciale, une croissance externe, et, bien entendu, un nouvel outil informatique : autant de changements à traduire sur votre PCA, pour le maintenir à jour et opérationnel.

C'est ce que l'on appelle le Maintien en Condition Opérationnelle (MCO) du PCA qui doit prendre en compte toutes les évolutions et mises à jour de votre PCA au sein de votre organisation.

CONCLUSION

Toute décision de mise en place d'un PCA exige une volonté affirmée, demande du temps et de l'énergie, suppose un budget en conséquence. Le PCA impose également un suivi permanent, requiert un pilote motive, disponible, rigoureux et méthodique. D'un autre côté, le PCA va devenir à terme un élément commercial différenciateur : il est un moyen et non une finalité.

3° PARTIE : ASPECTS MATERIELS

MYTHES ET LEGENDES DE LA QUALITE DE SERVICE

Jacques Baudron, iXTEL

MYTHE N° 1 :
LA QUALITE DE SERVICE S'OBTIENT EN DIFFERENCIANT LES SERVICES

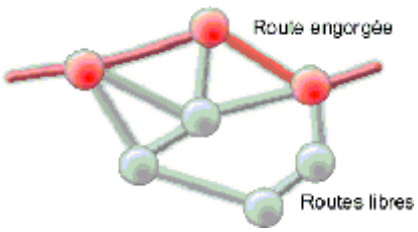
Ce n'est pas tout à fait exact. La différenciation de services gère la pénurie de ressources en situation de congestion.

Qu'est-ce que la congestion ? C'est une situation temporaire où un, voire plusieurs équipements, ne sont plus en mesure d'acheminer les flux pour cause de surcharge. En fonctionnement normal les équipements de réseaux – routeurs par exemple – orientent les paquets vers les ports de sortie. Lorsque la charge du routeur est importante les paquets doivent patienter en mémoire que les ressources se libèrent ; dès que la charge dépasse la capacité de l'équipement, des paquets sont perdus. La différentiation de service avantage dans ces opérations de délestage certains flux au détriment de flux moins prioritaires. L'ordre de priorité est attribué type de flux par type de flux à l'entrée dans le réseau. Par exemple un transfert de fichier sera retenu le temps que des flux sensibles au temps de transit (trafic interactif, réseaux de stockage …) et/ou des trafics sensibles aux variations de ce temps (voix, vidéo …) soient écoulés.

Parmi les limites inhérentes à ce mécanisme, précisons que la notion de priorité n'a de signification que si suffisamment de trafic est … non prioritaire. Dans quelle proportion ? 50 ? 70% ? Un chiffre absolu est délicat à déterminer. Ce qui est certain, c'est que la « concentration » en trafic prioritaire augmente à chaque traversée de nœud en congestion, dégradant d'autant les performances du mécanisme.

Effet de bord : les paquets détruits lors de la congestion seront ré-émis, augmentant ainsi la charge d'un réseau déjà sous tension.

Une piste pour améliorer la qualité de service est donc, non pas de gérer la pénurie en cas de congestion, mais de cerner les mécanismes à l'origine de la congestion. L'accusé numéro un est le comportement grégaire des paquets lors de leur périple dans le réseau. Partant tous des mêmes règles et des mêmes informations sur le réseau, les calculs de routes pour chacun des paquets aboutissent à des conclusions similaires. Résultat : le trafic se concentre sur un nombre restreint de routes. Et ceci quels que soient les pondérations et coûts attribués à chacun des liens du réseau.



Ce fonctionnement peut être visualisé à partir d'outils très simples sous forme d'historique. L'information intéressante n'est pas alors de voir qu'il y a eu congestion, - ça, tout le monde l'avait constaté - mais de savoir que des routes de contournement à même d'absorber le trafic étaient disponibles à ce moment..

Bien entendu, ce raisonnement ne vaut que dans la mesure où il y a plusieurs chemins physiques ou logiques disponibles. Les technologies WiFI qui partagent un médium unique entre plusieurs utilisateurs ne sont par exemple pas concernées.

C'est maintenant le travail de l'ingénierie de trafic de répartir le trafic sur l'ensemble des ressources du réseau à l'aide des outils et technologies disponibles.

MYTHE N° 2 :
LA PROTECTION CONTRE LES COUPURES SE FAIT EN MOINS DE 50 MILLISECONDES

Vrai et faux.

La protection consiste à basculer « rapidement » (en moins de 50 millisecondes) d'une voie normale vers une voie de secours pré-déterminée, contrairement à la restauration où les routes sont calculées après un défaut.

Cette valeur de 50 ms, arbitraire, est directement héritée des réseaux télécoms. La référence en matière de protection est le modèle SDH qui a construit ses mécanismes autour de ce chiffre.

Il faut considérer deux phases : la détection du défaut et la commutation sur des ressources de secours.

Aujourd'hui, toutes les technologies sont à même de commuter en quelques millisecondes d'une voie normale sur une voie de secours. Mais qu'en est-il de la détection du défaut ?

Les « antiques » réseaux de télécoms monopolisaient la bande passante en envoyant en permanence un signal qu'il y ait des informations à transporter ou non. Ce comportement coûteux présente un avantage pour la protection : il permet de détecter immédiatement (autrement dit en quelques centaines de micro-secondes) une détérioration du signal.

Dans le cas des réseaux par paquets, le principe de fonctionnement est différent. On n'envoie des paquets que lorsqu'on veut transmettre des informations. Mais alors, à partir de quel critère une absence de paquet doit-elle être interprétée comme une coupure ? Comment peut-on détecter une coupure dans un réseau IP ?

Remarquons que fondamentalement IP est un protocole d'interconnexion de réseaux (Internetwork Protocol) : par définition, il ignore la nature des réseaux interconnectés. Il perd la vue physique pour ne travailler qu'au niveau logique. Il est alors « logique » de ne plus avoir accès aux alarmes qui sont des informations liées à l'état physique du réseau.

Deux méthodes permettent néanmoins de retrouver ces informations d'alarme.

La première voie consiste à établir un échange permanent de messages (KeepAlive) entre nœuds voisins pour détecter les coupures. La cadence à laquelle il est recommandé d'effectuer cet échange est de 5 millisecondes. Malheureusement, que pèsent 5 millisecondes face à une congestion ? Combien de millisecondes dure une congestion ? 10 ? 100 ? 1000 ? Le problème est que toutes ces valeurs sont correctes, car ce temps est par nature non déterminé. Les 5 millisecondes sont de ce fait dans une zone d'incertitude et sont la source de fausses alarmes ; elle deviennent alors le plus fréquemment dans les configurations de réseau 1 voire 3 secondes. On se retrouve ainsi avec un système capable de cicatriser un défaut en moins de 50 millisecondes … après une détection en 1 seconde !

La deuxième voie consiste à faire fi du modèle en couches et à aller chercher directement au niveau physique les informations d'alarme. Le monde étant petit, la couche physique est typiquement SDH.

MYTHE N° 3 :
LA PROTECTION CONTRE LES COUPURES NE CONSOMME QUE PEU DE BANDE PASSANTE

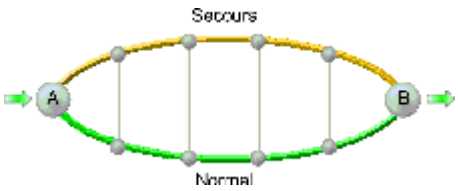
En terme de protection, la référence est constituée par les réseaux télécoms de type SDH, qui ont donné lieu à la définition de mécanismes aujourd'hui éprouvés. La définition de la protection dans les réseaux IP ou plus généralement par paquets laisse espérer une meilleure occupation de la bande passante. Or nous allons voir que si il y a effectivement un gain en l'absence de contrainte de temps, l'objectif de 50 millisecondes limite les options d'optimisation de la bande passante.

> Quel protocole pour une protection en 50 millisecondes? *La durée d'une congestion est incertaine, comprise le plus souvent entre 10 millisecondes et quelques secondes. Dans ces conditions, il n'est pas possible de garantir la réalisation d'un dialogue par échange de paquets dans un délai de 50 millisecondes.*

Première question : peut-on écouler du trafic de moindre priorité dans des ressources prévues pour la protection lorsque celle-ci n'est pas activée ? La réponse est oui si il n'y a pas de contrainte de temps et non dans le cas contraire.

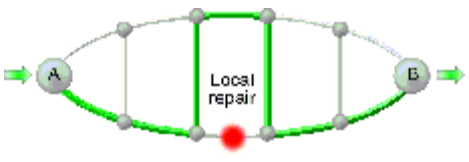
Dans un réseau « IP », deux situations peuvent se trouver. Soit les ressources sont suffisamment dimensionnées pour accepter le trafic rerouté en protection auquel cas on est dans la situation où il n'y pas de gain en bande passante, soit les ressources sont insuffisantes et la congestion, alors créée, est gérée par des mécanismes de priorité qui écartent le trafic « Best effort » au profit du trafic à protéger. Ces conditions de congestion ne permettent pas de spécifier une valeur maximum pour le temps mis à accomplir le reroutage.

Si une cicatrisation en moins de 50 millisecondes est recherchée, les ressources de protection doivent être prêtes à accueillir le trafic. Les ressources de protection doivent être réservées au même titre que les ressources de transport en mode normal. Il n'y a alors pas de gain en bande passante par rapport aux techniques de protection SDH.



Une deuxième question se pose au niveau des routes de protection. La solution la plus intuitive consiste à prévoir deux routes disjointes et de basculer de l'une à l'autre lors de l'apparition d'un défaut. Ce principe est utilisé pour la protection des réseaux télécoms classiques.

Malheureusement, ce principe s'accomode mal de la contrainte des 50 millisecondes. Pour pouvoir basculer de la voie « normale » vers la voie « secours », il faut faire parvenir l'information de défaut aux extrémités. Or cette information circule dans un réseau soumis aux situations de congestion encore amplifiées par la réaction à la coupure. Il n'est dans ces conditions pas possible de garantir un basculement sur la ressource de protection en temps requis.



Pour pallier le problème, le mécanisme « Fast Reroute » par exemple préconise une commutation directe de la part des extrémités du lien endommagé vers une route de secours locale sitôt le défaut constaté (local repair). Il n'y a plus ainsi à propager l'information jusqu'aux extrémités du flux. Par contre ce n'est pas sans conséquence sur l'occupation des ressources. La bande passante de secours est réservée sur chaque maille traversée.

La protection contre les coupures a un coût modéré tant qu'il n'y a pas de contrainte de temps mais est très exigeante dès que l'on cherche à retrouver les conditions des réseaux télécoms classiques.

MYTHES ET LEGENDES DES TECHNOLOGIES VOCALES

Philippe Poux, VocalNews.info

Reconnaissance automatique et synthèse de la parole sont nées sous l'impulsion de quelques chercheurs, autour du Professeur Jelinek, dans les laboratoires IBM.

Rapidement ce qui semblait aisé en traitement informatisé du signal s'est avéré mathématiquement complexe, gourmand en puissance de calcul … démontrant ainsi que notre cerveau est nettement plus efficace qu'un simple calculateur.

Avec des algorithmes basés sur les modèles de Markov, et l'augmentation régulière de la puissance de calcul des processeurs, ces technologies de la parole sont devenues réalité. On a vu alors des variantes dégradées envahir nos téléphones mobiles et d'autres les serveurs vocaux interactifs, avec plus ou moins de bonheur, laissant le champ libre à plusieurs idées reçues.

MYTHE N° 1 : LES CLIENTS N'AIMENT PAS PARLER A UN ORDINATEUR

La plupart des responsables de relation client pensent instinctivement déplaire à leurs clients en leur proposant ces technologies, sans étayer leur point de vue sur la moindre étude ou analyse. Et en oubliant que le premier souhait d'un client qui appelle … c'est d'obtenir une réponse. Le mode d'interaction importe peu.

En corollaire, on entend souvent que les technologies de la parole déshumanisent la relation client … rien n'est dit de tel concernant le site web ou les scripts contraignants imposés aux téléacteurs ;-)

Alors, basons-nous sur quelques faits démontrés. L'étude Forrester de début 2010 a montré que les consommateurs notent mieux les systèmes automatisés que les agents pour certaines interactions … car ces derniers sont tellement enfermés dans des scripts qu'ils répondent moins bien qu'un SVI. Le sondage a également révélé que les systèmes téléphoniques automatisés sont un attendus et acceptés comme service par 82 % des clients.

Par ailleurs l'impression désagréable de nombre de services vocaux vient de leur ergonomie déficiente. En effet, pourquoi faire confirmer les demandes lorsque l'on sait que le moteur de reconnaissance est bon dans 96% des cas ? C'est ce qu'a très bien compris Air France avec son service 3654, qui remercie à chaque information client et passe à la phase suivante.

L'étude BVA Service Client 2010 montre que la satisfaction client est de 79% avec un email et 75% au téléphone, contre 93% en face à face …

MYTHE N° 2 : LES HUMAINS SONT PLUS EFFICACES

Rien ne vaut un être humain, que ce soit pour écouter, comprendre, ou entrer en empathie. Les prescripteurs comme les chercheurs dévoués aux technologies vocales ne cherchent pas à remplacer l'humain, seulement à l'accompagner, l'aider. Et les questions complexes sont

plus du ressort de l'intelligence humaine, l'artificielle restant encore plus limitée que la reconnaissance de la parole.

Mais une fois ces jalons posés, force est de constater que si l'humain est plus efficace que l'ordinateur, c'est aussi une denrée rare et chère. Les entreprises continuent de considérer les centres de contacts comme des centres de coût et non de véritable relation client, aussi ils limitent le nombre des opérateurs. Au détriment de leurs clients.

MYTHE N° 3 :
INTERNET REMPLACE LES SERVICES VOCAUX

Les SVI auraient été un moyen de proposer du renseignement et self service avec le téléphone, Internet supplée donc à tous ces besoins. Ce point de vue se tient à un détail près, l'émergence de l'autre phénoménale révolution de ces dernières années, le Mobile.

Les usages ont profondément évolué, le mobile est nettement plus présent que l'accès internet et la convergence ne fera qu'accélérer la prédominance du Mobile.

C'est ce qu'ont très bien compris Larry Page et Sergei Brin, les fondateurs de Google, en expliquant fin 2008 qu'il leur fallait devenir aussi les leaders de la recherche d'information sur ces appareils et que l'interaction la plus naturelle était … la voix !

Ils ont alors créé un département entier pour développer leurs moteurs vocaux, lancé un service gratuit d'annuaire pages jaunes (1-800-GOOG-411) afin d'appréhender les comportements et d'affiner leurs modèles. Ce service a tellement bien fonctionné qu'ils proposent maintenant leurs premières applications vocales pour smartphones avec une qualité étonnante. Maintenant qu'il a rempli sa mission, le service 411 a été fermé …

MYTHE N° 4 :
LA RECONNAISSANCE VOCALE EST MORTE

Certaines technologies prennent moins de temps pour devenir matures. Aussi, certains analystes, constatant que les taux d'erreur réduisent lentement, que la parole n'a pas encore envahi tous nos appareils, en déduisent la mort de cette technologie.

Et il est vrai que la plupart des recherches en intelligence artificielle ont pris beaucoup de temps. Plus que prévu, pensé, rêvé … Car l'intelligence humaine est beaucoup plus complexe que ne le supposaient certains chercheurs. Ce n'est pas une raison pour jeter aux orties les systèmes experts, réseaux neuronaux et autres avancées.

Enfin, on verra rapidement que des usages simples de la reconnaissance de la parole dans des mobiles arrivent et rendent de véritables services. Il suffit de voir le succès de ces applications sur l'AppStore de l'iPhone ou sur Android.

MYTHES ET LEGENDES DU PAIEMENT MOBILE

Philippe Poux, MobilePaymentExpo

L'omniprésence des téléphones mobiles permet d'envisager une nouvelle dynamique pour les logiques de porte-monnaie électronique. Nous ne sortons plus jamais sans notre mobile alors que nous n'avons pas toujours un sou en poche, la solution semble donc évidente.

Pourtant le paiement depuis un mobile peine à décoller en Europe, alors qu'il s'est fortement développé en Asie (80 millions de porteurs au Japon) et que les transferts d'argent par ce biais sont largement en avance en Afrique.

En 2010, le nombre d'utilisateurs de solutions de paiement mobile dans le monde à dépassé les 108 millions, contre 70 en 2009, soit une progression de 54%. Selon Juniper Research, leurs achats représenteront 200 milliards de dollars en 2012 et plus de 600 en 2014 …

MYTHE N° 1 : NOUS AVONS ASSEZ DE MOYENS DE PAIEMENT

Il est vrai qu'avec la monnaie, le chèque, le virement et la carte bancaire, nous ne manquons guère de moyens de paiement. A la différence des pays africains où le taux de bancarisation est dramatiquement faible.

Mais cela n'explique pas tout. Nombreux sont les cas où la carte bancaire ne peut remplacer l'absence d'argent liquide … freinant notre capacité à satisfaire nos désirs d'achat. Le besoin d'une alternative existe donc bien. Il s'agit plutôt de résistance au changement. Et l'histoire a montré que l'assignat a eu besoin de bousculer les mentalités pour remplacer les pièces d'or.

Mais l'histoire a eu besoin aussi de batailles de pouvoir entre banquiers et opérateurs, chacun cherchant à imposer son modèle, pour profiter au maximum de cette manne de transactions monétaires qui s'annonce.

Au risque de laisser le champ libre à de nouveaux acteurs ?

MYTHE N° 2 : LES TECHNOLOGIES MANQUENT

Il y a débat entre NFC[45], non-NFC … mais c'est un faux débat. La vraie condition d'un déploiement de ce type de solution, c'est la disponibilité des offres et services. La technologie qui les fait fonctionner importe peu. Nos téléphones mobiles n'ont pas grand chose à voir avec les premiers radiotélécoms, mais le besoin de téléphoner est resté le même.

Par ailleurs, de grands acteurs, comme Nokia, Samsung, RIM, Apple, Google, ou Gemalto, préparent leurs offres.

Les conditions du marché existent, les technologies sont fiables, il ne manque plus qu'un consensus entre les acteurs.

[45] *NFC : Near Field Communication*

MYTHE N° 3 :
LES PROJETS PILOTES SONT DECEVANTS

17 initiatives en France, aucune dont vous ayez vraiment entendu parler … sauf pour Nice, l'initiative la plus récente et la plus prometteuse, qui a réuni Bouygues Télécom, SFR, Orange et NRJ Mobile autour du NFC.

Paypal, Amazon, Starbucks, Carrefour, Franprix, SNCF ... nombreux sont les acteurs économiques qui y sont allés de leur propre projet. Ce qui, à l'heure du village mondial et d'Internet, semble présomptueux, car on voit mal comment ils pourraient imposer un modèle à l'ensemble des autres marchands, institutions financières et opérateurs.

MYTHES ET LEGENDES DE LA FIN DES CABLES EN CUIVRE

Luc BARANGER, FFIE
Ladji DIAKITE, Syndicat professionnel des fabricants de fils et câbles énergie et télécom
Guy PERROT, Nexans

LES FAUSSES CERTITUDES

Certains Opérateurs ont tenté de nous persuader il y quelques années que tout notre trafic passerait par le WiMAX, et que de toute façon, à terme, il n'y aurait plus que des applications radio.

Puis la problématique du très haut débit est apparue; les difficultés de ces mêmes Opérateurs aussi. Malgré des contorsions impressionnantes – certains n'ayant pas hésité à parler de haut débit à 50 kbit/s – on décide alors que seule la fibre optique nous permettra de résoudre tous nos problèmes.

D'ailleurs, le câble de cuivre souffre de tous les maux : il est cher, nécessite le déploiement par des Installateurs, il génère des problèmes de CEM, et enfin, on peut se prendre les pieds dans les cordons !

A telle enseigne que tel Opérateur qui veut détourner notre attention des effets physiologiques éventuels des réseaux radio n'a pas hésité à assimiler les utilisateurs de câbles en cuivre à des crétins.

La question se pose de savoir s'il faut prévoir de mettre ces câbles au musée, à côté de la batterie de casseroles en cuivre, ou bien s'il faut continuer à prévoir de les utiliser.

MYTHE N° 1 : LA FIBRE OPTIQUE EST LE SEUL MEDIUM CAPABLE DE FOURNIR LES DEBITS DEMANDES AUJOURD'HUI

La question primordiale est de savoir de quoi l'on parle, de ne pas confondre débit et bande passante et de ne pas mélanger les transmissions à longue distance et les communications locales.

Le développement des fibres optiques dans les années soixante dix a fait naître d'immenses espoirs chez les opérateurs télécom qui y ont vu le Graal qui allait remplacer paires torsadées, coaxiaux et autres guides d'ondes.

La fibre optique en fait n'est qu'un guide d'onde comme un autre et ses propriétés de transmissions sont comme pour les autres guides d'ondes (y compris les paires torsadées et coaxiales) régies par les équations de Maxwell.

Son avantage réside dans sa petite taille qui lui permet de (ou l'oblige à) travailler à des fréquences beaucoup plus élevées que n'importe quel autre guide d'onde métallique. Corollairement les déperditions en fonction de la longueur deviennent quasiment négligeables (aujourd'hui de l'ordre de 0.1 à 0.3 dB au km).

Le câble de cuivre a longtemps été limité en fréquence par les imperfections des procédés de fabrication. Il faut dire qu'il y a cinquante ans on ne demandait pas à ces câbles de travailler au delà de 3 KHz, ce qui était largement suffisant pour transporter la voix !

La demande pour des fréquences plus élevées est née avec le développement des ordinateurs et la création de l'Ethernet. On s'est rapidement aperçu que si pour les longues distances la fibre était la solution indiscutable, pour les réseaux locaux (arbitrairement limités à 100 m) la paire torsadée était le média le plus fiable, le plus simple, le moins coûteux et le plus robuste.

Lorsque l'on a commencé à parler de 100 Mbit/s sur paire cuivre (1992) tout le monde a crié au fou. Mais la signature cette année de la norme 10Gbit/s est quasiment passée inaperçue. Plus encore, les travaux ont déjà commencé pour écrire une norme pour le 40 Gbit/s alors que d'autres rêvent du 100 Gbit/s.

Réalité ou fiction ?

Les détracteurs des câbles cuivre agitent le spectre du théorème de Claude Shannon qui est censé donner le débit maximum d'un câble en fonction de son affaiblissement:

La capacité d'un canal de transmission de bande passante H s'exprime de la façon suivante :

C = H log2 (1 + PS/PN) bit/s

où PS/PN représente le rapport signal sur bruit du canal.

Le fait est qu'aujourd'hui l'application de ce théorème démontre la capacité d'un câble « cat7 » à supporter 40 Gbit/s sur 100 m tandis que 100Gbit/s apparait inatteignable.

Aurait-on fait ces calculs il y a quinze ans que l'on aurait trouvé que 10 Gbit/s ne serait jamais atteint. Depuis on a fait des progrès en diminuant le bruit dans les câbles (améliorations de la diaphonie) mais l'affaiblissement est resté quasiment stable. Si demain on trouve comment réduire les pertes diélectriques (primordiales en haute fréquence) de ces câbles alors on atteindra les 100 Gbit/s. Mais cela pourrait aussi se faire en augmentant l'impédance de ces câbles (120 ou 150 ohms au lieu de 100).

Il faut maintenant mettre en perspective les débits réellement demandés.

- Dans l'entreprise aujourd'hui le débit de 100 Mbit/s Ethernet domine, et l'on peut espérer que le Gigabit Ethernet l'aura totalement remplacé dans dix ans ;
- Dans les data center le 10 Gbit/s commence à s'imposer ;
- En câblage résidentiel la tendance est d'arriver dans un réseau FttH avec un débit de 100 Mbit/s dans un délai de 5 ans ;
- Certains parlent déjà du FttH à 1 Gbit/s.

MYTHE N° 2 :
IL N'Y A PAS D'AUTRES SOLUTIONS QUE DE REMPLACER LES CABLES EN CUIVRE PAR DES CABLES OPTIQUES

Pourquoi remplacer les câbles en cuivre par des câbles optiques ?

- Aujourd'hui le câble en cuivre peut non seulement fournir les signaux (le débit) mais aussi l'alimentation électrique nécessaire aux terminaux.
- Aujourd'hui tous les terminaux sont équipés de connecteurs cuivre (RJ45).
- Aujourd'hui on sait installer des câblages cuivre insensibles aux perturbations électromagnétiques.

Le câble optique n'apporte aucun progrès sur des distances de l'ordre de 100m. De plus, il n'existe encore aucun accord sur ce que devrait être un câblage terminal générique en fibre

optique. Les acteurs se déchirent sur le choix de la fibre, le choix des connecteurs, le choix de la longueur d'onde.

Mais si nous ne nous limitons pas au dernier 100m, il faut aussi noter que alors que le DSL a vu le jour au milieu des années 1990 et que nous avons longtemps cru qu'il était limité à quelques Mégabit/s sur des distances inférieures au kilomètre. Des expérimentations récentes ont démontré que le 800 Mbit/s pouvait être atteint sur des distances de 400 m au prix, il est vrai, de l'utilisation de plusieurs circuits en parallèle.

Remplacer les câbles en cuivre par des câbles à fibre optiques sur des distances courtes n'est donc pas la panacée. Il est au contraire coûteux sans que, le plus souvent, le bénéfice attendu soit probant.

MYTHE N° 3 : DEMAIN ON S'AFFRANCHIRA DE TOUS LES CABLES (EN CUIVRE OU EN FIBRE OPTIQUE) QUI EMPECHENT TOUTE REELLE MOBILITE

Le rêve est de se passer tout bonnement de câbles. On entend beaucoup parler des progrès (réels) des transmissions radio. Ces progrès sont dus à des systèmes de codages de plus en plus complexes permettant d'augmenter le nombre d'informations transmises pour une même bande passante.

Tous ces nouveaux systèmes peuvent de toute évidence être injectés sur les câbles existants ce qui permet d'en démultiplier l'efficacité. Pour simplifier, disons que le mode guidé (ou conduit), celui utilisé dans les câbles quels qu'ils soient, est toujours plus efficace que les modes rayonnés (radio, wifi, LTE…).

Ceci induit donc que dans la course au débit, les câbles auront toujours une longueur d'avance même s'ils doivent utiliser des inventions prévues pour la radio. L'exemple du DVB et du DSL devrait donner à réfléchir à tous ceux qui souhaitent enterrer prématurément le cuivre (et non enterrer des câbles en cuivre !).

L'immense avantage du mode guidé, outre qu'il peut se démultiplier à l'infini (lorsque le câble est saturé on en met un autre, alors que, lorsque l'éther est saturé on s'arrête), c'est aussi que les informations transmises sont confinées.

Il est pathétique de voir le combat de la TNT contre la télévision sur IP, lorsque la télévision sur IP offre déjà des milliers de chaines, la TNT en offre dix fois moins en faisant des prouesses.

Un vieux principe admis par tous était que tout ce qui est diffusé (rayonné) peut être capté et décrypté. Aucun système ne garantira jamais la sécurité d'informations radio, comme vous pouvez le lire dans d'autres chapitres de cet ouvrage.

Ce principe n'a jamais encore été infirmé et est une des causes du développement dès les années 1990 des liaisons optiques sous-marines alors que les satellites semblaient apporter la solution à la croissance des communications téléphoniques intercontinentales.

Le meilleur moyen de sécuriser les informations a toujours été et est encore d'en empêcher la divulgation à l'extérieur d'un volume donné. C'est justement ce que fait un câble cuivre ou optique.

Paradoxalement, là encore, le cuivre n'a pas dit son dernier mot. Alors que l'on a appris à « durcir » les câbles cuivre par des écrans empêchant quiconque d'accéder aux informations transitant dans ces câbles sans être immédiatement repéré, les câbles optiques actuels

peuvent être « piratés » par de petits malins qui ayant accès à la fibre peuvent « bricoler » un coupleur dont l'incidence sera le plus souvent indétectable sur le bilan de transmission.

En fait le « sans fil » n'est et ne sera jamais un concurrent pour les liaisons filaires (cuivre ou optique), il en est un complément comme le vélo est un complément à la voiture automobile. La sécurité y est faible, le débit est plus faible, mais il n'est pas cher et pratique à mettre en œuvre.

Enfin un dernier point mérite que l'on s'y arrête, l'aspect santé des utilisateurs.

Alors que les câbles Ethernet sont absolument sans danger, on connait déjà les dangers potentiels des transmissions optiques sur des utilisateurs non avertis et des risques de cécités encourus par ceux-ci. Mais ce n'est rien comparé au débat qui depuis plusieurs années fait rage sur la nocivité présumée de trop de champs électromagnétiques. Il est peu probable que ce débat s'éteigne rapidement alors que la société demande toujours plus de précautions sanitaires.

CONCLUSION

La première conclusion est que nous sommes encore loin aujourd'hui d'avoir besoin de plus de débit qu'un câble cuivre peut fournir sur 100m.

La fibre n'est donc pas le seul médium capable de fournir les débits demandés aujourd'hui.

La seconde conclusion est donc qu'il existe encore des solutions pour accroitre lorsque c'est nécessaire le débit pouvant être supporté par les lignes de transmission en cuivre.

Contrairement aux idées reçues il n'y a aucune raison pour le moment de remplacer un câble cuivre par un câble optique sachant qu'en plus il faudra reconvertir les signaux sur cuivre pour alimenter le terminal.

On ne s'affranchira jamais de tous les câbles (en cuivre ou en fibre optique) même si le sans fil se répandra toujours plus pour des applications spécifiques, à moins que le principe de précaution ne finisse par le tuer.

La troisième conclusion est donc que les liaisons filaires ne seront jamais détrônées par le sans fil en raison de la fiabilité et de la confidentialité des communications qu'elles préservent, et que parmi les liaisons filaires celles en cuivre ne sont pas plus menacées voire moins menacées que les liaisons optiques.

4° PARTIE : ASPECTS NORMES ET STANDARDS

MYTHES ET LEGENDES DE LA CERTIFICATION CRITERES COMMUNS

Gérard Peliks, CASSIDIAN,
an EADS Company

LA CONFIANCE OBJECTIVE EN UNE SOLUTION DE SECURITE

L'Information que vous détenez est sans doute protégée par des solutions de sécurité. Mais ces solutions sur lesquelles réside votre confiance, sont-elles sécurisées ?

Un logiciel de sécurité n'en reste pas moins un logiciel et comme toute œuvre de l'esprit humain, il peut être entaché d'erreurs de programmation, ou d'implémentation, qui sont autant de vulnérabilités ouvertes aux attaques que le logiciel est censé contrer. Il en est de même pour les cartes à puce et pour les logiciels embarqués.

Qu'est ce qui pourrait alors motiver la confiance que vous accordez à un logiciel de sécurité ? Serait-ce parce que votre voisin n'a pas eu de problèmes avec la même solution ? Est-ce la notoriété que le produit rencontre sur le marché ? Seraient-ce les sirènes d'un constructeur qui vous affirme que son produit est le meilleur ? Non, tout ceci n'est que confiance suggérée…

Une confiance objective peut-elle s'établir ? Oui, un certain niveau de confiance objective reste possible si la solution de sécurité a été soumise à des essais normalisés, conduits par un organisme indépendant, étroitement surveillé, et si un organisme officiel reconnu au plan international, quand les tests ont donné un résultat satisfaisant, appose sa signature sur l'attestation de certification. Et bien sûr chaque solution de même type doit passer les mêmes tests. C'est l'un des buts de la norme des Critères Communs[46] (ISO/IEC 15408) conçue à la fin des années 1990 et qui évolue. Mais ces résolutions cachent bien des mythes et légendes, en voici quelques uns.

MYTHE N° 1 : MA SOCIETE EST CERTIFIEE "CRITERES COMMUNS"

Non, la certification Critères Communs ne s'applique en aucun cas à un organisme. Elle ne peut être attachée qu'à une solution de sécurité. Si un produit qui a obtenu cette certification n'est plus commercialisé par le même éditeur, suite par exemple à un rachat de technologie ou suite à un rachat de l'éditeur qui a créé le produit, le produit n'en demeure pas moins certifié Critères Communs pour la version qui a obtenu cette certification.

Le sérieux affirmé par un organisme vis-à-vis de la sécurité, en d'autres termes vis à vis de la gestion de la sécurité de son propre système d'information, peut être certifié par rapport à d'autres normes comme celles de la famille ISO 2700x, en particulier par l'ISO 27001 qui est à la sécurité d'un système d'information, ce que l'ISO 9001 est à la qualité. Pour obtenir la certification ISO 27001, l'organisme doit gravir une pente qui le conduit à plus de sécurité en adoptant le modèle dit "roue de Deming". A chaque tour de la roue de Deming, les étapes

[46] *www.ssi.gouv.fr/site_rubrique71.html et www.commoncriteriaportal.org/*

"Plan, Do, Check, Act" se succèdent et la société mesure l'écart entre ce qui devrait être et ce qui est réellement, pour réduire cet écart. Cette ascension de la roue de Deming qui gravit une pente, conduit l'organisation à obtenir, puis à maintenir, sa certification ISO 27001. Mais cela est une autre facette de la sécurité et ne porte pas sur la certification d'un produit ou d'une solution intégrée de sécurité, donc sur la certification Critères Communs, objet de cet article.

Une société qui propose des services, mais aucun produit, peut être certifiée ISO 27001 et un constructeur ou éditeur de logiciels de sécurité qui n'est pas certifié ISO 27001 peut faire certifier ses produits "Critères Communs". Mais souvent il y a confusion entre ces normes.

La certification Critères Communs peut d'ailleurs s'appliquer également à des solutions comme des IPBX (autocommutateurs téléphoniques sur protocole IP) ou à des systèmes d'exploitation pour contrôler et affirmer dans le détail la robustesse c'est à dire l'exactitude des annonces de sécurité, et répondre à des questions comme : les protections sont-elles efficaces face aux menaces ?

MYTHE N° 2 :
LA CERTIFICATION CRITERES COMMUNS PORTE SUR L'ENSEMBLE D'UN PRODUIT

C'est un mythe de croire qu'un pare-feu (firewall), par exemple, certifié Critères Communs l'est sur l'ensemble de ses fonctionnalités, quelle que soit sa version et ses conditions d'emploi. La certification Critères Communs porte sur une version précise d'un produit, qui tourne sur une version précise d'un système d'exploitation ; le tout dans un environnement qui doit respecter un certain nombre d'hypothèses spécifiées dans le document « Cible de Sécurité ». Quand le pare-feu, ou autre logiciel, est proposé déjà intégré sur un calculateur (une Appliance), la certification porte seulement sur certains des modèles de cet Appliance. Et quand l'Appliance comporte un pare-feu, un antivirus et un antispam, ni l'antivirus, ni l'antispam ne sont, le plus souvent, couverts par la cible de sécurité.

Tout ceci est écrit sur l'attestation remise avec la certification, encore faut-il la lire attentivement. Il ne serait pas très honnête, par exemple, pour un éditeur, d'affirmer "mon Appliance de sécurité a obtenu la certification Critères Communs au niveau EAL3+ (en insistant toujours sur le "+" !) alors que cette certification a été obtenue sur une version déjà ancienne de cette Appliance et qui n'est plus commercialisée, et peut-être sur un autre système d'exploitation que celui proposé à la vente. La sécurité du produit n'a pas forcément régressé depuis l'obtention de sa version certifiée, mais rien ne le prouve. Un programme de maintenance de la certification de la solution existe, qui établit la non régression de la sécurité du produit sur la surface testée (la cible de sécurité) à chaque nouvelle version, ou après chaque action de maintenance majeure; mais l'éditeur a-t-il souscrit à ce programme ?

MYTHE N° 3 :
DEUX PRODUITS DE MEME TYPE, CERTIFIES CRITERES COMMUNS, SONT COMPARABLES

Il est certain que l'un des buts principaux des Critères Communs a été de permettre la comparaison, côté sécurité, entre des produits de même type, par exemple des pare-feux, des réseaux virtuels chiffrés (VPN) ou des produits de chiffrement sur disque. Les certifications précédentes, comme l'Orange Book aux USA ou les ITSEC en Europe n'avaient pas intégré cette possibilité, et c'est en quoi les Critères Communs se démarquent principalement des autres certifications de produits. Mais affirmer que deux produits de même type, certifiés Critères Communs à un même niveau, par exemple deux pare-feux certifiés Critères

Communs EAL3+, sont comparables, peut être un mythe si on ne sait pas exactement ce que la certification recouvre pour chacun d'eux.

Une certification porte sur une certaine surface de fonctionnalités du produit, et sur certaines menaces que le produit doit contrôler. Tout ceci est consigné dans un document appelé la "cible de sécurité" (ST : Security Target). Deux outils de chiffrement sur disque certifiés EAL4+, chacun sur des cibles de sécurité différentes, ne sont assurément pas comparables. Avant de commencer une démarche de tests, le commanditaire doit faire accepter la cible de sécurité par l'organisme officiel qui signera le certificat. En France, l'ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Information) est cet organisme. L'ANSSI, qui est rattachée au Premier Ministre, engage son sérieux par sa signature, et la confiance que porte un utilisateur dans un produit certifié dépend bien sûr de la confiance qu'inspire l'ANSSI

De plus, pour éviter que le commanditaire de la certification n'opère un savant découpage en dentelles de la cible de sécurité afin de n'y inclure que les fonctionnalités qu'il juge devoir réussir les tests sans problème, il a été introduit la notion de "Profil de Protection" (PP). Si des profils de protection existent, l'ANSSI peut exiger que le périmètre proposé à la certification respecte les exigences spécifiées dans ces documents. Ainsi deux produits de même type, peuvent présenter une cible minimale commune, mais bien sûr un constructeur peut faire certifier une cible plus étendue que celle constituée par l'ensemble des profils de protection exigés, afin de se démarquer de ses concurrents. Les produits ne sont alors plus comparables.

MYTHE N° 4 :
DANS EALX+, LE "+" EST LE PRINCIPAL FACTEUR DE QUALITE

Le niveau d'assurance (aussi communément appelé "niveau d'évaluation" ou "niveau de certification") définit la liste des contrôles qui doivent être réalisés sur le produit et son environnement de développement. Choisir un niveau d'évaluation, par exemple le niveau EAL4 (Evaluation Assurance Level de niveau 4) signifie sélectionner un paquet standard de contrôles tel que définit dans les Critères Communs. Les Critères Communs définissent 7 paquets de EAL1 à EAL7 comportant un nombre croissant de contrôles à réaliser. Mais les Critères Communs offrent aussi la possibilité aux commanditaires des évaluations de demander des contrôles supplémentaires, par exemple qui seraient requis pour des paquets EAL supérieurs. Cet ajout est nommé une "augmentation" du paquet standard EAL. Si la terminologie officielle impose de détailler dans le certificat la liste des augmentations, les fournisseurs de produits se contentent souvent d'un "+".

Ce que recouvre le "+" est parfois négligeable par rapport à ce que recouvre le paquet imposé par le niveau de certification choisi. Hors souvent l'acheteur est plus impressionné par le "+" que par le niveau de certification et ainsi se constitue le mythe du +, qui n'est pas le vrai différentiateur de qualité d'une certification Critères Communs. Mais le "+" peut tout de même recouvrir des éléments significatifs, comme les tâches d'assurance liées à la correction des défauts, ce qui intéresse directement l'acheteur.

MYTHE N° 5 :
UN CERTIFICAT CRITERES COMMUNS A UNE DATE DE PEREMPTION

Oui et Non. Comme nous l'avons indiqué auparavant, un certificat ne s'applique qu'à une version précise d'un produit. Il atteste qu'à la date de signature du certificat, le produit a passé avec succès tous les tests spécifiés dans sa cible de sécurité. Dans l'absolu, cette

attestation n'a pas de raison d'être invalidée. En revanche, une personne qui souhaiterait utiliser ce certificat doit se poser la question suivante : vu les évolutions des techniques d'attaque depuis la signature de ce certificat, le produit ne risque-t-il pas aujourd'hui ou demain de ne plus passer la certification ? La ligne Maginot aurait sans doute obtenu la certification Critères Communs … avant 1940.

L'ANSSI propose un programme de « Surveillance » qui revient à mettre à jour régulièrement les résultats des tests. Si cette surveillance est bien adaptée à des produits matériels qui n'évoluent pas, elle l'est moins pour des logiciels en constante évolution. En effet, il faudrait alors se poser la question : si la version précédente du produit a passé avec succès l'évaluation il y a quelques mois, qu'en est-il de la nouvelle version aujourd'hui ?

Pour répondre à cette question, l'ANSSI propose deux solutions :

- fournir un rapport de maintenance qui, sur la base d'une analyse d'impact réalisée par le développeur, estime un niveau de "certificabilité" de la nouvelle version,
- faire réaliser par un CESTI une réévaluation de la nouvelle version du produit avec réutilisation au maximum des travaux déjà réalisés sur la version antérieure.

MYTHE N° 6 :
UNE CERTIFICATION CRITERES COMMUNS OBTENUE DANS UN DES PAYS CERTIFICATEURS EST AUTOMATIQUEMENT RECONNUE DANS TOUS LES PAYS

Les pays qui possèdent des centres de tests des produits et aussi des organismes officiels qui délivrent et maintiennent les certificats obtenus sont en nombre très limité. Seuls ces pays peuvent être des centres de certification. Un commanditaire qui veut faire certifier une solution de sécurité doit écrire la cible de sécurité sur laquelle portera la certification et la faire accepter par l'organisme officiel d'un des pays certificateurs, même s'il n'y réside pas. Les tests ayant donné un résultat satisfaisant, l'organisme officiel signera le certificat. La certification obtenue dans un des pays certificateurs est reconnue, en théorie, dans tous les pays. Mais cela n'est vrai que jusqu'au niveau de certification EAL4. Au-delà, cela peut être un mythe. A partir du niveau de certification EAL5, une certification obtenue dans un des pays de la Communauté Européenne n'est reconnue que dans certains des pays de cette Communauté, et seulement aujourd'hui pour les "microcontrôleurs sécurisés et produits similaires". Cette certification Critères Communs au-delà du niveau EAL4 ne sera pas reconnue, aujourd'hui, par les USA. De même, une certification à partir du niveau EAL5 obtenue aux USA n'est pas reconnue dans les pays de la Communauté Européenne. Tout est question d'accords mutuels entre les organismes d'état de chacun des pays (CCRA, SOG-IS) et ces accords évoluent avec le temps.

MYTHE N° 7 :
UN NIVEAU DE CERTIFICATION EVALUE LES FONCTIONNALITES DE SECURITE D'UN PRODUIT

C'est ce qu'on pense généralement mais c'est une idée fausse. Le niveau EALx (Evaluation Assurance Level niveau "x") indique non pas l'étendue des fonctionnalités de sécurité soumises aux tests – c'est la cible de sécurité (ST) qui l'indique - mais la liste des contrôles qui doivent être réalisés sur ces fonctionnalités.

La documentation Critères Communs est constituée de trois volumes. Le deuxième volume est un catalogue de composants fonctionnels qui doivent être utilisés pour spécifier, dans le document Cible de Sécurité, les fonctionnalités de sécurité à évaluer. Une fois la cible de

sécurité acceptée par l'organisme officiel (l'ANSSI en France), le niveau de certification sélectionné va définir la manière dont vont se dérouler les tests sur les fonctionnalités de la cible. Cette manière est définie par les composants d'assurance décrits dans le volume 3 des Critères Communs.

Ce niveau peut représenter une évaluation en boîte noire (EAL1) qui consiste à vérifier que le produit se comporte comme l'indique sa Cible de sécurité et sa documentation, ou en boîte blanche, à partir du niveau EAL2 où on commence à regarder comment le produit est conçu. La fourniture d'une partie des sources peut être exigée à partir du niveau EAL4.

A partir du niveau EAL5, les Critères Communs demandent à l'évaluateur de vérifier si le développeur a utilisé des méthodes semi-formelles ou formelles lors de la conception du produit pour la politique de sécurité (EAL5), pour la conception détaillée EAL6), pour la vérification du code (EAL7).

MYTHE N° 8 : UNE SOLUTION DE SECURITE DOIT ETRE CERTIFIEE CRITERES COMMUNS POUR ENTRER DANS LE CATALOGUE DE L'ADMINISTRATION FRANÇAISE

Comme la démarche pour obtenir une certification Critères Communs dure plusieurs mois et coûte cher, y compris par les ressources internes du commanditaire qu'elle mobilise, peu de PME peuvent se permettre de réunir ce budget.

Pour permettre à tous de faire certifier un produit de sécurité, et même pour que les logiciels libres puissent obtenir une certification, l'ANSSI a conçu une certification plus légère : la CSPN (Certification de Sécurité de Premier Niveau). En 25 jours de travaux (coûts limités), 35 jours si le produit comporte des mécanismes cryptographiques, une organisation peut faire évaluer son produit pour obtenir la certification CSPN. Bien entendu, la solution de sécurité peut ne pas obtenir cette évaluation à l'issue des 25 ou 35 jours mais les coûts sont limités et connus d'avance.

Pour entrer dans le catalogue des solutions de sécurité des administrations française, le produit certifié doit être également qualifié. La qualification implique une vérification par l'ANSSI que la cible de sécurité est conforme à des profils d'exigences et correspond aux besoins des administrations. Trois niveaux de qualifications sont définis : élémentaire, standard, et renforcé. La qualification élémentaire implique une certification CSPN, les deux autres une certification Critères Communs. Il est donc faux d'affirmer qu'une solution de sécurité qui n'a pas la certification Critères Communs ne peut être vendue aux administrations. Un logiciel libre peut ainsi trouver un commanditaire dans son club d'utilisateurs pour être évalué CSPN et entrer dans le catalogue des solutions de sécurité des administrations. TrueCrypt par exemple est certifié CSPN. Attention, la certification CSPN qui est purement française n'est reconnue qu'en France.

MYTHE N° 9 : EN FRANCE, C'EST L'ANSSI QUI CONDUIT LES TESTS D'EVALUATION

Non, l'ANSSI n'intervient que dans la supervision le contrôle de la conformité des actions d'évaluations de sécurité effectuées par des laboratoires, et l'analyse du rapport d'évaluation, donnant ou non lieu à la délivrance du certificat Critères Communs ou CSPN. L'ANSSI publie les résultats sur son site Web.

Les tests d'évaluation sont menés par une société d'experts qui réalise les tests sur la base du document cible de sécurité écrit par le commanditaire et qui constitue son cahier des charges.

Ces sociétés d'experts s'appellent des CESTI (Centre d'Évaluation de la Sécurité des Technologies de l'Information). Il existe en France deux CESTI habilités à mener les tests d'évaluation Critères Communs pour les logiciels et trois CESTI habilités à mener des tests pour les logiciels embarqués et les cartes à puces. Le CESTI est l'interface obligée entre le commanditaire et l'ANSSI qui signe le certificat au vue des rapports techniques délivrés par le CESTI. Toutefois, si la solution de sécurité comporte des mécanismes cryptographiques, l'ANSSI peut mener des analyses complémentaires sur ces mécanismes.

5° PARTIE : ASPECTS JURIDIQUES

MYTHES DE L'IMPUNITE JURIDIQUE, DE L'ARGENT FACILE ET DE LA SURVEILLANCE TOTALE

Christian Aghroum
Ancien chef de l'OCLCTIC
Directeur de la sécurité d'un groupe international suisse

Mais que fait la police ? On a souvent l'impression que le policier et le gendarme sont seulement là pour nous verbaliser au bord des routes ... rassurez vous, ils veillent aussi sur les autoroutes de l'information ...

MYTHE N° 1 : INTERNET PERMET AUX DELINQUANTS D'ECHAPPER AUX POURSUITES.

Faux, il n'est pas nécessaire de connaître à priori l'auteur ou le suspect des faits commis. Rien n'interdit d'ouvrir une enquête contre personne inconnue, contre X... dit-on, dès lors que l'auteur des faits est inconnu. Il faut cependant reconnaître que la cybercriminalité profite de tous les atouts accordés à la criminalité moderne : un caractère organisé, transfrontalier, complété par l'utilisation de technologies toujours nouvelles, dont n'auraient pu bénéficier que les services secrets il y a à peine deux décennies. La cryptologie, la miniaturisation ne serait-ce que des caméras et appareils photos, des microphones, la simplification des outils de transmission sont autant d'élément de progrès dont les criminels ont rapidement su tirer profit. Enfin, la capacité à disséminer rapidement une information sur la planète entière permet au criminel de tout poil d'élargir considérablement le panel de ses victimes possibles. On pêche avec un immense filet aux mailles très serrées ...

La collaboration entre services de police et autorités judiciaires progresse aussi en matière de lutte contre la cybercriminalité, tout particulièrement grâce à un texte fondateur, la convention de Budapest du 23 novembre 2001.

Alors bien sûr, dans le lot, échappent quelques délinquants, aidés par l'hébergement de leurs activités dans des pays corrompus aux législations défaillantes voire inexistantes. Il n'en reste pas moins vrai que les progrès techniques profitent aussi à la justice. Les services de police se spécialisent et se dotent d'outils performants, la justice se forme et s'adapte. Les cyberpatrouilleurs veillent dorénavant.

L'action pénale ne peut être efficace par contre qu'avec l'aide de la victime qui prendra soin de déposer plainte et de fournir très rapidement et sans hésitation tous les éléments en sa possession. Cela permettra des constatations exhaustives et une meilleure connaissance de l'environnement victimiologique, seules garanties d'une enquête ancrée sur de bonnes bases.

MYTHE N° 2 : LA POLICE ET LA JUSTICE ONT TOUJOURS UN TEMPS DE RETARD.

Voilà une approche bien rapide et faisant fi de la réalité pragmatique du terrain. Le temps de la justice ne peut pas être celui de l'infraction si l'on veut que la justice demeure objective et impartiale. Police et justice sont ancrées dans le temps de l'action, déclenchée avant tout par leur information. Si nul ne se plaint, si aucune information ne filtre, il ne peut y avoir

d'action pénale. Combien d'entreprises refusent de déposer plainte de peur d'une perte d'image, combien de particuliers ont honte d'avoir été si naïfs à postériori ...

Il faut cependant admettre que les approches traditionnelles volent en éclat face à la cybercriminalité : souveraineté nationale, espace frontalier, asymétrie des législations sont autant de frein à une action efficace. Cela n'empêche pas, à force de pugnacité, d'obtenir des succès réguliers grâce à une coopération policière et judiciaire forte et voulue par tous, dès lors que les intérêts individuels ne supplantent pas l'intérêt public.

Enfin, l'apport des services de renseignement en amont de la commission de l'infraction doit demeurer discret, leur permettre d'être efficaces ; il n'en est pas moins indispensable.

MYTHE N° 3 :
EN FRANCE, POLICE ET JUSTICE N'ONT PAS LES COMPETENCES NECESSAIRES.

Encore un lieu commun sans fondement. Depuis la fin des années 80, des unités de police et de gendarmerie se sont progressivement spécialisées, pour permettre à l'heure actuelle la présence sur l'ensemble du territoire national de spécialistes dits "NTECH" pour la gendarmerie nationale (enquêteurs spécialisés en nouvelles technologies) et "ICC" (investigateurs en cyber criminalité) pour la police nationale, nonobstant les cyber correspondants des deux forces placés au plus près des besoins dans les brigades de gendarmerie et commissariat de police. Les douanes concourent à la cyber protection de la France dans la lutte contre les contrefaçons et produits illégalement importés.

La justice forme dès l'Ecole Nationale de la Magistrature ses magistrats et complète leur mise à niveau par des formations spécialisées.

La CNIL participe au dispositif en encadrant les activités de tous et limitant les abus vite tentants en la matière.

La France est enfin dotée d'un arsenal juridique à jour et régulièrement actualisé (la LOPPSI II devrait apporter une dernière touche d'actualité). Cette ossature juridique existe depuis ... 1978 et la loi "informatique et libertés" plaçant la France dans le peloton de tête des précurseurs en matière de lutte contre la cybercriminalité et de protection de ses concitoyens.

MYTHE N° 4 :
L'ARGENT EST FACILE A GAGNER SUR INTERNET.

Quel argent ?

L'argent propre : comme toute activité humaine, le créatif, innovateur, consciencieux, et travailleur peut gagner sa vie au prix des efforts qu'il mettra à la bonne avancée de son entreprise. Encore que sans idée novatrice, sans un entourage compétent, sans l'appui d'un banquier, il est dur d'imaginer que l'argent puisse miraculeusement couler par le biais de connexions diverses vers un compte bancaire en ligne.

L'argent sale : lui pourra plus facilement alimenter les caisses de votre organisation dès lors que sans scrupules vous envisagez de voler, infiltrer, escroquer, trahir la confiance de votre prochain. Bienvenue dans le monde des criminels peuplé de trahisons, de dénonciations, de surveillances par les services de police, d'années de prison, de saisie complète de vos biens considérés à juste titre comme des avoirs criminels. Au résultat, loin des clichés cyberromantiques véhiculant de modernes Robin des Bois, de richissimes magnats enrichis rapidement par quelques magouilles sans risques physiques sortes de Spaggiari à la mode cyber, vieillissent le lot des criminels usés par les années de prison, désociabilisés et bannis.

MYTHE N° 5 :
BLANCHIR ET CACHER SON ARGENT EST A LA PORTEE DE TOUS SUR INTERNET.

Ce n'est déjà pas à la portée de tous les délinquants, il est dur d'imaginer que cela puisse être à la portée des honnêtes gens ... qui de toutes façons deviendraient alors délinquants ... Des affaires récentes ont également démontré que la fragilité de certains systèmes d'information conduit aussi les pays réputés pour leur discrétion bancaire à revoir leur position et permet aux services de l'Etat de récupérer quelques listes de citoyens indélicats envers leur système fiscal, au moins ...

MYTHE N° 6 :
INTERNET EST ENTIEREMENT SOUS LA SURVEILLANCE DES ETATS UNIS ET DE LA PLUPART DES PAYS.

Bien sûr qu'il est possible de surveiller internet, comme il l'est des communications en général. Cependant, la surveillance exercée par les services de renseignement ou par les services judiciaires ne saurait être exhaustive. Au delà des contraintes légales, de la déontologie et de l'éthique des forces en charge de son exercice, cette surveillance totale ne peut de toute façon l'être, faute de temps et de moyens tout simplement. On est encore loin de "Big Brother" fort heureusement. La surveillance s'exerce en destination de cibles préalablement repérées grâce à toutes les méthodes existantes dont les plus traditionnelles sont les plus efficaces. La source, l'informateur, l'aviseur, ou quelque soit le terme par lequel on le désigne, sera toujours le meilleur point de départ d'une enquête dès lors recoupée par des surveillances physiques et techniques.

Le contrôle d'accès à internet est par contre opéré dans de nombreux pays dont la proximité à la démocratie est aussi lointain que l'âge de pierre l'est au cyber espace. Ce filtrage est la forme moderne de la censure par ailleurs exercée sur tous les médias au sein de ces dictatures déclarées ou non.

"Big brother is watching you !". Laissons ce cauchemar à Orwell mais gardons cet avertissement à l'oreille ; qu'il nous permette de nous prémunir de toute dérive vers laquelle nous conduirait une technique totalement débridée.

MYTHE N° 7 :
ON PEUT TOUT DIRE ET TOUT FAIRE SUR INTERNET, C'EST UN TOTAL ESPACE DE LIBERTE.

Internet n'appartient plus aux seuls internautes, Internet est devenu un espace public ! Dès lors, il doit être soumis aux mêmes règles que tout espace de communication. La loi encadre pour le bien de tous l'expression publique : on peut penser ce que l'on veut, s'exprimer tant que l'on veut, dès lors que l'on respecte son prochain. Ainsi, l'injure, la diffamation, la propagation de fausses nouvelles, l'incitation à la haine raciale, l'excitation à la débauche sont autant de formes d'expressions déviantes, insupportables aux règles d'une vie courtoise et paisible en société et ne permettent ni à la tolérance et ni au respect de l'autre de s'exprimer. Il en est de même pour internet, les mêmes infractions sont tout aussi détestables, détectables et poursuivables.

Une étape mériterait d'être franchie, celle de la création d'un droit international d'Internet au même titre qu'il existe un droit de l'espace aérien ou de l'espace maritime. Nul doute qu'il simplifierait la circulation, l'installation et l'expression de tous. A condition de trouver outre

l'ICANN et la convention de Budapest un nouveau leader et un outil légal plus universel encore ... auprès de l'O.N.U. peut-être ?

MYTHE N° 8 :
IL N'Y A QUE LES NAÏFS QUI SE FONT AVOIR SUR INTERNET.

Faux ... si le caractère naïf des victimes de phishing ou d'escroquerie à la nigériane est souvent mis en avant, c'est mal connaître la malignité des cyberdélinquants et leurs capacités à mettre en place des dispositifs d'ingénierie sociale de plus en plus ingénieux. Même les plus attentifs peuvent si faire prendre par négligence, fatigue ou du fait d'une trop grande confiance dans des dispositifs techniques qui même mis à jour à temps sont parfois détournés par une technique nouvelle. Enfin, chacun a ses petites faiblesses, ses penchants, ses passions qui le conduiront à répondre trop rapidement à un mail alléchant, une publicité plus vraie que nature, un appel à la charité bien ciblé ; une seule parade : faire preuve de bon sens, prendre le temps nécessaire à la réflexion et à l'interrogation, les sites d'aide et de prévention sont à cet égard suffisamment nombreux.

MYTHE N° 9 :
SIGNALER LES FAITS NE SERT A RIEN.

Bien sûr que si, signaler des faits apparemment illégaux relevés sur internet procède du civisme et de l'esprit d'entraide de son prochain. Il ne s'agit en rien de délation ! Si je suis témoin d'un accident de la route et que le chauffard s'enfuit en laissant une victime agonisante sur le bord de la chaussée, je préviens police et services de secours. De la même manière, si je détecte incidemment un site pédopornographe ou d'escroqueries sur internet, je le signale auprès du service créé à cet effet sur le site www.internet-signalement.fr, même anonymement. L'information sera vérifiée, qualifiée pénalement et adressée en France ou à l'étranger vers le service de police, de douanes, de répression des fraudes compétent. En quelques clics de souris, j'aurais aidé à protéger les enfants de mes voisins ou épargner à quelqu'un de se faire arnaquer par un escroc sans scrupules ...

De même est-il vain de croire que de petites infractions, pour lesquelles on a déposé plainte et qui ne sont pas poursuivies, demeurent lettres mortes. C'est à travers le recoupement de ces informations que les services de police décèlent des organisations criminelles transnationales et activent leurs homologues étrangers. Une victime à 100 euros ne motivera pas un service à l'étranger, 10 000 victimes des mêmes faits permettront de déclencher une opération internationale. Alors consolons nous, si malheureusement notre cas n'est pas résolu, la plainte ou le signalement du fait permettra certainement d'en prévenir de nombreux autres.

MYTHE N° 10 :
LE PARTENARIAT PUBLIC PRIVE EST UN SERPENT DE MER.

Le PPP est bien souvent cité, rarement décrit, ce qui laisse penser à la Belle Arlésienne. Pourtant, dans le cadre de la lutte contre la cybercriminalité, le partenariat public privé est une réalité quotidienne. L'enquête de police est de plus en plus une enquête de traçabilité dans laquelle sur la base de constatations, les services cherchent des traces physiques, biologiques, techniques et technologiques. La plupart de ces traces numériques sont détenues par d'autres que l'Etat : banques, fournisseurs d'accès, opérateurs de téléphonie, fournisseurs d'accès ... Les services de l'Etat en quête de vérité sont dépendants de partenaires privés qu'il

faut alors requérir selon les formes légales. Il devient donc incontournables pour les uns et les autres de mieux se connaître : comment rechercher ce qu'on ne connaît pas, comment répondre avec pertinence et célérité à un interlocuteur inconnu ou envers lequel on a de la défiance, comment conjuguer impératifs de service public, continuité, horaires et contraintes financières, reports de charges et impératifs légaux de stockage de l'information ... Toutes ces questions trouvent réponse dans une connaissance mutuelle basée sur la découverte et la confiance mutuelle encadrée.

Le guide des bonnes pratiques voté et publié par le Conseil de l'Europe[47] suivi de celui de la Commission Européenne[48] sont des avancées juridiques considérables. Signal-Spam est une organisation publique-privée, dont la compétence et l'efficacité dans la lutte contre le spam ne sont plus à démontrer.

Un regret : l'absence d'un véritable dispositif interministériel calqué sur la mission interministérielle de lutte contre la drogue et la toxicomanie qui permettrait d'organiser de manière cohérente la synthèse des actions des différentes entités publiques et privées dans un effort commun et concerté. Ce rôle n'est pas celui de l'ANSSI ne celui de la CNIL et n'a pu être tenu par le forum des droits de l'internet. La MILC, mission interministérielle de lutte contre la cybercriminalité, dotée d'un budget et d'une autorité réglementaire, répondant directement au Premier Ministre, pourrait efficacement fonctionner sous la présidence d'un Monsieur ou d'une Madame "Cyber" charismatique et reconnu(e).

[47] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/Reports-Presentations/567%20prov-d-%20guidelines%20provisional2%20_3%20April%202008_FRENCHrev.pdf

[48] http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/fr/jha/103548.pdf

MYTHES ET LEGENDES DE L'INFORENSIQUE

Daniel Guinier, Expert judiciaire en cybercriminalité

L'inforensique *fait partie intégrante du processus global d'investigation. Il s'agit d'une méthode de préservation de l'intégrité et d'analyse des supports de données pour identifier et extraire des éléments utiles, avec pour but essentiel l'établissement de la preuve.*

MYTHE N° 1 :
LE CHAMP DE L'INFORENSIQUE EST LIMITE AUX INVESTIGATIONS INFORMATIQUES :

D'abord réservé à l'informatique judiciaire, *-ou informatique légale par analogie à la médecine légale ("forensics")-*, le terme *"inforensique"* englobe l'ensemble des technologies de l'information numérique sous l'anglicisme *"Digital forensics"*, où les investigations afférentes traitent maintenant non seulement de l'informatique, sous le nom de *"Computer forensics"*, mais aussi des supports digitaux voisins, des réseaux et télécoms. Une autre spécialité relève des téléphones mobiles, sous la dénomination de *"Phone forensics"*.

Les supports informatiques sont les ordinateurs de tous types, les assistants personnels ou PDA *pour* **Personal Digital Assistant**, les disques de tous types : *magnétiques, SSD pour Solid-State Drive, optoélectroniques*, disquettes, bandes et cassettes magnétiques, mémoires flash : *carte ou clé USB,* mémoire vive RAM pour un examen à chaud seulement, sinon par le recours à la cryogénie! Déjà, les disques durs ne sont donc pas les seuls supports à examiner. **Les supports voisins** sont les appareils de prises de vue numérique : *photographiques et vidéo,* les *"boxes TV",* consoles de jeux, baladeurs, lecteurs-enregistreurs et supports CD et DVD etc., les dispositifs d'encodage et de lecture et les cartes d'accès, d'identification et de paiement, les téléphones cellulaires et les cartes SIM et USIM, les terminaux GPS, etc.

Le domaine inforensique résultant est indispensable à la preuve, notamment en matière pénale. Il s'inscrit comme une véritable spécialité au tableau criminalistique, de façon à être plus proche des besoins, d'une part, pour la lutte contre la cybercriminalité ou les crimes et délits classiques facilités par les TIC et, d'autre part, pour la découverte d'indices et d'éléments probants dans des affaires correctionnelles et criminelles, en complément des autres moyens d'enquête. Ces éléments peuvent se trouver dissimulés, y compris dans des lieux insolites : *réfrigérateur, porte-monnaie, etc., et même entre les dents d'une personne, concernant une carte mémoire micro SD, dont le contenu s'est avéré irrécupérable!*

Ainsi, l'inforensique ne se limite pas aux investigations sur des supports informatiques, mais intéresse l'ensemble des supports électroniques, en menant des investigations étendues à tous les moyens et supports informatiques et voisins.

MYTHE N° 2 :
L'INFORENSIQUE EST LE DOMAINE RESERVE AUX ENQUETEURS SPECIALISES :

Sur le territoire national des enquêteurs de la police et de la gendarmerie sont spécialisés avec des compétences techniques dans le domaine de l'inforensique. La formation de ces derniers constitue une priorité du ministère de l'Intérieur qui abrite les deux grandes directions que sont la DGPN et la DGGN. Au niveau central, les uns appartiennent à l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication

(OCLCTIC), ils sont épaulés par la Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information (BEFTI) dont la compétence territoriale est limitée à Paris et sa petite couronne. A son tour, la Direction Centrale du Renseignement Intérieur *(DCRI)*, dispose d'un domaine de compétence qui concerne plus généralement la sécurité intérieure. Les autres appartiennent à la gendarmerie nationale et sont rattachés à l'Institut de Recherches Criminelles de la Gendarmerie Nationale *(IRCGN)*, ou à une division du service technique de recherches judiciaires et de documentation *(STRJD)*. En plus de ces centres de compétences, des enquêteurs spécialisés en criminalité informatique *(ICC ou NTECH)*, sont disséminés au sein de bon nombre de services sur l'ensemble du territoire.

Les enquêteurs spécialisés et les spécialistes en inforensique de la police nationale ou de la gendarmerie font partie de la **chaîne d'enquête** pour intervenir au cours d'enquêtes judiciaires, où ils agissent sur les instructions du parquet ou d'un juge d'instruction. Ces derniers puisent aussi dans le savoir-faire de l'IRCGN et de l'OCLCTIC et les spécificités propres à certains laboratoires de l'Institut National de Police Scientifique *(INPS)*. Une fois les objets saisis mis sous scellés, ceux-ci seront alors analysés **dans le cadre d'une expertise**.

Certains experts judiciaires disposent de compétences techniques et de savoir-faire **dans le domaine de l'inforensique**, où ils agissent sur réquisition d'un OPJ ou d'un ODJ, en cours d'enquête de flagrance *(Art. 60 du CPP)* ou préliminaire *(Art. 77-1 du CPP)*, ou sur ordonnance d'un juge d'instruction *(Arts.156 et suivants du CPP)* dans le cadre d'une procédure pénale, correctionnelle ou criminelle. Leur statut relève de la loi n° 2004-130 du 11 février 2004 et du décret n° 2004-1463 du 23 décembre 2004. La désignation de l'expert se réfère à une liste établie chaque année par une Cour d'Appel ou par la Cour de Cassation, ou à sa réputation s'il est non inscrit : *honoraire ou spécialiste reconnu*. Le juge d'instruction peut également faire appel à un des organismes cités ou à un spécialiste de la police ou de la gendarmerie nationale de la **chaîne criminalistique**.

Les opérations d'expertise inforensique débutent par la remise des scellés jusqu'au dépôt du rapport qui fait suite aux investigations, conformément à la mission donnée à l'expert. Celle-ci sera centrée sur les qualifications dont il faudra apporter la preuve, et orientée sur des points découlant des interrogatoires, de l'environnement de faits similaires, ou vus préalablement, en laissant une possibilité d'ouverture en faisant *"…toutes constatations et remarques techniques utiles à la manifestation de la vérité"*. Lors d'un procès l'expert appelé devra répondre à une citation à comparaître *(Arts. 437, 438 du CPP)* remise par huissier de justice. Il procèdera à sa déposition et répondra au questionnement du Tribunal, en tant qu'expert-témoin, après avoir prêté serment.

Les expertises inforensiques sont diverses en termes de qualifications : pédopornographie et cyber-pédophilie, vols, fraudes, escroqueries, détournements, piratage, diffamation, atteintes à la vie privée, menaces de mort, appels à la haine et au racisme, faux documents administratifs, fausse monnaie, trafics : *êtres humains, stupéfiants, armes, véhicules, etc.*, concurrence déloyale, intrusions, vols de données, contrefaçons et diffusion par l'Internet de produits contrefaits, blanchiment, financement du terrorisme, vols avec violences, attaques de banques en bande organisée, et très utiles dans des affaires de viols sur mineurs, notamment moins de 15 ans, y compris sous drogue ou avec violence, meurtres et homicides, etc.

L'inforensique n'est donc pas le domaine réservé aux enquêteurs spécialisés, les experts judiciaires interviennent diversement, notamment en complément et en aval de ces derniers.

MYTHE N° 3 :
LES MESURES ANTI-INFORENSIQUES SONT EFFICACES POUR FAIRE DISPARAITRE LES PREUVES :

Le régime probatoire français est fonction du droit auquel il se réclame : *droit du travail, civil, commercial, administratif ou pénal.* Dans ce dernier cas, la preuve est libre et sans hiérarchie et **le juge a un rôle actif dans la recherche de la preuve**, et par conséquent les délinquants ou criminels mettront tout en œuvre pour dissimuler au mieux les traces d'actes illicites par des mesures anti-inforensiques.

Les mesures antérieures aux actes illicites concernent la recherche d'informations, d'outils et de sites d'anonymisation, pour réaliser des intrusions, déposer des logiciels malveillants et procéder à des téléchargements et des vols de données, *par ex.* **Les mesures postérieures** seront de plusieurs types. Il s'agira de l'effacement des enregistrements et de traces diverses *(Formatage, suppression de partition, usage d'un utilitaire (ex. CCleaner), etc.),* du camouflage de partitions ou d'enregistrements, de la banalisation de la dénomination de dossiers, de fichiers, pour leur donner une extension ou une apparence neutre *(ex. sys, txt, au lieu de jpg)*, les cacher ou les encapsuler dans d'autres d'apparence ordinaire *(ex. images pédophiles dans des fichiers Word)*, masquer leur contenu par un dispositif stéganographique, ou le crypter pour le rendre inintelligible. Il s'agira aussi de fausser l'horodatage ou le rendre incohérent pour la preuve, et plus rarement, d'indiquer des répertoires classifiés de défense pour tenter de qualifier leur contenu *"intouchable"* en l'état, etc.

Il existe des réponses inforensiques aux problèmes posés par ces mesures anti-inforensiques visant à détruire, camoufler, modifier des traces et en prévenir la création. Tout d'abord, il est possible de retrouver des partitions cachées ou supprimées *(ex. avec TestDisk ou autre outil inforensique)* et de récupérer la table des partitions et le secteur de *"boot"* des systèmes de fichiers *(ex. FAT3, NTFS)*, ainsi que les répertoires et les fichiers supprimés. Par ailleurs, il est aisé de reconnaître les fichiers non pas par leur extension mais par leurs entêtes *"header"* et *"footer"* et une méthode de *"carving"* permettra de retrouver des fichiers *(ex. images)* encapsulés dans d'autres. Sans traces particulières de logs, avec les systèmes usuels, les horodatages faussés pourront parfois être détectés par une incohérence, et quelquefois retrouvés, par analogie avec des fichiers jumeaux disposant de métadonnées non altérées. Des informations pourront être extraites de zones non allouées, et d'autres relâchées en fin de fichier.

La détection de l'usage de la stéganographie et l'extraction est délicate mais reste possible. Enfin, les fichiers cryptés avec un algorithme fort *(ex. AES)*, une clé de taille et d'entropie suffisantes resteront difficiles à décrypter, sans disposer d'éléments dans la mémoire RAM par une analyse à chaud, ou de points de fragilité d'implémentation ou de paramétrage du dispositif, ou encore de traces rémanentes enregistrées sur disque. Le temps nécessaire pourrait toutefois être réduit en ayant recours à un accélérateur équipé de nombreux processeurs en parallèle, ou à une grappe de microordinateurs dont la carte graphique pourra être utilisée avantageusement comme moyen de calcul. En dernier ressort, du fait de délais importants, le décryptage pourrait être confié au Centre Technique d'Assistance *(CTA)*, à la demande des autorités judiciaires selon la procédure de saisine, par l'intermédiaire de l'OCLCTIC, et sur réquisition écrite, avec maintien du secret des informations détenues par le CTA dont les moyens mis en œuvre sont classifiés au niveau *"Secret Défense"*.

Ainsi, les mesures anti-inforensiques peuvent être efficaces, si on dispose des connaissances et parfois… d'une volonté plus forte que le désespoir pour retrouver des éléments de preuves.

MYTHE N° 4 :
DE SIMPLES OUTILS ET CONNAISSANCES INFORMATIQUES SONT SUFFISANTS :

En cas de suspicion, il paraît légitime pour un organisme de chercher à pratiquer la collecte et l'analyse des preuves numériques. La direction peut être tentée de s'en remettre directement à son responsable informatique ou à un administrateur système ou réseaux, voire au responsable de la sécurité des systèmes d'information (RSSI). Bien que formés à leur métier, et disposant de divers outils, ces professionnels sont rarement des spécialistes formés à l'inforensique et les opérations peuvent être soumis à des risques.

Du point de vue juridique, il est fortement recommandé de disposer de l'appui d'un conseil juridique interne ou d'un avocat avant toute action. Dans la plupart des cas il est souhaitable de faire appel à un huissier de justice qui pourra consigner la réalité des opérations, assisté d'un expert judiciaire, sur la base d'une ordonnance du tribunal compétent pour délimiter le champ d'action et respecter en tout cas le droit, pour ne pas remettre en cause les opérations.

Du point de vue technique, la formation et la documentation techniques, mais aussi la pratique, sont indispensables avant toute activité de type inforensique. **Dans la phase de saisie**, une erreur de méthodologie, *-en particulier pour la préservation de l'intégrité d'un contenu-*, un dispositif inadapté ou une erreur d'utilisation dans la copie ou la collecte risque de détruire ou de corrompre les seules données disponibles. **Dans la phase d'analyse**, une méthode ou un outil inadapté peut être trop restreint et ne pas présenter d'éléments démonstratifs. C'est pourquoi des outils comme : *Encase, X-Ways Forensic, FTK, Coroner, Sleuth, etc.,* sont utiles. Enfin, une mauvaise interprétation serait en mesure d'anéantir tous les efforts et rendre le rapport irrecevable ou contrecarré devant la juridiction compétente.

Ainsi, de simples outils et même des connaissances informatiques de haut niveau ne sont pas suffisants, quand il est nécessaire d'opérer avec des méthodes et des outils inforensiques, lesquels exigent des connaissances technico-juridiques et de la pratique.

MYTHE N° 5 :
L'ADRESSE IP EST UN IDENTIFIANT INDISCUTABLE :

Le statut légal de l'adresse IP *pour Internet Protocol* **n'est pas clairement déterminé par la loi** en France *; tantôt considérée comme une donnée à caractère personnel, tantôt non.* La Cour de cassation, dans son arrêt du 13 janvier 2009, a jugé qu'il ne s'agissait pas d'une donnée identifiable, et donc que ce n'était pas une donnée à caractère personnel, telle que définie par la loi française. **Du point de vue de la jurisprudence**, **l'adresse IP matérialise l'infraction**, **mais n'identifie pas son auteur**, au vu cet arrêt de la Cour de cassation et de la décision du 1er février 2010 de la cour de Paris. Même si les renseignements obtenus par les enquêteurs auprès du fournisseur d'accès Internet *(FAI)* conduisent à une identification, le responsable des actes a pu utiliser l'ordinateur de ce tiers titulaire de cette adresse, ou encore usurper cette dernière.

Une proposition de loi tente d'énoncer le statut de l'adresse IP de façon à rendre cette dernière comme *"un moyen indiscutable d'identification, fût-elle indirecte, d'un internaute, au même titre qu'une adresse postale ou un numéro de téléphone"*. Il reste à voir si cette proposition sera adoptée, et déjà si elle est conforme à la réalité technique en rapport avec l'usurpation d'identité électronique. Ce point est au centre du problème et mérite explication *; qu'il s'agisse de l'adresse logique IP attribuée ou de l'adresse physique MAC du matériel correspondant.*

Concernant la mystification d'adresse logique IP : Le protocole IP ne vérifie pas l'adresse source des paquets. Aussi, au travers l'envoi de paquets modifiés, l'adresse IP de l'expéditeur peut être substituée par une autre. Il ne s'agit pas d'un changement d'adresse IP proprement-dit mais d'une mystification au niveau des paquets émis, en masquant l'adresse du véritable émetteur, lequel peut alors envoyer des paquets de façon *"anonyme",* en usurpant l'identité IP de la machine d'un tiers, suspecté mais pourtant sans rapport avec les faits.

Concernant la mystification d'adresse physique MAC : Au travers d'une connexion non filaire *(ex. WiFi après découverte de la clé WEP ou d'une clé WPA faible),* la clé est introduite dans les préférences d'Ethereal *(IEEE 802.11/clé WEP),* pour lire les paquets et obtenir l'adresse MAC de la victime. Il ne reste plus qu'à l'intrus à associer cette dernière à sa propre carte réseau, *-indication dans les propriétés avancées du panneau de configuration, ou avec un programme spécifique-*, puis de redémarrer sa machine qui sera maintenant vue avec l'adresse MAC substituée par celle de sa victime.

Des vérifications essentielles à la preuve s'imposent sur le système concerné par l'une ou l'autre adresse. Ceci implique de disposer de la machine suspectée et du bon support, *-disque dur ou autre sur système mobile-*, et de l'habilitation requise pour cette mission.

Ainsi, si l'adresse IP repérée est à considérer comme un premier indicateur. En aucun cas elle ne peut prétendre être un identifiant indiscutable.

MYTHES ET LEGENDES DES ERREURS JUDICIAIRES

Fabrice Mattatia
Ingénieur en chef des mines,
Docteur en droit

UN DIFFICILE APPRENTISSAGE

Un tribunal doit dans une même journée examiner des affaires très diverses. Vols, escroqueries, atteintes aux personnes, fraudes diverses, protection des mineurs… Le juge doit être polyvalent et s'adapter à toutes les infractions possibles. Il lui arrive aussi d'avoir à appliquer les textes relatifs au monde numérique. Or sauf exceptions, les magistrats n'ont eu dans leur formation aucune notion concernant le fonctionnement des TIC. Leur ignorance n'est pas blâmable, quand l'on songe à la technicité de cette matière, et à son rythme d'évolution qui fait que nous-mêmes ne pouvons suivre tous les développements récents : on ne peut demander à un juge d'être expert en tout. Mais cela pose parfois des difficultés lorsqu'il doit se confronter à des textes contenant des références techniques très pointues : le risque existe alors que le juge ne comprenne pas correctement les concepts en cause, et prononce une décision erronée ou mal fondée. Pensons par exemple à la loi sur la signature électronique et à ses décrets d'application, qui sans le dire explicitement supposent l'utilisation de la cryptographie asymétrique, si contraire au sens commun (voir : *Mythes et légendes de la signature électronique*).

Les juges ne sont pas les seuls à méconnaître les fondements techniques des TIC : les utilisateurs aussi sont parfois pris au piège. Les décisions de justice leur rappellent dans ce cas que l'usage des TIC peut avoir des conséquences juridiques.

Les paragraphes suivants recensent quelques cas de mauvaise interprétation des textes, ou de mythes dus à l'ignorance. Ces exemples plaident pour une plus large diffusion des notions techniques, aussi bien en direction de la population en général, qu'auprès des magistrats.

MYTHE N° 1 : UNE SIGNATURE SCANNEE EST UNE SIGNATURE ELECTRONIQUE

Saisie d'un litige sur la validité d'une signature scannée apposée sur un courrier papier, la Cour d'appel de Besançon a jugé le 20 octobre 2000 que la loi du 13 mars 2000 sur la signature électronique ne pouvait s'y appliquer.

Cet arrêt devrait donc rassurer le lecteur : tout le monde sait qu'une signature scannée n'est pas une signature électronique !

Malheureusement, une lecture plus attentive de l'arrêt jette le trouble. En effet, la Cour précise que « les parties s'accordent pour reconnaître que la signature apposée […] en date du 1er avril 1999 […] est la signature informatique de [l'expéditeur]. » La Cour le reconnaît également, mais elle tient à préciser les lois en vigueur à la date des faits : « l'acte litigieux a été établi antérieurement à la promulgation de la loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique. En conséquence, les dispositions de ce texte sont inapplicables en l'espèce ». Bref, selon cet arrêt, une signature scannée apposée en 1999 sur un document ne relève pas de la loi sur la signature électronique *uniquement parce que cette loi n'était pas en vigueur à l'époque.*

La Cour de cassation a confirmé cette interprétation le 30 avril 2003, en précisant que « dans le régime antérieur à la loi du 13 mars 2000, la validité du recours à cette signature ne pouvait être admise ».

On pourrait donc craindre que la Cour admette comme signature électronique une signature scannée réalisée *après* la promulgation de la loi de 2000. Toutefois, dans un arrêt récent (30 septembre 2010), la Cour de cassation a rappelé qu'il était indispensable de vérifier toutes les conditions posées par la loi (et inscrites dans le Code civile, articles 1316-1 à 1316-4) avant de conclure à la validité d'une signature électronique.

MYTHE N° 2 : UNE USURPATION D'ADRESSE MAIL CONSTITUE UN ACCES FRAUDULEUX A UN SYSTEME INFORMATIQUE

Le délit d'accès et de maintien frauduleux dans un système de traitement automatisé de données est défini de façon très large dans l'article 323-1 du Code pénal, ce qui permet de réprimer un spectre très étendu de fraudes. Toutefois, il arrive que certains jugements y aient recours de manière excessive, moins par commodité sans doute que par méconnaissance de la signification technique d'un « accès à un système ».

Le groupe médical Smith and Nephew a porté plainte contre un ancien employé qui, suite à un licenciement en 1998, envoyait aux clients de la société des documents mensongers ou falsifiés mettant en cause la réputation de l'entreprise. Afin de faire croire que les mails calomnieux provenaient de l'entreprise, le prévenu falsifiait dans leur en-tête l'adresse expéditeur, opération techniquement très simple. Comme l'indique le jugement du tribunal de grande instance du Mans du 7 novembre 2003, les mails falsifiés « comport[aient] la racine « @smith-nephew.com », laissant penser que leur auteur était effectivement membre du réseau interne du groupe Smith and Nephew ». Le jugement précise ensuite que « l'usage de fausses adresses électroniques d'expéditeur dont certaines ont été usurpées à leur détenteur, ainsi que l'envoi de tels messages sur les services de messageries électroniques de l'entreprise constituent de façon incontestable un moyen frauduleux d'accès dans le système de traitement automatisé gérant les services de messagerie électronique du groupe Smith and Nephew ». Ces motifs ont conduit le tribunal à reconnaître le prévenu coupable des délits de faux et usage de faux, et d'entrave à un système de traitement automatisé de données (pour des faits de mail bombing qui ont accompagné l'envoi de mails falsifiés). Il l'a condamné à 10 mois d'emprisonnement avec sursis et mise à l'épreuve, ainsi qu'à des dommages et intérêts qui se montaient à plus de 23.000 €.

Qualifier l'usage de fausses adresses mail de *moyen frauduleux d'accès*, comme l'a fait le tribunal, constitue pourtant une erreur. En effet, par définition, un *accès* suppose d'*accéder* au fonctionnement d'un système ou à ses données, ce qui n'est pas le cas lorsqu'on envoie un message. Lorsqu'on usurpe une adresse électronique en modifiant frauduleusement l'en-tête de ses mails, on n'accède nullement au système de traitement du titulaire légitime de l'adresse. Le fait d'envoyer de tels mails falsifiés vers le service de messagerie dont on usurpe l'adresse ne permet pas non plus un accès. L'interprétation « incontestable » des faits établie par le tribunal est au contraire très fortement contestable, même si l'équité du jugement ne fait aucun doute.

MYTHE N° 3 :
CELUI QUI SIGNALE UNE FAILLE DE SECURITE SERA RECOMPENSE

On peut s'attendre à ce qu'une entreprise ou une administration remercie chaleureusement celui qui lui signale une faille de sécurité dans son système d'information. Malheureusement, de telles marques de reconnaissance sont très rares. Le plus souvent, l'organisation concernée répond par le silence. Au pire, elle porte plainte contre celui qui l'a avertie.

Ainsi, en 1999, Antoine C., journaliste, s'est aperçu qu'en visitant au moyen d'un navigateur grand public le site de la société Tati, il était possible de suivre des liens jusqu'à des bases de données clients. Il en avertit deux fois la société Tati, sans résultat, puis révéla cette faille dans un article en novembre 2000. Tati porta alors plainte contre lui pour accès frauduleux à son système d'information. En première instance, le journaliste fut condamné, le tribunal estimant qu'un accès est effectivement frauduleux dès lors qu'il a lieu sans le consentement du propriétaire du système. La Cour d'appel de Paris, au contraire, considéra le 30 octobre 2002 que les données en cause sur le site web de Tati n'étant ni protégées par un quelconque dispositif technique, ni indiquées comme confidentielles, on ne pouvait reprocher à un internaute d'y accéder en suivant simplement les liens affichés sur le site.

Un autre arrêt de la Cour d'appel de Paris, statuant en référé le 9 septembre 2009, apporte un point de vue différent. Dans une affaire a priori similaire à la précédente, un journaliste du site spécialisé Zataz avait, après avoir averti la société FLP de l'existence d'une faille dans son système, publié un article sur le sujet. FLP l'avait alors attaqué en diffamation, procès que le journaliste avait gagné. Mais la Cour d'appel de Paris avait ensuite énoncé que l'accès non autorisé à un système constituait un « trouble manifestement illicite ». En conséquence, elle avait ordonné au journaliste de rendre inaccessible son article, et de détruire les pièces copiées sur le site de FLP, tout en étant condamné aux dépens. Cette procédure en référé (c'est-à-dire pour faire cesser un trouble en urgence) semblait en fait surtout destinée à faire supporter des frais de justice au journaliste, le « trouble » constitué par l'accès litigieux ayant cessé depuis longtemps, et l'article ayant déjà été retiré par le journaliste dès la première demande de la société FLP.

Notons que la situation à laquelle on aboutit ainsi est paradoxale : le Code pénal (article 226-17) fait par ailleurs obligation aux responsables de traitements de données personnelles de protéger ces données, sous peine de 5 ans de prison et de 300.000 euros d'amende. Or dans les affaires Tati et Zataz, les responsables des traitements en question, qui n'avaient pourtant pas satisfait aux exigences de la loi, n'ont même pas été poursuivis, et encore moins sanctionnés. Au contraire, ce sont ceux qui ont révélé leur négligence qui ont été poursuivis !

Cette dernière jurisprudence de la Cour d'appel de Paris risque désormais de dissuader ceux qui découvrent des failles de les signaler aux responsables informatiques, par peur de poursuites judiciaires. Les sites mal conçus resteront alors plus longtemps vulnérables face à des internautes mal intentionnés. Il devient indispensable de mieux protéger ceux qui découvrent et signalent des failles de sécurité. Après tout, le code pénal existant (article 221-5-3) prévoit bien d'exempter de peine « toute personne qui a tenté de commettre les crimes d'assassinat ou d'empoisonnement […] si, ayant averti l'autorité administrative ou judiciaire, elle a permis d'éviter la mort de la victime et d'identifier, le cas échéant, les autres auteurs ou complices ». Alors, pourquoi ne pas prévoir la même protection pour les « hackers blancs » ? Une modification législative en ce sens serait souhaitable.

MYTHE N° 4 :
UNE ADRESSE IP EST UNE DONNEE PERSONNELLE

Sur internet, la trace la plus répandue de l'identité de l'internaute réside dans l'adresse IP de son ordinateur. La capacité de relier via une adresse IP un historique de navigation à l'identité d'une personne, permet de dresser le profil de cette dernière et de retracer ses activités, mettant ainsi en danger sa vie privée. Toutefois, l'adresse IP est à proprement parler celle d'une machine, pas d'une personne. De nombreux débats ont donc eu lieu pour déterminer si l'adresse IP est ou non une donnée personnelle. Cette question représente notamment un enjeu dans la lutte contre le téléchargement illégal et dans la protection des droits d'auteur. Elle conditionnait pour les sociétés propriétaires de droits, avant l'adoption de la loi Hadopi, la possibilité de surveiller les téléchargements des internautes en les identifiant par leur adresse IP. Si l'adresse IP est une donnée à caractère personnel, alors elle est protégée par la loi Informatique et Libertés, et sa surveillance sans autorisation était illégale. La loi Hadopi promulguée en 2009, en autorisant spécifiquement la collecte d'IP pour lutter contre le téléchargement illégal, a réduit l'enjeu de ce débat, sans pour autant avoir précisé le statut de l'adresse IP.

En 2006-2007, plusieurs décisions contradictoires ont été rendues à ce sujet par les tribunaux.

Dans le cadre de deux procédures visant des échanges illégaux de fichiers musicaux, la Cour d'appel de Paris devait examiner la validité de procès-verbaux dressés à l'aide de traitements informatisés non déclarés préalablement à la CNIL par des agents assermentés des sociétés de gestion de droits d'auteurs. Ces agents avaient relevé les adresses IP des contrevenants et avaient ensuite demandé leurs noms aux fournisseurs d'accès à internet. L'enjeu de la question posée à la Cour était le suivant : si l'adresse IP est une donnée personnelle, alors les procédures en cause, dressées de manière viciée (sans déclaration à la CNIL), étaient entachées de nullité. Si l'adresse IP n'est pas une donnée personnelle, les procédures étaient bien valides. La Cour a estimé (27 avril et 15 mai 2007) que l'adresse IP ne constitue pas une donnée personnelle et qu'en conséquence son traitement ne relève pas de la loi Informatique et Libertés.

La CNIL s'est inquiétée publiquement de ces deux arrêts dans un communiqué du 2 août 2007, rappelant que toutes ses homologues européennes considéraient l'adresse IP comme une donnée personnelle. Plusieurs juridictions ont suivi la position de la CNIL. Ainsi, pour le tribunal de grande instance de Bobigny (14 décembre 2006), comme pour celui de Saint-Brieuc (6 septembre 2007), ainsi que pour la Cour d'appel de Rennes (22 mai 2008, 23 juin 2008), l'adresse IP constitue une donnée personnelle.

La Cour de cassation n'a pas saisi l'occasion, offerte par le pourvoi concernant un des arrêts de la Cour d'appel de Rennes, pour trancher le débat. Du coup, le législateur s'est penché sur la question. Celle-ci a été abordée en mars 2010 à l'occasion de la discussion en première lecture au Sénat de la proposition de loi des sénateurs Détraigne et Escoffier « visant à mieux garantir le droit à la vie privée à l'heure du numérique ». La rédaction initiale de la proposition de loi disposait que « constitue en particulier une donnée à caractère personnel toute adresse ou tout numéro identifiant l'équipement terminal de connexion à un réseau de communication », ce qui établissait clairement que l'adresse IP est une donnée personnelle. Cette rédaction a été modifiée lors des travaux en commission. La rédaction finalement adoptée précise que « tout numéro identifiant le titulaire d'un accès à des services de communication au public en ligne est visé par le présent alinéa». Cette phrase peut toutefois sembler tautologique, puisque la définition de la donnée à caractère personnel, énoncée dans

l'alinéa en question, se réfère déjà au fait que la donnée doit identifier une personne. La question n'est donc pas tranchée de manière définitive. En outre, cette proposition de loi doit encore, pour devenir définitive, être examinée par l'Assemblée nationale.

Le Contrôleur européen de la protection des données a d'ailleurs indiqué (2 septembre 2008) qu'une décision définitive sur le statut de l'adresse IP n'est pas nécessairement souhaitable. En effet, comme pour toute autre donnée, le caractère personnel ou non de l'adresse IP doit selon lui être évalué au cas par cas.

MYTHE N° 5 :
UNE CONVERSATION ENTRE AMIS SUR FACEBOOK EST PRIVEE

Des salariés de la société Alten ont été licenciés en 2010 pour avoir critiqué leur hiérarchie lors d'échanges sur leur mur Facebook. Les propos en cause avaient été dénoncés à leur supérieur par un de leurs « amis » qui avait accès à cette discussion.

Les salariés ont contesté le licenciement aux prud'hommes, invoquant une violation de leur vie privée. Mais le conseil des prud'hommes de Boulogne-Billancourt leur a donné tort le 19 novembre 2010. En effet, selon ce dernier, le mur sur lequel se tenait la discussion en cause était accessible non seulement à leurs amis, mais aussi aux amis des amis, bref à un nombre indéterminé de personnes. Or, pour être considéré comme privé, un échange doit être restreint à un cercle connu d'interlocuteurs.

MYTHES ET LEGENDES DU DROIT DE LA COMMUNICATION SUR L'INTERNET

Sadry Porlon
Avocat au Barreau de Paris
Docteur en droit

Le droit de la presse, dont la pierre angulaire reste la loi 29 juillet 1881, a été suivi par la création d'un droit plus large dit de la communication après l'apparition de la télévision, de la radio et plus récemment d'internet.

Ce droit de la communication qui, de prime abord, semble abordable, est en réalité un droit des plus techniques au sein duquel un formalisme des plus stricts doit être respecté pour envisager intenter avec succès une action devant les tribunaux ou encore faire valoir ses droits devant le responsable d'un site internet.

Il convient, en effet, de savoir distinguer la diffamation, de l'injure, du dénigrement ou encore de la simple atteinte à la vie privée pour être certain de voir ses demandes accueillies valablement par les juges.

L'apparition d'internet, sans pour autant avoir révolutionné le droit de la communication, a nécessité la mise en place des textes spécifiques contenus, pour la plupart, dans la loi du 24 juin 2004 dite Loi de Confiance dans l'Économie Numérique.

De nombreuses idées reçues sont diffusées autour du droit de la communication quand il touche à internet.

Gros plan sur certaines d'entre elles…

MYTHE N° 1 : UNE INJURE OU UNE DIFFAMATION DONT ON EST VICTIME SUR INTERNET EST SUSCEPTIBLE D'UNE ACTION DEVANT LES TRIBUNAUX TANT QUE LE MESSAGE EST VISIBLE SUR LE SITE LITIGIEUX

A la fin des années 1990, la doctrine s'est penchée sur la question de savoir si les infractions de presse commises sur internet devaient ou non présenter une spécificité d'ordre procédural par rapport aux infractions propres à la presse écrite.

Elle s'est demandée si ces infractions devaient être considérées comme continues, lesquelles subsistent tant que les messages sont accessibles et ne font courir le délai de prescription qu'à compter de la date de leur suppression, ou comme « instantanées », ce délai démarrant alors dès la date de la mise en ligne, constitutive du fait de publication. La Cour de cassation a posé, après quelques hésitations jurisprudentielles, que « lorsque des poursuites pour l'une des infractions prévues par la loi de 1881 sont engagées à raison de la diffusion, sur le réseau internet, d'un message figurant sur un site, le point de départ du délai de prescription de l'action publique prévu par l'article 65 de la loi du 29 juillet 1881 doit être fixé à la date du premier acte de publication ; que cette date est celle à laquelle le message a été mis pour la première fois à la disposition des utilisateurs ». (Cass. crim., 27 nov. 2001, C. : Comm. com. électr. 2002, comm. 32, obs. A. Lepage ; Légipresse 2002, n° 189, III, p. 26 et 27).

Dès lors, il faut donc considérer que sur internet, comme en matière de presse écrite, le délai de prescription commence à courir à compter du premier jour de la publication et que le fait que le message demeure accessible ou disponible n'y change rien.

Ce principe, qui peut paraître injuste à bien des égards, oblige celui qui s'interroge sur le bien fondé d'une action pour diffamation ou pour injure, suite à la découverte sur internet de propos litigieux, à s'assurer préalablement que le message a bien été publié moins de trois mois avant.

L'article 6-V de la loi de la Loi de Confiance dans l'Économie numérique du 21 juin 2004 renvoie, en effet, aux dispositions de l'article 65 de la loi de 1881 qui prévoit que ce délai de prescription est de trois mois à compter de la date de la publication.

Par ailleurs, depuis une loi n° 2004-204 du 9 mars 2004, le délai de prescription des infractions à caractère raciste (exemples : provocation à la discrimination ou à la haine raciale, diffamation raciale, injure raciale) est d'un an. Ce délai s'applique également à Internet.

MYTHE N° 2 :
IL FAUT AVOIR ETE INJURIE, DIFFAME OU DENIGRE POUR POUVOIR OBTENIR UN DROIT DE REPONSE AUPRES DU SITE INTERNET A L'ORIGINE DE L'INFRACTION

Le droit de réponse à un caractère général et absolu. Cela implique donc qu'il n'est pas subordonné à la preuve que les propos auxquels il répond soient motivés par une intention de nuire de la part de son auteur.

L'article 6, IV alinéa 1 de la loi du 21 juin 2004 dispose en effet que :

« Toute personne nommée ou désignée dans un service de communication au public en ligne dispose d'un droit de réponse, sans préjudice des demandes de correction ou de suppression du message qu'elle peut adresser au service (…) ».

Il suffit donc d'avoir été nommée ou désignée sur internet pour pouvoir prétendre à un droit de réponse auprès du directeur de publication du site.

Dans l'absolu, même un article flatteur et complètement exact est susceptible de provoquer un droit de réponse des plus valables de la part de la personne nommée ou désignée dans l'article ou le message disponible sur internet. Une disposition des plus utiles pour une personne physique ou morale qui, ne trouvant pas la matière suffisante à une action pour diffamation ou pour injure aurait, par cet intermédiaire, l'occasion de donner son point de vue et sa version des faits en réplique à l'article ou au message litigieux.

MYTHE N° 3 :
IL FAUT AVOIR ETE INJURIE, DIFFAME OU DENIGRE POUR POUVOIR OBTENIR UN DROIT DE REPONSE AUPRES DE LA TELEVISION OU DE LA RADIO A L'ORIGINE DE L'INFRACTION

Tout dépendra en réalité du moyen de diffusion de cette télévision ou de cette radio.

Il faut savoir que la réglementation du droit de réponse dans les services de communication audiovisuelle (c'est à dire à la télévision ou à la radio) est extérieure à la loi du 29 juillet 1881.

Le droit de réponse spécifique à la presse écrite n'a donc pas été, contrairement à internet, directement transposé en matière audiovisuelle.

Le droit de réponse à la radio ou à la télévision est subordonné à la démonstration « d'imputations susceptibles de porter atteinte à l'honneur ou à la réputation d'une personne ».

L'article 6 de la loi du 29 juillet 1982 dispose que : « Toute personne physique ou morale dispose d'un droit de réponse dans le cas où des imputations susceptibles de porter atteinte à son honneur ou à sa réputation auraient été diffusées dans le cadre d'une activité de communication audiovisuelle (…)

Il existe néanmoins une exception à ce principe.

Dans le cas de ce qu'on appelle une web télé ou d'une web radio (médias diffusés exclusivement sur internet), la réglementation relative au droit de réponse redevient celle prévue à l'article 6 IV de la loi du 21 juin 2004, ce qui implique que tout message désignant une personne peut être à l'origine d'un droit de réponse ; quelle que soit sa teneur.

MYTHE N° 4 :
DEMANDER UN DROIT DE REPONSE A L'EDITEUR D'UN SITE INTERNET ET L'OBTENIR EMPECHE TOUTE ACTION DEVANT LES TRIBUNAUX CONTRE L'AUTEUR DES PROPOS.

Les actions pour diffamation ou pour injure sont indépendantes de l'exercice du droit de réponse. Une personne peut donc légitimement solliciter un droit de réponse en engageant simultanément une action devant les tribunaux contre l'auteur du message diffusé sur internet.

MYTHE N° 5 :
LE FAIT QUE L'AUTEUR D'UN MESSAGE DIFFAMATOIRE OU INJURIEUX SE SOIT EXCUSE PUBLIQUEMENT SUITE A LA DIFFUSION DU PROPOS LUI PERMETTRA D'ECHAPPER A UNE SANCTION EN CAS D'ACTION DEVANT LES TRIBUNAUX.

Le repentir actif, c'est-à-dire l'action qui consiste pour l'auteur d'un message injurieux ou diffamatoire à présenter ses excuses publiques ou à publier un rectificatif, ne supprime pas l'intention coupable.

La personne directement visée par les propos litigieux pourra toujours agir et obtenir la condamnation de son auteur.

MYTHE N° 6 :
LE FAIT POUR L'EDITEUR D'UN SITE INTERNET DE NE PAS AVOIR MIS A DISPOSITION DES INTERNAUTES UN CERTAIN NOMBRE D'ELEMENTS D'IDENTIFICATION COMME, POUR LES PERSONNES PHYSIQUES, (SON NOM, SON PRENOM, SON DOMICILE) OU POUR LES PERSONNES MORALES (SA DENOMINATION, SA RAISON SOCIALE OU ENCORE SON SIEGE SOCIAL) NE PEUT PAS LUI VALOIR UNE CONDAMNATION DEVANT LES TRIBUNAUX.

Le non-respect des obligations prévues à l'article 6-III-1 de la loi du 21 juin 2004 est « puni d'un an d'emprisonnement et de 75 000 euros d'amende ». (Article 6-VI-2 de la loi du 21 juin 2004).

Les personnes morales peuvent se voir interdire d'exercer leur activité « pour une durée de cinq ans au plus ». (L. 131-38 et L. 131-39 du Code pénal).

L'article 6-III-2 prévoit une exception notamment pour les blogueurs anonymes qui exercent cette activité à titre non professionnel. Cet article pose, en effet, que « les personnes éditant à titre non professionnel un service de communication au public en ligne peuvent ne tenir à la disposition du public, pour préserver leur anonymat, que le nom, la dénomination ou la raison sociale » de leur fournisseur d'hébergement, « sous réserve de lui avoir communiqué

les éléments d'identification personnelle » exigés des éditeurs de services agissant à titre professionnel.

C'est d'ailleurs cette distinction entre les obligations d'identification auxquelles sont tenus les éditeurs professionnels et les éditeurs non professionnels de services en ligne qui a motivé la fameuse proposition de loi en date du 3 mai 2010 du Sénateur Jean-Louis Masson, laquelle tendait « à faciliter l'identification des éditeurs de sites de communication en ligne et en particulier des « blogueurs » professionnels et non professionnels ».

MYTHE N° 7 :
IL EST POSSIBLE DE REPRODUIRE INTEGRALEMENT L'ARTICLE D'UN AUTEUR SUR SON SITE A CONDITION DE CITER SON NOM ET LA SOURCE DE L'ARTICLE.

L'article L. 122-4 du Code de la propriété intellectuelle dispose que :

« Toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droits est illicite. Il en est de même pour la traduction, l'adaptation ou la transformation, l'arrangement ou la reproduction par un art ou un procédé quelconque. »

L'article L. 335-2 alinéa 3 du Code de la propriété intellectuelle ajoute que :

« Toute édition d'écrits, de composition musicale, de dessin, de peinture ou de toute autre production imprimée ou gravée en entier ou en partie, au mépris des lois et règlements relatifs à la propriété des auteurs, est une contrefaçon, et toute contrefaçon est un délit ».

Il s'agit d'un délit puni de trois ans d'emprisonnement et de 300.000 euros d'amende.

L'article L. 122-5 du Code de la propriété intellectuelle prévoit néanmoins une exception dans le cas où il s'agit d'une courte citation de l'article. La courte citation s'évaluera par rapport aux dimensions de l'œuvre citée, mais aussi de celle de l'œuvre citante. Cette citation devra être justifiée par certaines finalités (critique, polémique, pédagogique, scientifique ou d'information) de l'œuvre d'origine. Elle devra également être intégrée à une œuvre ayant une autonomie propre en dehors des citations.

MYTHE N° 8 :
LE FAIT DE REPRODUIRE UNE ŒUVRE OU UN CONTENU SUR UN SITE INTERNET A VOCATION NON COMMERCIALE PERMET D'ECHAPPER A UNE CONDAMNATION POUR CONTREFAÇON.

Malgré une forte croyance chez l'internaute lambda, la loi n'a jamais entendu faire de distinction l'éditeur d'un site qui reproduit l'œuvre d'un tiers sans autorisation et dans un but commercial et celui qui le fait dans un but non commercial. Les deux sont, dès lors, potentiellement condamnables pour contrefaçon à ce titre tant sur le plan pénal que sur le plan civil.

CONCLUSION

Ces quelques exemples contribuent à illustrer le fossé qui existe entre la perception qu'à l'internaute lambda d'un internet dans lequel régnerait le vide juridique et la réalité dans laquelle ce média n'a finalement eu que peu de mal à se voir appliquer des règles datant du XIXème siècle. Les contentieux sans cesse croissants générés par quelques uns des millions de messages diffusés quotidiennement sur les blogs, les forums de discussion ou encore à travers les réseaux sociaux comme Facebook ou Twitter, sont d'ailleurs là pour en témoigner.

MYTHES ET LEGENDES DES TELECHARGEMENTS ILLEGAUX

Sadry Porlon
Avocat au Barreau de Paris
Docteur en droit

La loi du 12 juin 2009 favorisant la diffusion et la protection de la création (dite HADOPI 1), puis celle du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet (dite HADOPI 2) ont conduit d'une part, à la création de la HADOPI, Haute autorité pour la diffusion des œuvres et la protection des œuvres, à celle de création d'une obligation pour le titulaire de l'accès à l'internet ne soit pas utilisé à des fins de contrefaçon, sorte d'obligation de sécurisation de l'accès à l'internet à la charge de l'abonné, faute de quoi il s'exposera notamment à la contravention de négligence caractérisée, et d'autre part à adapter le dispositif pénal applicable aux contrefaçons commises sur internet.

Quelques idées reçues existent encore sur le téléchargement illégal en général et sur HADOPI en particulier…

MYTHE N°1 :
L'EXCEPTION POUR COPIE PRIVEE PERMET A CELUI QUI TELECHARGE UNE ŒUVRE SUR INTERNET SANS AUTORISATION DE NE PAS ETRE CONDAMNE DEVANT LES TRIBUNAUX S'IL DEMONTRE QUE LADITE COPIE A FAIT L'OBJET D'UNE UTILISATION STRICTEMENT PRIVEE

L'article L. 122-5 du Code de la propriété intellectuelle prévoit qu'il est possible de copier une œuvre pour un usage privé.

L'article L. 122-5 alinéa 2 refuse, en effet, la possibilité à l'auteur de l'œuvre d'interdire « les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective (…) ».

L'exception affirmée par le Code de propriété intellectuelle ne distingue pas selon les supports.

Mieux, il n'est nulle part exigé que le copiste se doive de disposer de l'œuvre originale pour en faire la copie. L'article L 122-5 du Code de la propriété intellectuelle qui accorde à l'utilisateur un droit à la copie privée ne distingue pas non plus selon que la copie soit légale ou pas ou encore que l'utilisateur possède l'original dont il fait la copie.

La question de savoir si l'exception de copie privée trouve ou non à s'appliquer dans le cas d'une copie d'œuvres téléchargées sur internet, notamment via logiciel peer to peer, a donc longtemps été, de ce fait, l'objet d'une vive controverse doctrinale et jurisprudentielle.

Des opinions défavorables à la prise en compte de l'exception pour copie privée en cas de téléchargement sans autorisation se sont développées à partir de l'idée selon laquelle la copie réalisée à partir d'un exemplaire contrefaisant est elle-même contaminée par ce caractère illicite et ne peut donc pas être couverte par l'exception pour copie privée.

La jurisprudence est venue depuis clarifier quelque peu la situation.

Dans une affaire qui a fait beaucoup parler, un étudiant avait gravé près de 500 films sur cédéroms ; films qu'il avait, notamment, auparavant téléchargés sur Internet. Poursuivi devant les tribunaux pour contrefaçon de droit d'auteur par la majeure partie de l'industrie cinématographique mondiale, il a tenté de se prévaloir de l'exception pour copie privée.

En premier instance, le Tribunal correctionnel de Rodez a conclu, le 13 octobre 2004, à l'absence de contrefaçon, ce qu'à confirmé la Cour d'Appel de Montpellier, dans un arrêt en date du 10 mars 2005, sans pour autant se prononcer sur le caractère licite ou illicite de la source des copies.

La Cour de Cassation est venu casser l'arrêt précité en retenant notamment que :

« Attendu que, pour confirmer le jugement entrepris, l'arrêt retient qu'aux termes des articles L 122-3, L 122-4 et L 122-5 du code de la propriété intellectuelle, lorsqu'une œuvre a été divulguée, l'auteur ne peut interdire les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective ; que les juges ajoutent que le prévenu a déclaré avoir effectué les copies uniquement pour un usage privé et qu'il n'est démontré aucun usage à titre collectif ;

Mais attendu qu'en se déterminant ainsi, sans s'expliquer sur les circonstances dans lesquelles les œuvres avaient été mises à disposition du prévenu et sans répondre aux conclusions des parties civiles qui faisaient valoir que l'exception de copie privée prévue par l'article L 122-5, 2°, du code de la propriété intellectuelle, en ce qu'elle constitue une dérogation au monopole de l'auteur sur son œuvre, suppose, pour pouvoir être retenue que sa source soit licite et nécessairement exempte de toute atteinte aux prérogatives des titulaires de droits sur l'œuvre concernée, la cour d'appel n'a pas justifié sa décision ; ».

Dès lors, il n'est donc pas possible de prétexter valablement de l'exception pour copie privée pour télécharger, sans autorisation, des œuvres sur internet.

MYTHE N°2 : DEPUIS LES LOIS HADOPI, LE TELECHARGEMENT ILLEGAL D'UNE ŒUVRE SUR INTERNET NE PEUT PLUS ETRE SANCTIONNE « QUE » PAR UNE SUSPENSION D'INTERNET PENDANT UN MOIS MAXIMUM ET D'UNE AMENDE NE DEPASSANT PAS 1500 EUROS.

Un décret du 25 juin 2010, pris en application de la loi HADOPI 2 est venu définir ce qu'est la contravention de négligence caractérisée tout en précisant la caractérisation de ce manquement et les sanctions encourues par l'abonné.

L'article R. 335-5 du Code de la propriété intellectuelle dispose désormais que :

« I.-Constitue une négligence caractérisée, punie de l'amende prévue pour les contraventions de la cinquième classe, le fait, sans motif légitime, pour la personne titulaire d'un accès à des services de communication au public en ligne, lorsque se trouvent réunies les conditions prévues au II :

1. Soit de ne pas avoir mis en place un moyen de sécurisation de cet accès ;
2. Soit d'avoir manqué de diligence dans la mise en œuvre de ce moyen.

II.-Les dispositions du I ne sont applicables que lorsque se trouvent réunies les deux conditions suivantes :

1. En application de l'article L. 331-25 et dans les formes prévues par cet article, le titulaire de l'accès s'est vu recommander par la commission de protection des droits de mettre en œuvre un moyen de sécurisation de son accès permettant de prévenir le

renouvellement d'une utilisation de celui-ci à des fins de reproduction, de représentation ou de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise ;

2. Dans l'année suivant la présentation de cette recommandation, cet accès est à nouveau utilisé aux fins mentionnées au 1° du présent II.

III.-Les personnes coupables de la contravention définie au I peuvent, en outre, être condamnées à la peine complémentaire de suspension de l'accès à un service de communication au public en ligne pour une durée maximale d'un mois, conformément aux dispositions de l'article L. 335-7-1.

L'abonné s'expose donc à ce titre à une contravention de 5ème classe (amende de 1500 euros maximum) ainsi qu'à une peine complémentaire de suspension de l'accès à internet qui ne pourra excéder un mois.

Cependant, le recours à la procédure judiciaire simplifiée de l'ordonnance pénale prévue par la loi HADOPI 2 n'est qu'une possibilité qui vient s'ajouter aux actions civiles et pénales liées à la contrefaçon de droit d'auteur et en aucun un préalable nécessaire à l'engagement de poursuites.

Tout abonné dont l'accès à internet a été utilisé à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits reste, en effet, sous la menace d'une action en contrefaçon de droit d'auteur et des sanctions encourues en matière de contrefaçon soit une peine maximum d'emprisonnement de 3 ans et une amende de 300.000 euros (article L. 335-2 du Code de la propriété intellectuelle).

La loi HADOPI 2 a d'ailleurs apporté des changements en matière de sanctions pénales en précisant qu'une nouvelle possibilité de sanction pénale est donnée au juge lorsque le délit de contrefaçon a été commis par le biais d'un service de communication au public en ligne à savoir celle de prononcer une peine complémentaire de suspension de l'accès à internet pendant une durée maximale d'un an (Article L. 335-7 alinéa 1).

MYTHE N°3 :

SI MON ACCES A INTERNET EST SUSPENDU SUITE A UNE DECISION DU JUGE, IL ME SUFFIT DE SOUSCRIRE IMMEDIATEMENT UN NOUVEL ABONNEMENT

Il est interdit à un abonné dont l'accès à internet aurait été suspendu suite à une décision du juge de se réabonner par un autre moyen.

L'article L. 335-7-1 du Code de la propriété intellectuelle prévoit d'ailleurs que le fait pour la personne condamnée à la peine complémentaire de suspension d'internet de ne pas respecter l'interdiction de souscrire un autre contrat d'abonnement à un service de communication au public en ligne pendant la durée de la suspension est puni d'une amende d'un montant maximal de 3 750 euros.

MYTHE N°4 :

SI LE JUGE DECIDE D'UNE SUSPENSION DE MON ABONNEMENT, JE NE VAIS QUAND MEME PAS ETRE CONTRAINT DE CONTINUER A PAYER CET ABONNEMENT PENDANT LA DUREE DE CETTE SUSPENSION

Dans l'hypothèse d'une suspension d'internet pendant un maximum d'un an au motif qu'une sanction pénale au titre d'une contrefaçon aurait été prononcée par le juge cette suspension

de l'accès n'affecte pas, par elle-même, le versement du prix de l'abonnement au fournisseur du service.

L'article L. 121-84 du code de la consommation qui dispose : « Tout projet de modification des conditions contractuelles de fourniture d'un service de communications électroniques est communiqué par le prestataire au consommateur au moins un mois avant son entrée en vigueur, assorti de l'information selon laquelle ce dernier peut, tant qu'il n'a pas expressément accepté les nouvelles conditions, résilier le contrat sans pénalité de résiliation et sans droit à dédommagement, jusque dans un délai de quatre mois après l'entrée en vigueur de la modification » n'est pas applicable au cours de la période de suspension.

Les frais d'une éventuelle résiliation de l'abonnement au cours de la période de suspension sont supportés par l'abonné.

Pour information, le fait pour une le fournisseur d'accès à internet de ne pas mettre en œuvre la peine de suspension qui lui a été notifiée est également puni d'une amende maximale de 5 000 euros.

MYTHE N°5 :

L'ABONNE QUI REÇOIT DES RECOMMANDATIONS DE LA PART DE LA HADOPI DEVRA ATTENDRE D'ETRE POURSUIVI DEVANT LES TRIBUNAUX POUR FAIRE VALOIR SES DROITS

L'abonné qui reçoit un ou plusieurs avertissements peut directement présenter ses observations à la Commission de protection de la HADOPI et demander des précisions sur le contenu des œuvres et objets protégés concernés par le ou les manquements qui lui sont reprochés.

Il pourra notamment être convoqué ou demandé à être entendu et pourra se faire assister du conseil de son choix.

Si une ordonnance pénale venait à être rendue à son encontre, l'abonné aura également la possibilité de contester la décision rendue, dans un délai de quarante cinq jours à compter de la notification en formant opposition à l'exécution de ladite ordonnance.

Cela a pour conséquence de renvoyer l'affaire devant le tribunal correctionnel pour un débat qui sera, cette fois, contradictoire.

Il reviendra alors à l'abonné de monter, le cas échéant avec l'aide de son conseil, un dossier visant à démontrer, preuves à l'appui, qu'il n'est en aucun cas le responsable des faits qui lui sont directement reprochés et qu'eu égard à l'article 121-1 du Code pénal disposant que : « Nul n'est responsable que de son propre fait », il ne peut être valablement sanctionné.

MYTHE N°6:

EN PRESENCE D'UN TELECHARGEMENT ILLEGAL AVERE, LE JUGE A UNE MARGE DE MANŒUVRE ASSEZ FAIBLE DANS LA FIXATION DE LA DUREE DE LA SUSPENSION DE L'ACCES A INTERNET

L'article L. 335-7-2 du Code de la propriété intellectuelle prévoit que pour prononcer la peine de suspension (peine complémentaire à l'amende de contravention de 5ème catégorie) prévue aux articles L. 335-7 (un an maximum en cas de contrefaçon) et L. 335-7-1 (un mois maximum en cas de négligence caractérisée) et en déterminer la durée, la juridiction prend en compte les circonstances et la gravité de l'infraction ainsi que la personnalité de son auteur, et notamment l'activité professionnelle ou sociale de celui-ci, ainsi que sa situation socio-économique.

Ainsi, cet article permet notamment au juge de tenir compte de la personnalité de l'abonné afin de déterminer la peine complémentaire de suspension d'internet.

On imagine que cela puisse être le cas d'une entreprise pour laquelle le maintien de la connexion à internet est la condition sine qua non du maintien de son activité ou encore d'un particulier qui justifierait que ce média est pour lui une ouverture indispensable sur le monde.

L'article 335-7-2 du Code de la propriété intellectuelle précise d'ailleurs que la durée de la peine prononcée doit concilier la protection des droits de la propriété intellectuelle et le respect du droit de s'exprimer et de communiquer librement, notamment depuis son domicile.

MYTHE N°7 :
C'EST LA HAUTE AUTORITE POUR LA DIFFUSION DES ŒUVRES ET LA PROTECTION DES ŒUVRES QUI COLLECTE, ELLE-MEME, LES ADRESSES IP DES ABONNES DONT L'ACCES A SERVI A TELECHARGER DES ŒUVRES

La HADOPI, saisie en cela par les ayants droits des œuvres, peut constater et établir des procès verbaux de manquements à l'obligation de sécurisation, adresser des avertissements aux abonnés ou encore transmettre au procureur de la République tout fait susceptible de constituer une infraction.

Elle ne collecte pas directement les adresses IP. Ce sont les organismes assermentés représentant les titulaires des droits (pour l'heure, la société Trident Media Guard - TMG) qui, ayant reçu préalablement les autorisations nécessaires de la CNIL pour effectuer ces démarches, se chargent d'observer les œuvres circulant sur les réseaux et de collecter ce type informations.

La HADOPI se contente de recevoir les saisines des sociétés de perception et de répartition des droits et des organismes de défense professionnelle ayant reçu une autorisation de la CNIL.

Elle peut par la suite obtenir des fournisseurs d'accès à l'internet ou des prestataires d'hébergement, l'identité, l'adresse postale, l'adresse électronique et les coordonnées téléphoniques de l'abonné dont l'accès à l'internet à été utilisé à des fins de contrefaçon et ce sur la base des adresses IP collectées par les sociétés privées mandatées par les ayants droit pour surveiller les réseaux de téléchargement illégal. La réponse graduée débutera ensuite par l'envoi d'une recommandation ou « avertissement » à l'abonné par le biais d'un courriel et par l'intermédiaire du fournisseur d'accès auprès duquel il a souscrit un abonnement.

Celle-ci prévoit notamment un rappel de l'obligation de sécurisation, la mention de la date et l'heure auxquelles les faits susceptibles de constituer un manquement à l'obligation de sécurisation ont été constatés ainsi que les coordonnées téléphoniques, postales et électroniques où l'abonné peut s'adresser, s'il le souhaite, pour formuler ses observations et obtenir des précisions sur ce qui lui est reproché.

Si dans les six mois suivant cette recommandation l'accès à internet devait à nouveau être utilisé pour « des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits lorsqu'elle est requise », une seconde recommandation pourra lui être adressée par le biais d'une lettre recommandée avec avis de réception ou encore par tout autre moyen permettant d'établir la preuve de la date de présentation de cette recommandation.

La loi HADOPI 1 a imposé à la personne titulaire de l'accès à des services de communication au public en ligne l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits lorsqu'elle est requise.

Si malgré un second avertissement l'accès internet de l'abonné devait de nouveau servir à des fins de contrefaçon de droit d'auteur, la HADOPI pourra remettre son dossier à un juge afin que l'abonné soit, notamment, sanctionné d'une amende et/ou d'une suspension de son accès à internet ou encore transmettre au procureur de la république tout fait susceptible de constituer une infraction.

MYTHE N°8 :
JE NE SUIS PLUS DANS L'ILLEGALITE A PARTIR DU MOMENT OU J'UTILISE UN SERVICE PAYANT POUR OBTENIR DE LA MUSIQUE OU DES FILMS SUR INTERNET

Les plates-formes légales de téléchargements de musique, dont la plus connue est iTunes, sont autorisées par les ayant droits à commercialiser sous format numérique des œuvres, notamment, musicales ou audiovisuelles.

A côté d'elles, on a vu éclore ces derniers mois des sites internet, qui, profitant de l'épouvantail que constitue la loi HADOPI, proposent, pour une dizaine d'euros par mois, des téléchargements illimités d'œuvres diverses et variées.

A l'occasion du MIDEM 2011 de Cannes, la HADOPI a présenté une étude intitulée : « *Hadopi, biens culturels et usages d'Internet : pratiques et perceptions des internautes français* », qui laisse apparaître « *une incompréhension et un manque de distinction* » chez l'internaute lambda de ce qu'est une offre légale par rapport à une offre illégale. Selon cette étude, pour 59% des internautes déclarant des usages licites et pour 53% des internautes en moyenne, le caractère payant est une garantie de la légalité.

Les internautes déclarant des usages illicites sont plus nombreux à savoir que le payant n'est pas forcément légal, alors que presqu'un tiers des internautes « ne sait pas ».

Il convient donc de rappeler aux internautes que les plates-formes légales de téléchargements sont celles qui sont autorisées expressément par les titulaires de droits (ayant droits) à commercialiser et distribuer les contenus et qu'il est, à l'heure actuelle, difficile d'envisager une offre légale qui, pour 10 euros, donnerait légalement accès à un catalogue exhaustif d'œuvres musicales, audiovisuelles, de jeux vidéos et de livres numériques français et étrangers.

Le 10 novembre 2010, un décret n° 2010-1366 du 10 novembre 2010 relatif à la labellisation des offres des services de communication au public en ligne et à la régulation des mesures techniques de protection et d'identification des œuvres et des objets protégés par le droit d'auteur a d'ailleurs mis en place la procédure visant à obtenir un label de « légalité » de la part de la HADOPI.

CONCLUSION

Ces quelques exemples démontrent une fois de plus le fossé qui existe entre le grand public qui associe assez souvent internet gratuité et le législateur qui n'a finalement qu'à de rares exceptions accepté que ce média puisse déroger aux grands principes du droit de la propriété intellectuelle.

MYTHES ET LEGENDES DE LA CONTREFAÇON SUR L'INTERNET

Sadry Porlon
Avocat au Barreau de Paris
Docteur en droit

Le fléau mondial qu'est la contrefaçon sur internet prend différentes formes. L'une des plus connues, à savoir le téléchargement illégal, ayant été abordée dans un chapitre précédent, nous allons cette fois nous intéresser à quelques unes des actions qu'il est possible d'intenter devant les tribunaux pour faire cesser l'infraction qu'il s'agisse de contrefaçon de droit d'auteur, de marque ou encore de concurrence déloyale (cybersquatting).

MYTHE N°1 : DE SIMPLES IMPRESSIONS D'ECRAN SUFFISENT POUR PROUVER DEVANT LES TRIBUNAUX LA MATERIALITE D'UNE CONTREFAÇON SUR INTERNET

L'article 1315 du Code civil fait peser la charge de la preuve sur le demandeur. En vertu de ce principe fondamental, le juge attend que celui qui intente une action en justice lui apporte la preuve de l'infraction alléguée.

Plusieurs décisions récentes sont venues rappeler que la preuve d'une infraction sur internet, qu'il s'agisse d'une contrefaçon ou encore d'un délit de presse (injure ou diffamation), n'est pas une preuve comme les autres.

Même si la preuve d'un fait juridique (événement susceptible de produire des effets juridiques) peut se faire par tous moyens en vertu de l'article 1348 du Code civil, le juge n'accepte, en effet, pas tous les moyens de preuve qui lui sont présentés quand il s'agit d'une infraction commise sur internet.

Ces moyens de preuve doivent respecter un certain nombre d'exigences pour pouvoir prétendre à une valeur probante aux yeux des juges.

Depuis plusieurs années, il est, en effet, établi que faire constater une infraction sur internet se doit de respecter un formalisme des plus stricts. Le juge impose à l'huissier ou encore à l'Agence de protection des programmes[49] qui se charge du constat, de respecter un certain nombre d'étapes lors son établissement.

Il devra notamment :

- Décrire le matériel grâce auquel le constat est établi (configuration technique)
- Effacer l'historique, les cookies, les répertoires de la mémoire cache de l'ordinateur avant de procéder au cheminement lui permettant d'accéder à la page internet litigieuse.

[49] Même si l'Agence de Protection des Programmes (APP) dispose d'agents assermentés qui ont autorité pour constater la preuve de la matérialité de toute infraction relative à un droit d'auteur, à un droit sur un logiciel, sur la base de données, ou à un droit relatif à un artiste interprète, l'infraction sur internet est souvent constatée par un procès verbal dressé par un huissier de justice.

La Cour d'Appel de Paris, dans un arrêt du 17 novembre 2006, a refusé d'admettre comme preuve un constat d'huissier au motif que l'huissier n'avait pas vidé les caches contenus dans la mémoire du serveur proxy, service offert par le fournisseur d'accès.[50]

- Inscrire le numéro IP de la machine ayant servi à dresser le constat sur son procès verbal dans le but de permettre en cas de contestation « *de vérifier au moyen du journal de connexion du serveur interrogé les pages réellement consultées pendant les opérations de constat* ».[51]
- Décrire le cheminement qu'il a lui-même effectué pour accéder à la page internet contenant l'infraction. Le constat doit « *établir l'existence de liens hypertextes* » dans le but de s'assurer que le cheminement doit pouvoir être effectué par n'importe quel internaute « *sans connaissance de l'organisation du site* ».[52]
- Matérialiser la page internet contenant l'infraction en l'imprimant puis en l'annexant au procès-verbal.

Un jugement du Tribunal de Grande Instance de Mulhouse en date du 7 février 2007[53] a retenu que « *le fait de ne pas avoir cliqué sur le lien et imprimé la page du site rend cette recherche sur internet incomplète et ne permet pas d'apprécier la réalité des griefs invoqués* ».

Toutes ces décisions rappellent l'importance pour le demandeur de disposer d'une preuve respectant des règles strictes et non pas de simples copies d'écran établies par lui-même dans des conditions inconnues, faute de quoi il prendrait le risque de ne pas voir l'action qu'il engagera couronnée de succès.

MYTHE N°2 : DANS L'HYPOTHESE OU LES INFRACTIONS AURAIENT ETE SUPPRIMEES DU SITE PAR SON EDITEUR, UN SITE D'ARCHIVAGES DE PAGES WEB PERMET DE PALLIER L'ABSENCE DE PREUVE

Parce que les informations disponibles sur internet peuvent être rapidement modifiées et que la preuve de leur présence avant cette modification est souvent difficile à établir, de nombreux contentieux ont vu apparaître des constats internet au sein desquels figuraient des copies de pages de site d'archivages, comme celui du site internet www.archive.org.

Ce type de site permettant d'avoir une représentation « fidèle » de tout ou partie d'un site internet tel qu'il était plusieurs mois, voire plusieurs années auparavant, nombreux sont les demandeurs qui ont tenté de contourner la difficulté de l'absence de preuves « actuelles », en faisant constater par un huissier, la présence de l'infraction sur le site litigieux (par l'entremise du site d'archivage) à une date antérieure à la supposée modification.

La question s'est néanmoins très vite posée de la valeur probante des pages internet constatées par le biais de ce site d'archivage.

La Cour d'Appel de Paris a récemment eu l'occasion de se prononcer sur ce point.

---

[50] *CA Paris, 4è ch., B. 17 nov. 2006, SARL Net Ultra c/ AOL, RLDI 2006/22, n°706, obs/ Auroux J.B.*

[51] Tribunal de Grande Instance de Paris, 3ème chambre, 1ère section, Jugement du 4 mars 2003.

[52] Tribunal de Grande Instance de Paris, 3ème chambre, 1ère section, Jugement du 4 mars 2003.

[53] TGI Mulhouse, 1re ch., 7 février 2007, Ste Groupe Bosc c/St MMT

Dans un arrêt en date du 2 juillet 2010, les juges ont retenu qu'aucune force probante ne pouvait être reconnue audit constat, quant au contenu, pendant la période au cours de laquelle les actes de contrefaçon auraient été commis au motif que « *le constat a été effectué à partir d'un site d'archivage exploité par un tiers à la procédure, qui est une personne privée sans autorité légale, dont les conditions de fonctionnement sont ignorées* » avant d'ajouter que « *cet outil de recherches n'est pas conçu pour une utilisation légale* » et que « *l'absence de toute interférence dans le cheminement donnant accès aux pages incriminées n'était donc pas garantie* ».

MYTHE N°3 :
LE SEUL MOYEN DE LUTTER EFFICACEMENT CONTRE UN CYBERSQUATTEUR ET DE RECUPERER SON NOM DE DOMAINE CONSISTE A ENGAGER CONTRE LUI UNE ACTION DEVANT LES TRIBUNAUX

Le cybersquatting se définit comme le fait pour une personne d'usurper le signe distinctif d'autrui en l'enregistrant en tant que nom de domaine.

Cette pratique qui existe depuis plus d'une dizaine d'années a évolué au cours du temps.

Ce fléau mondial est désormais combattu en France tant par la voie judiciaire (référé, action au fond) que par la voie de l'arbitrage (procédure UDRP[54], ADR[55], CERDP[56] DCDRP[57], STOP[58], IPDRCP[59], PARL[60], PREDEC[61] et de la médiation.[62]

Les signes distinctifs auxquels il est fréquemment porté atteinte, par le biais d'une réservation de nom de domaine, sont notamment la marque, le nom commercial, la dénomination sociale, l'enseigne, le nom patronymique ou le nom d'une collectivité territoriale.

En France, il est établi que les procédures de référé ne peuvent aboutir, eu égard aux pouvoirs du juge des référés, à un transfert du nom de domaine au bénéfice du requérant.

---

[54] Uniform Domain Name Dispute Resolution Policy pour les extensions en .com, .net et .org et pour les litiges opposant des noms de domaine et des marques.

[55] Alternative Dispute Resolution pour les extensions en .eu.

[56] Charter Eligibility Dispute Resolution Policy pour les extensions en .aero, .coop et .museum.

[57] DotCoop Dispute Resolution Policy pour l'extension en .coop

[58] *Star-up Trademark Opposition Policy pour l'extension en .biz.*

[59] *pour l'extension en .pro*

[60] Procédure alternative de résolutions des litiges adaptée aux extensions .fr et .re.

[61] Procédure de Règlement de Résolutions des cas de violations manifestes des dispositions du Décret du 6 février 2007.

[62] Pour ce qui concerne le .fr et le .re, l'AFNIC (Association Française pour le nommage Internet en Coopération) délègue au Forum des Droits sur l'Internet, par l'intermédiaire du service mediateurdunet.fr, le règlement extrajudiciaire de litiges entre deux particuliers ou entre un particulier et une entreprise.

Un arrêt dit Sunshine (Cass. com., 9 juin 2009, n°08-12-904) est, en effet, venu préciser que le transfert d'un nom de domaine ordonné par ledit juge « ne constituait ni une mesure conservatoire, ni une mesure de remise en état » au sens de l'article 809, alinéa 1er du Code de procédure civile. Il sera néanmoins possible d'obtenir le gel ou le blocage du nom de domaine dans le cadre d'une action devant le juge des référés.

Il faudra donc, pour obtenir le transfert du nom de domaine, engager une action au fond devant les tribunaux. Il est utile de rappeler que les procédures UDRP ou PARL aboutissent à ce même transfert dans un délai qui excède rarement les quatre mois suivant la saisine.

L'inconvénient principal de ces procédures dites UDRP tient dans le fait qu'elles ne possèdent aucun caractère dissuasif. Même si le transfert du nom de domaine litigieux est ordonné, la décision ne sera pas accompagnée de dommages-intérêts ni même du remboursement des frais de procédure engagés par le demandeur à la charge du défendeur, lesquels restent l'apanage des décisions de justice qui suivent les actions en référé ou au fond engagés devant les tribunaux.

Il convient donc de bien peser le pour et le contre avant de décider de la stratégie à adopter pour faire cesser définitivement un trouble lié à la reprise, par un individu lambda ou par un concurrent, de son signe distinctif dans un nom de domaine.

MYTHE N°4 :
QUAND IL EXISTE UN CONFLIT ENTRE UNE MARQUE ET UN NOM DE DOMAINE ENREGISTRE POSTERIEUREMENT A CETTE MARQUE, IL SUFFIT QUE LE NOM DE DOMAINE SOIT IDENTIQUE OU SIMILAIRE A LA MARQUE POUR QUE LA CONTREFAÇON DE MARQUE SOIT ETABLIE

Quand il existe un conflit entre une marque et un nom de domaine enregistré postérieurement à cette marque, on estime désormais que pour qu'il y ait contrefaçon, il faut un acte consistant à utiliser un signe identique ou similaire pour désigner des produits identiques ou similaires.

La règle de la spécialité, qui existe en matière de marques, a été transposée aux noms de domaine.

Il faut savoir que les juges ont un temps retenu la contrefaçon de marque selon une méthode différente d'identification de la spécialité du nom de domaine. Ils considéraient, en effet, que les noms de domaine avaient pour spécialité les services de communication par réseau informatique (services de communication en ligne ou services assimilés) prévus dans la classe 38 de la classification de Nice.

Ce raisonnement avait pour conséquence de ne pas reconnaître la contrefaçon alors même que les services proposés par le site étaient de la même spécialité que la marque contrefaite, faute pour le titulaire de la marque d'avoir visé dans son dépôt le « service de communication » en ligne de la classe 38.

Inversement, quand la marque visait expressément le « service de communication en ligne » de la classe précitée, les juges retenaient la contrefaçon alors que le site internet utilisant le nom de domaine exploitait des produits ou des services différents.

Un important arrêt dit Locatour (Cass. Com. 13 décembre 2005) est venu préciser clarifier la situation en indiquant qu' : « *Attendu qu'un nom de domaine ne peut contrefaire par reproduction ou par imitation une marque antérieure, peu important que celle-ci soit déposée en classe 38, pour désigner des services de communication télématique, que si les produits et services offerts sur ce site sont soit identiques, soit*

similaires à ceux visés dans l'enregistrement de la marque et de nature à entraîner un risque de confusion dans l'esprit du public ».

Il convient désormais se déterminer par rapport aux produits ou services proposés par le site du nom de domaine, et non par référence automatique à la classe 38 pour les noms de domaines.

La spécialité du nom de domaine, en cas de conflit avec une marque, sera liée à la spécialité du site auquel il renvoie.

MYTHE N°5 :
EN CAS DE CONFLIT ENTRE DEUX TITULAIRES DE NOMS DE DOMAINES IDENTIQUES OU SIMILAIRES, L'ANTERIORITE SE DEDUIT DE LA DATE D'ENREGISTREMENT DU NOM DE DOMAINE

Faux : en cas de conflit entre deux noms de domaines, c'est la date de commencement d'exploitation des noms de domaines et non la date d'enregistrement de ces derniers qui compte.

En pratique, cela signifie que le titulaire d'un nom de domaine, qui ne l'aurait pas utilisé pour un site internet, ne pourra pas se prévaloir d'une antériorité valable et d'une action pertinente en concurrence déloyale pour cybersquatting à l'égard d'un réservataire postérieure qui aurait exploité, avant lui, un nom de domaine identique ou similaire dans le cadre d'un site internet.

MYTHE N°6 :
UTILISER UNE PHOTO, UN DESSIN OU L'ŒUVRE D'UN TIERS SANS SON AUTORISATION POUR ILLUSTRER UN BLOG OU UN SITE PERSONNEL N'EST PAS CONDAMNABLE

À l'heure du web 2.0, il devient toujours plus facile de créer un site internet, notamment via l'émergence de blogs tels que wordpress. La tentation est donc assez forte pour les utilisateurs de ces plates-formes d'utiliser des contenus qu'ils ont piochés çà et là sur la toile afin d'illustrer leurs sites.

Ces choix ne sont cependant toujours pas sans conséquence. En effet, un créateur de site web ou un particulier peut être tenté d'utiliser une œuvre sans autorisation en minimisant volontairement l'importance que cet emprunt pourrait avoir sur la suite.

Rappelons à ce propos que la mise en ligne d'une création littéraire ou artistique, quelle qu'elle soit, correspond à un acte de représentation et que le droit commun de la propriété littéraire et artistique s'applique de manière classique à internet.

L'article L. 122-1 du Code de la propriété intellectuelle prévoit en effet que « le droit d'exploitation appartenant à l'auteur comprend le droit de représentation et le droit de reproduction ». Ce sont ces droits lui permettent de tirer profit de l'exploitation de son œuvre.

L'article L. 122-4 du CPI précise que « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants illicite » tandis que l'article L. 335-3 du CPI ajoute qu' « *est (…) un délit de contrefaçon toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur* ».

En vertu de ces articles, un auteur peut donc agir contre un créateur de site web ou un simple particulier pour avoir reproduit ou représenté son œuvre sur son site internet sans

autorisation et réclamé des dommages-intérêts pour contrefaçon de droit d'auteur au titre du préjudice tant moral que patrimonial qu'il a subi.

Les tribunaux ont été amenés à sanctionner, à plusieurs reprises, des personnes qui avaient, sans autorisation, diffusé des œuvres artistiques sur leur site internet.

Même si dans la pratique, les internautes ne sont pas systématiquement poursuivis pour avoir reproduit une œuvre sans en avoir préalablement demandé l'autorisation à son auteur, le risque encouru mérite qu'il soit également rappelé que les conditions d'utilisation de l'œuvre, en l'occurrence pour un site à but non-lucratif, n'empêchent en rien que l'atteinte soit constituée.

MYTHE N°7 :

EN CAS DE CONTREFAÇON DE PRODUITS SUR UN SITE E-COMMERCE QUI LES LIVRE A SES CLIENTS A TRAVERS PLUSIEURS PAYS DU MONDE, LE DEMANDEUR PEUT OBTENIR LA REPARATION DU PREJUDICE MONDIAL SUBI EN SAISISSANT LA JURIDICTION FRANÇAISE.

Malgré le fait que le site internet soit disponible depuis n'importe quel pays du monde, le juge français, notamment en matière de contrefaçon, n'est compétent que pour réparer les préjudices subis sur le territoire français.

En France, l'article 46 du Code de Procédure Civile précise que le demandeur peut saisir à son choix, outre la juridiction du lieu où demeure le défendeur (article 42 du Code de Procédure civile) :

- en matière contractuelle, la juridiction du lieu de la livraison effective de la chose ou du lieu de l'exécution de la prestation de service ;
- en matière délictuelle, la juridiction du lieu du fait dommageable ou celle dans le ressort de laquelle le dommage a été subi ;

La contrefaçon étant un délit, le demandeur devra démontrer que le produit a bien été vendu en France pour que le juge français puisse s'estimer compétent.

CONCLUSION :

Ces quelques exemples illustrent l'importance pour le demandeur de bien cerner les enjeux légaux et procéduraux avant d'intenter une action en justice dont l'objectif sera de voir réparer le préjudice subi par la contrefaçon commise sur Internet.

MYTHES ET LEGENDES DE LA PUBLICITE SUR INTERNET

Sadry Porlon, avocat au barreau de Paris
Docteur en droit

Même si le droit de la publicité a vocation à s'appliquer sur internet, quelques nouveaux outils de communication, à commencer par le système publicitaire Google AdWords, quelques lois ou encore quelques décisions de justice sont venues rappeler que le Web présente quelques spécificités dont il convenait de tenir compte.

MYTHE N° 1 : SUR INTERNET, IL EST PERMIS DE SE PRETENDRE LE N°1 D'UN SECTEUR SANS QUE CELA SOIT EXACT

Eu égard au fait qu'elles ne sont pas aussi agressives et affirmées qu'aux Etats-Unis, on croit souvent, à tort, que la publicité comparative est interdite en France. La licéité de la publicité comparative a pourtant été affirmée par la loi n° 92-60 du 18 janvier 1992 et confirmée par l'ordonnance n° 2001-741 du 23 août 2001.

La publicité comparative doit cependant remplir certaines conditions parmi lesquelles ne pas être parasitaire. L'article L. 121-8, 1° du Code de la consommation affirme également que la publicité comparative ne doit pas être trompeuse ou de nature à induire en erreur.

Une pratique commerciale est trompeuse notamment lorsqu'elle repose sur des allégations, indications ou présentations fausses ou de nature à induire en erreur et portant sur l'identité, les qualités, les aptitudes et les droits du professionnel.

En l'occurrence, prétendre être le n°1 d'un secteur donné sans que cela corresponde à la réalité expose la société qui le prétend à un risque d'action pour publicité comparative trompeuse de la part de l'un des concurrents visés dans la publicité.

Un jugement du 30 septembre 2009 de la 8ème chambre du Tribunal de commerce de Paris en est l'illustration.

Il a notamment obligé, dans cette affaire qui opposait deux sites consacrés aux médias dont l'un se prétendait leader du secteur, le défendeur à cesser la publication des annonces litigieuses et à publier sur son site internet pendant trente jours le résumé suivant du jugement : « *Par jugement en date du... , le tribunal de commerce de Paris a condamné la société T….. pour avoir diffusé sur le site internet j…..com deux annonces affirmant faussement que le site " j….com " était le premier blog média de France alors que sur la période de référence il était devancé de plus de 10 000 visiteurs par le site internet www.o……com édité par la société L.…*», en haut de la page d'accueil, sur toute la largeur de la page et un tiers de sa hauteur.

Même si ce jugement a été frappé d'appel, le fait qu'une action en justice ait été menée à son terme dans ce cas de figure rappelle la nécessité de bien verrouiller juridiquement les éléments qui serviront à promouvoir votre entreprise sur internet.

Dès lors qu'une publicité sera jugée contraire aux dispositions des articles L. 121-8 à L. 121-14 du Code de la consommation, le juge pourra, en effet, estimer que cette faute cause au concurrent cité un préjudice qui mérite réparation.

Pour être précis, dans l'affaire susvisée, le concurrent à l'origine de l'action n'était pas cité, ce qui rendait difficile les chances de succès de l'action au titre de la publicité comparative trompeuse.

Comme l'a retenu le jugement du Tribunal de Commerce : « *Les deux annonces ne mettent pas en comparaison des biens et des services mais se limitent à affirmer la suprématie d'un site. Les conditions de la publicité comparative, posées par l'article L.121-8 du code de la consommation sur la publicité comparative ne sont dès lors pas remplies* ».

MYTHE N° 2 :
LA PUBLICITE PROMOUVANT L'ALCOOL EST INTERDITE SUR INTERNET

La publicité en faveur des boissons alcooliques est régie par les dispositions de l'article L. 3323-2 du Code de la santé publique, texte, issu de la loi n° 91-32 du 10 janvier 1991 relative à la lutte contre le tabagisme et l'alcoolisme, dite « loi Évin », qui énumère limitativement les supports sur lesquels « *la propagande ou la publicité, directe ou indirecte, en faveur des boissons alcooliques* », est autorisée.

La question s'est rapidement posée de savoir si un industriel du secteur de l'alcool pouvait promouvoir son activité par le biais d'internet.

Le Conseil d'État y est allé de son interprétation, dans un rapport publié en 1998 en indiquant que l'intention du législateur était d'inclure dans la liste des messages autorisés ceux adressés par minitel et par téléphone et que dans le silence de la loi la publicité sur Internet devait être autorisée. Il invitait le législateur a confirmer son interprétation.

Une série de décisions de justice a ensuite interprété strictement la loi Évin et estimé que le réseau internet ne faisait pas partie des supports autorisés.

Dans une ordonnance de référé du 2 avril 2007, le Tribunal de Grande Instance de Paris a retenu que l'article L3323-2 « *définit les supports autorisés exclusivement à diffuser la propagande ou la publicité, en faveur des boissons alcooliques ; que leur énumération, limitative, ne comprend pas le réseau internet ; que la seule diffusion sur un site internet d'une publicité en faveur d'une boisson alcoolique constitue un trouble manifestement illicite* ». Une vision reprise par leTribunal de Grande Instance de Paris dans une seconde ordonnance de référé du 8 janvier 2008, et confirmée en appel, obligeant le site incriminé de cesser la diffusion du message publicitaire.

Suite aux réactions provoquées par ces décisions, tant du côté des acteurs économiques des industriels de la filière vitivinicole que de celui des associations de santé publique, de protection des mineurs et de défense des consommateurs et des familles, Le Forum des Droits sur l'Internet a mis en place un groupe de travail réunissant des professionnels d'internet et de la publicité, des représentants des utilisateurs et des observateurs publics et adopté le 15 décembre 2008 une Recommandation dans laquelle il préconisait d'autoriser la publicité pour l'alcool sur internet de manière raisonnée en recommandant notamment d'interdire la publicité pour l'alcool sur les sites internet sportifs et sur ceux destinés à la jeunesse.

Suivant en cela quelques unes des préconisations de feu le Forum des Droits sur l'Internet, la Loi n° 2009-879 du 21 juillet 2009, portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires, dite « Loi Bachelot » ou « Loi Hôpital, patients, santé, territoires » la publicité en faveur de l'alcool est désormais autorisée, à l'exception des sites « *principalement destinés à la jeunesse* » et des sites sportifs, sous réserve qu'elle ne soit « *ni intrusive ni interstitielle* ».

L'article 97 de la loi portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires a, en effet, introduit dans le Code de la santé publique un 9° à l'article L. 3323-2 intégrant ainsi « *les services de communications en ligne* » à la liste des supports autorisés pour effectuer de la publicité en faveur des boissons alcooliques : « *Après le 8° de l'article L. 3323-2 du code de la santé publique, il est inséré un 9° ainsi rédigé : « 9° Sur les services de communications en ligne à l'exclusion de ceux qui, par leur caractère, leur présentation ou leur objet, apparaissent comme principalement destinés à la jeunesse, ainsi que ceux édités par des associations, sociétés et fédérations sportives ou des ligues professionnelles au sens du code du sport, sous réserve que la propagande ou la publicité ne soit ni intrusive ni interstitielle* ».

MYTHE N° 3 :
LE FAIT D'UTILISER LA MARQUE DE SON CONCURRENT DIRECT DANS LE CADRE DU SERVICE GOOGLE ADWORDS ENGAGE L'ANNONCEUR ET GOOGLE SUR LE TERRAIN DE L'ACTION EN CONTREFAÇON DE MARQUES AINSI QUE SUR CELUI DE LA PUBLICITE TROMPEUSE.

Un nouveau type de contentieux est né suite à la création par Google d'un système publicitaire permettant d'afficher des bannières publicitaires ciblées en fonction des mots-clés que tapent les internautes tant sur son moteur de recherche que sur son service de messagerie électronique.

Dénommé AdWords, ce système de publicité a parfois été détourné de sa finalité par certaines entreprises dans le but de promouvoir leurs produits et services.

Il est, en effet, fréquent qu'une entreprise s'aperçoive, en tapant le nom commercial de sa société dans le moteur de recherche de Google, qu'apparaîssent, à côté des résultats de référencement naturel, des liens commerciaux invitant l'internaute à se connecter à des sites internet qui sont ceux de sociétés concurrentes.

Pour cette raison, les sociétés titulaires de droits sur les marques ont décidé d'assigner l'annonceur indélicat, mais aussi Google pour contrefaçon de marques et publicité trompeuse et mensongère.

Les juges ont d'abord, dans une jurisprudence pour le moins hésitante, condamné ces sociétés à ce titre.

La Cour de justice de l'Union Européenne a alors été saisie par Google d'une série de questions préjudicielles de la part des sociétés Google de façon à ce qu'elle se prononce sur cette épineuse question mettant en jeu la responsabilité de Google sur ce système sur lequel repose une grande partie de son modèle économique.

Par un arrêt en date du 23 mars 2010, la CJUE a notamment retenu que :

« *le prestataire d'un service de référencement sur internet qui stocke en tant que mot clé un signe identique à une marque et organise l'affichage d'annonces à partir de celui-ci, ne fait pas un usage de ce signe au sens de l'article 5, paragraphes 1 et 2, de la directive 89/104 ou de l'article 9, paragraphe 1, du règlement n° 40/94* ».

Selon cette dernière, en proposant à des annonceurs l'usage comme mots-clés de signes déposés en tant que marques, Google ne commet donc pas d'actes de contrefaçon de marques et de publicité mensongère.

Par quatre arrêts du 13 juillet 2010, la Cour de cassation a mis en œuvre les solutions dégagées par la CJUE le 23 mars 2010[63].

Dès lors et contrairement à ce qui était antérieurement jugé, Google ne sera plus tenue pour responsable au titre de la contrefaçon de marques et de la publicité mensongère dans le cadre de l'exploitation de son service AdWords.

La responsabilité de Google pourra cependant être engagée sur le fondement du droit commun de la responsabilité civile sous certaines conditions.

Notons sur ce point que par un arrêt du 19 novembre 2010 (Google c/Syndicat français de la Literie), la Cour d'appel de Paris a qualifié Google d'hébergeur s'agissant de son activité de régie publicitaire AdWords en appliquant les principes posés par la CJUE dans son arrêt du 23 mars 2010 avant d'ajouter que sa responsabilité ne saurait être engagée sur le fondement du droit des marques mais sur uniquement sur celui du droit commun de la responsabilité civile (article 1382 du Code civil) et de retenir enfin « ***que le Syndicat Français de la Literie ne rapportait pas la preuve du caractère actif de Google dans la rédaction des annonces publicitaires ou dans la sélection des mots-clés (…)*** », condition sine qua non de l'engagement de sa responsabilité à ce titre.

Parce que Google est dès lors considérée comme un hébergeur, à défaut d'avoir eu un rôle actif dans la rédaction de l'annonce publicitaire ou dans l'établissement ou la sélection des mots clés, il faut en déduire qu'elle ne peut voir sa responsabilité engagée que si elle ne supprime pas promptement une annonce manifestement illicite qui lui a été notifiée (article 6-I-5 de la LCEN).

Ces différentes décisions ont le mérite de clarifier considérablement une activité qui a connu de multiples rebondissements jurisprudentiels ces dernières années et qui, au cœur même du modèle économique de Google, lui a valu d'être pointée du doigt par l'Autorité de la concurrence qui a retenu qu'elle **« *est en position dominante sur le marché de la publicité liée aux moteurs de recherche* »**[64].

La Commission européenne a d'ailleurs confirmé récemment avoir envoyé des questionnaires à différents acteurs d'Internet dans le cadre d'une enquête qui, ouverte à la fin du mois de novembre pour abus de position dominante, vise plus généralement les activités de la société Google dans le domaine de la recherche en ligne.

MYTHE N° 4 :

SI LA PUBLICITE DE MON CONCURRENT S'AFFICHE DANS LES LIENS COMMERCIAUX ADWORDS LORSQUE JE TAPE LE NOM DE MA MARQUE DANS LE MOTEUR DE RECHERCHE DE GOOGLE, C'EST DONC QU'IL A CHOISI MA MARQUE COMME MOT-CLEF ET QUE JE PEUX DES LORS ENGAGER DIRECTEMENT SA RESPONSABILITE.

Les choses ne sont pas aussi simples que cela.

---

[63] *Cass. Com., 13 juillet 2010, , pourvoi n° F 05-14.331, Google France c./ Viaticum, Luteciel ; Cass. Com., 13 juillet 2010, pourvoi n° B 06-1 5.136, Google France c./ CNRRH, Pierre-Alexis T., Bruno R. et M. Montravers, es qualité de mandataire liquidateur de la société Tiger ; Cass. Com., 13 juillet 2010, pourvoi n° X 08-13.944, Google France, Google Inc, Google Ireland Ltd c./GIFAM et autres ; Cass. Com., 13 juillet 2010, pourvoi n° P 06-20.230, Google France, Google Inc, c./ Louis Vuitton Malletier.*

[64] *Avis du 14 décembre 2010 sur le fonctionnement concurrentiel de la publicité en ligne.*

Même si à l'origine du système publicitaire de Google, la réponse à cette question aurait pu être automatiquement positive, les récents perfectionnements mis en place par la société précitée doivent pousser ceux qui s'estimeraient victimes d'actes de contrefaçon de marques à un minimum de prudence avant d'intenter une action devant les tribunaux.

Google a, en effet, mis en place un système dit de requête large qui lui permet de diffuser automatiquement des annonces pour des variantes pertinentes des mots-clés choisis par l'annonceur et ce, même si ces termes ou expressions ne figurent pas dans ses listes de mots clés.

Les variantes de mots clés englobent les synonymes, les formes au pluriel et au singulier, les variantes pertinentes des mots clés et les expressions contenant ces derniers.

Cette précision est importante puisqu'elle signifie que vous pourrez voir votre annonce s'afficher quand un internaute tape le nom de votre concurrent alors qu'à aucun moment vous n'avez choisi ce mot-clé dans votre campagne.

Conçu par Google afin de générer davantage de trafic sur votre site web, ce système a d'ores et déjà abouti à ce que des sociétés attaquent devant les tribunaux leur concurrent direct pour contrefaçon de marques en raison de l'utilisation de mots-clés qu'ils n'ont, dans certains cas, jamais utilisés.

Ce qui n'est pas sans poser des difficultés quant à l'issue de l'action ainsi engagée puisque le défendeur, sûr de son droit, pourra être tenté de réclamer du demandeur la preuve de ce qu'il allègue, à savoir la contrefaçon, conformément à l'article 1315 du Code civil et ce, au delà du simple constat selon lequel la publicité du concurrent s'affiche quand on tape le nom de la marque litigieuse.

Ainsi, faute de s'être assuré de l'utilisation effective de sa marque par le concurrent avant d'engager l'action, il prendra le risque de ne pas voir ladite procédure couronnée de succès si des investigations menées en cours de procédure auprès de Google Ireland Limited (société responsable du programme AdWords) laissaient apparaître que le concurrent n'a en aucun réservé le mot-clé correspondant à la marque.

MYTHE N° 5 :
POSTER DE FAUX AVIS DE CONSOMMATEURS SUR INTERNET AFIN DE PROMOUVOIR SES PRODUITS OU SERVICES EST TOLERE ET N'EST PAS CONDAMNABLE.

La gestion de tout ce qu'il se dit sur internet à propos d'une personne morale est, depuis quelques années, l'objet d'un véritable business dénommé « E-réputation ».

Parce que les commentaires négatifs sont nombreux tant sur les blogs, sur les sites internet que sur les forums de discussion (les mécontents étant bien souvent plus prompts à donner leur avis que ceux qui sont satisfaits), certains acteurs du net ont parfois été tentés de poster eux-mêmes de faux avis ou commentaires afin de contrebalancer ceux qui ne leur étaient pas favorables.

D'abord marginale, cette activité qui aurait tendance à se développer vient d'être pointée du doigt par le Gouvernement[65].

Le 21 janvier 2011, Frédéric Lefebvre, secrétaire d'Etat chargé du Commerce, à l'occasion d'une visite au Centre de surveillance du commerce électronique, l'antenne de la DGCCRF

[65] *http://www.01net.com/editorial/527226/le-gouvernement-veut-faire-le-tri-dans-les-avis-de-consommateurs/*

dédiée au commerce électronique basée à Morlaix, a décidé de se pencher sur ses pratiques dans le cadre d'un plan d'action consacré à l'e-commerce.

Il a confié à ces cyber-enquêteurs le soin de faire le point sur le secteur des avis de consommateurs, qu'il s'agisse de publications sur des sites marchands, des forums ou des réseaux sociaux. Ils ont dès lors un an pour mener à bien leur mission.

Si des preuves suffisantes venaient à être collectées par ces agents de la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), des dossiers seront constitués afin d'être envoyés devant les tribunaux pour pratiques commerciales trompeuses.

L'article 121-1 du Code de la consommation définit, notamment, une pratique commerciale trompeuse comme étant celle qui repose sur des allégations, indications ou présentations fausses ou de nature à induire en erreur et portant sur (…) l'identité, les qualités, les aptitudes et les droits du professionnel.

Les articles 121-2 à 121-7 du Code de la consommation prévoient, quant à eux, que la pratique commerciale trompeuse est punie d'un emprisonnement de deux ans au plus et d'une amende de 37 500 euros au plus, cette amende pouvant être portée à 50 % des dépenses de la publicité ou de la pratique constituant le délit.

Afin de tenter de régler la question de la fiabilité des commentaires sur internet, certains sites internet proposent d'ores et déjà, grâce à l'intervention active de professionnels, de « certifier » que le commentaire ou l'avis a bien été posté par une personne qui n'a aucun intérêt direct à favoriser une entreprise ou détriment d'une autre[66].

CONCLUSION

Une fois de plus, ces quelques exemples démontrent à quel point les implications juridiques d'une campagne orchestrée pour être diffusée sur internet méritent d'être cernées tant que par l'annonceur que par les sociétés qui s'estimeraient victimes de ladite campagne.

L'Internet n'est ni une jungle ni une zone de non droit dans lesquelles on pourrait tout dire et tout faire. Bien au contraire…

[66] *Voir en http://www.tooteclair.com/*

MYTHES ET LEGENDES DE L'E-COMMERCE

Sadry Porlon, avocat au barreau de Paris
Docteur en droit

Le commerce électronique, également appelé e-commerce, désigne l'échange de biens et de services entre deux entités sur les réseaux informatiques. Il est l'objet de nombreux mythes. Nous allons revenir sur quelques uns d'entre eux.

MYTHE N° 1 : ON EST LIBRE DE TOUT ACHETER SUR INTERNET

La liste des biens que l'on peut se procurer sur internet est longue.

Certains achats sont néanmoins formellement interdits par la loi au motif qu'il s'agit de produits dont la vente est prohibée en France. On citera par exemple le commerce d'organes humains, celui d'objets volés (recel), d'animaux protégés ou encore de produits contrefaits.

D'autres commercialisations sont interdites en raison du fait qu'elles nécessitent une autorisation préalable. C'est le cas des armes, des munitions de guerre, de certains végétaux, de médicaments, des parfums. En cas de manquement à ces règles, le vendeur comme l'acheteur, lui-même, sont susceptibles d'être exposés à des sanctions pénales.

MYTHE N° 2 : UN MINEUR N'A PAS LE DROIT D'ACHETER DES PRODUITS SUR INTERNET

Les choses ne sont pas si simples que cela. En effet, même si l'article 1124 du Code civil dispose que : « *Sont incapables de contracter, dans la mesure définie par la loi (notamment) les mineurs non émancipés* », la jurisprudence est venue progressivement assouplir cette règle en indiquant qu'un contrat conclu par un mineur non émancipé, dès lors qu'il est en âge de raison, sera considéré comme valable s'il a été réalisé à des conditions normales et qu'il constitue un acte de la vie courante.

Il s'agira d'une appréciation in concreto. Le juge saisi devra alors tenir compte de l'âge du mineur ou encore des ressources dont il dispose.

Acheter un appartement ne sera pas considéré comme un acte de la vie courante pour un mineur non émancipé, là où l'achat d'une application sur un iPhone pourrait l'être.

Quoi qu'il en soit, les actes considérés comme non courants nécessiteront le consentement préalable des personnes exerçant l'autorité parentale.

Si le juge retient que l'acte n'est pas de la vie courante, il pourra dès lors décider d'annuler le contrat ou encore de modifier le prix.

MYTHE N° 3 : LE DROIT DE RETRACTATION PERMET A QUICONQUE A ACHETE UN PRODUIT SUR INTERNET DE SE RETRACTER DANS UN DELAI DE SEPT JOURS

Le droit de rétractation a été institué au profit des consommateurs par la loi 6 janvier 1988 relative au « télé-achat ». Codifié aux articles L. 121-20 et suivants du Code de la consommation, ce droit n'est en réalité applicable qu'à la condition que le vendeur ou le

prestataire soit un professionnel. Si vous achetez, sur eBay par exemple, un bien a un particulier, vous ne bénéficierez pas de ce droit de rétractation.

Ce droit est, par ailleurs, opposable uniquement aux sites internet dont le siège social est situé en France ou dans une autre État membre de l'Union européenne grâce à la directive communautaire sur la vente à distance.

Parce qu'il est d'ordre public, il s'applique également aux produits d'occasion ou soldés.

MYTHE N° 4 :
LE DROIT DE RETRACTATION S'APPLIQUE AUSSI AUX ACHATS DE PLACES DE CONCERTS, AUX RESERVATIONS D'HOTELS OU ENCORE DE BILLETS D'AVION SUR INTERNET.

Le droit de rétractation permet au consommateur ayant conclu un contrat à distance avec un professionnel d'obtenir, sans motif, le remboursement de sa commande passée à distance, à condition d'agir dans un délai de sept jours à compter de la réception du bien ou de la conclusion du contrat pour les services. Ce droit n'est cependant pas valable pour tous les achats effectués en ligne.

Il connaît plusieurs exceptions, prévues aux articles L. 121-20-2 et L. 121-20-4 du Code de la consommation.

En vertu de ces textes, sont notamment exclus du droit de rétractation, les contrats de prestation de services d'hébergement, de transport, de restauration, de loisirs qui doivent être fournis à une date ou selon une périodicité déterminée, et notamment les voyages ou encore ceux de fourniture de biens susceptibles de se détériorer ou de se périmer rapidement ;

Un arrêt récent, Cour de cassation 1ère chambre civile du 25 novembre 2010 (Mme X et M. Y / Go Voyages) est d'ailleurs venu rappeler cette règle à une juridiction de proximité en indiquant ceci : « *Alors qu'il résulte des dispositions l'article L. 121-20-4 du code de la consommation que le droit de rétractation de sept jours prévu à l'article L. 121-20 du même code, n'est pas applicable aux prestations d'hébergement, quel que soit le mode de conclusion du contrat dont celles-ci sont l'objet, et notamment en cas de conclusion par la voie électronique ; qu'en jugeant néanmoins, pour condamner la société Go Voyages à réparer le préjudice résultant pour mademoiselle X... et monsieur Y... du fait qu'ils avaient été privés de leur droit de rétractation, que ces derniers qui avaient réservé plusieurs nuits d'hôtel par l'intermédiaire du site internet de cette société devaient bénéficier, nonobstant les stipulations contractuelles, d'un droit de rétractation conformément aux dispositions des articles L. 121-18 et L.121-19 du code de la consommation, la juridiction de proximité a violé par fausse interprétation ces dispositions ainsi que celles des articles L. 121-20 et L. 121-20-4 du même code* ».

MYTHE N° 5 :
LORSQUE L'ON VEND DES BIENS SUR INTERNET SANS ETRE UN VENDEUR PROFESSIONNEL OU UN COMMERÇANT, IL EST IMPOSSIBLE D'ETRE CONSIDERE COMME TEL

L'individu qui vend des produits sur des sites comme eBay, PriceMinister ou encore Leboncoin peut être qualifié de vendeur professionnel si certaines conditions sont réunies.

L'article L. 121-1 du Code de commerce dispose que « *sont commerçants ceux qui exercent des actes de commerce et en font leur profession habituelle* ». Les actes d'achat de biens meubles effectués en vue de leur revente sont considérés comme des actes de commerce.

Dès lors, quand vous effectuez des actes de commerce à titre habituel, vous pouvez être considéré comme un commerçant.

La jurisprudence ajoute souvent comme condition pour être commerçant que votre activité soit susceptible de vous procurer à l'individu des revenus suffisants pour vivre.

A titre d'exemple, dans une affaire du Tribunal de grande instance de Mulhouse, jugement correctionnel du 12 janvier 2006 (Ministère public c/ Marc W,) une procédure pénale avait été ouverte pour travail dissimulé par dissimulation d'activité, laquelle avait mené à une perquisition au domicile d'un certain Marc W., le 2 mai 2005.

Les enquêteurs y ont découvert de nombreux objets dont certains étaient mis en vente sur internet. Il a été établi qu'il avait vendu sur un site internet plus de 470 objets en deux ans. L'historique des trois derniers mois de ventes indique un montant de 6917,05 €.

Marc W. soutenait néanmoins qu'il était un particulier et non un professionnel. A l'audience, il a maintenu les mêmes arguments de défense et a plaidé la relaxe.

Le tribunal a, quant à lui, retenu que : *« Le caractère intentionnel de l'infraction résulte de la volonté de l'intéressé de se soustraire à la fois aux limites imposées aux non professionnels et aux règles encadrant l'activité des professionnels, et résultant notamment du code du travail. Marc W. reconnaît que le recours à ce site internet était un moyen de vendre mieux et davantage puisqu'il savait qu'un non professionnel ne pouvait effectuer ces opérations qu'une fois par an sur un marché aux puces. Il avait en outre, la conscience de pratiquer la même activité que des antiquaires. Il n'ignorait pas, pour connaître leurs usages, l'obligation d'immatriculation incombant à ces professionnels. Au surplus, le fait que le prévenu ait un emploi en Suisse et le caractère secondaire des revenus tirés de ces actes de commerce, sont sans effet sur la qualification pénale. Les éléments constitutifs de l'infraction n'exigent pas que l'activité à but lucratif soit exercée exclusivement ou principalement par le prévenu.*

Il n'existe aucune raison d'exclure le site internet de la réglementation qui est générale et ne comporte en l'état aucune exception en la matière ».

Par ailleurs, depuis une loi adoptée en 2008, Loi de modernisation de l'économie (dite LME), le fait de se présenter faussement comme un consommateur constitue une infraction sanctionnée d'une peine de deux ans d'emprisonnement au plus et d'une amende de 37 500 euros au plus ou de l'une de ces deux peines (article L. 121-1-1 21° du Code de la consommation).

La qualification de professionnel ne dépend pas d'un seuil de valeur ou d'un nombre d'objets vendus, mais plutôt d'un comportement. Il revient au vendeur de s'assurer qu'il n'est pas professionnel compte tenu, notamment, du caractère habituel de son activité.

MYTHE N° 6 :

QUAND JE CONSTATE UN DEBIT FRAUDULEUX EFFECTUE GRACE A MON NUMERO DE CARTE BANCAIRE, JE NE PEUX RIEN FAIRE A MOINS D'AVOIR SOUSCRIT UNE ASSURANCE SPECIFIQUE AUPRES DE MA BANQUE

Des personnes peuvent s'être procurés à votre insu votre numéro de carte bancaire, sa date de validité et son pictogramme. Si elles s'en servent pour régler des achats et que vous vous en apercevez, l'ordre de payer ne vous sera pas opposable si vous n'avez pas signé une facture ou composé votre code confidentiel à quatre chiffres sur le terminal du commerçant.

Dès lors, si vous constatez des prélèvements frauduleux sur votre relevé bancaire, il vous suffit de les contester par écrit auprès de votre banque et ce, avant l'expiration du délai légal de soixante-dix jours à compter de la date de l'opération contestée comme l'exige l'article L. 132-6 du Code monétaire et financier.

Dans ces conditions et à défaut de pouvoir produire votre signature, votre banque sera dans l'obligation de créditer votre compte, sans frais, des montants indûment prélevés dans le

délai d'un mois à compter de la réception de la contestation conformément à l'article L. 132-4 du Code monétaire et financier.

CONCLUSION :

Voici quelques uns des mythes et légendes qui existent sur l'e-commerce. Des idées reçues qui, régulièrement combattues par les organismes et entreprises présents sur ce marché, contribuent aujourd'hui à faire de l'e-commerce un secteur qui a connu, sur l'année 2010, une progression de 25 % du nombre des transactions en ligne en un an…malgré la crise.

MYTHES ET LEGENDES DE L'IMPUISSANCE DU JUGE FACE AUX RESEAUX

Jean-Claude Patin, JURITEL

A la question « parlez-vous le globish », je réponds toujours invariablement « oui, je suis sur internet ».

Si la formule est quelque peu provocante, elle a pourtant le mérite d'être claire : lorsque l'on est sur l'internet, on est partout, on comprend tout, on voit tout. Cette observation est régulièrement contestée par de nombreux internautes dès lors qu'il s'agit du rapport qu'ils entretiennent avec le monde du droit et de la loi. Asymétrie du raisonnement, méconnaissance, rumeurs, contresens, quelqu'en soient les motifs, l'internaute est souvent convaincu de son immunité relative ou absolue. Le postulat peut étonner mais il prend sa source dans l'un des nombreux mythes de l'internet : le juge et la justice sont dépassés par les nouvelles technologies des réseaux informatiques et télécom, prisonniers de leurs archaïsmes et de leurs frontières. Ce mythe s'exprime assez largement de quatre manières : la contrefaçon, la diffamation, l'effraction, l'ordre public.

MYTHE N° 1 : LE DROIT EST INSUFFISANT POUR LUTTER CONTRE LA CONTREFAÇON SUR INTERNET

La contrefaçon trouve sa définition dans la combinaison des dispositions des articles L121-1 et suivants du code de la propriété intellectuelle et de la jurisprudence. Les premières affaires de contrefaçon sur internet en France remontent à l'année 1996 où il fallut trancher d'aussi étranges questions que le droit de reproduire des paroles de chanson (affaire J.Brel) sur son site web ou d'user du nom de société pour son nom de domaine (Affaires Atlantel ou Framatome).

A l'époque et en coulisse, les jeunes techniciens échangeaient les bonnes informations pour user de cette liberté nouvelle qu'offrait le net, sûr que le juge ne comprendrait rien à leurs prouesses techniques tandis que les différentes lois entre les Etats les mettraient à l'abri des poursuites et qu'en tout état de cause ce juge pataud et maladroit irait trop lentement pour parvenir à finalement les faire condamner.

Ces raisonnements, largement construits sur une méconnaissance des mécanismes juridiques, ont contribué à l'élaboration d'une jurisprudence devenue au fil des ans plus abondante et plus riche, couronnée par des arrêts de principe rendus par la Cour de Cassation française (affaire Aurélien D notamment). La compétence du juge n'a pas connu de défaillance et lorsque les affaires étaient trop techniques, des forces de polices et des experts ont comblé les manques.

Les dernières affaires retentissantes de contrefaçon ont été tranchées en Juillet 2010 (Louis Vuitton c/ eBay) et les mécanismes de responsabilité du droit français ont joué leur rôle protecteur.

La lutte contre la contrefaçon dépend pour une part assez large de l'efficacité des systèmes juridiques. Au-delà des prouesses adulescentes de copie de fichiers vidéo ou musicaux, il faut avoir conscience des risques plus sérieux lorsqu'on aborde les contrefaçons de médicaments

ou de pièces détachées. Il faut souhaiter que nos systèmes juridiques et judiciaires s'améliorent afin de remplir convenablement leur office.

La limite actuelle des systèmes juridiques anti-contrefaçon se trouve essentiellement aujourd'hui dans les nouveaux dispositifs légaux (LCEN notamment), trop imprécis par certaines de leurs dispositions et ouvrant légalement la voie à une certaine impunité. Le règne des pirates en culotte courte s'achève, il faut désormais faire un peu de droit pour pirater en toute quiétude.

MYTHE N° 2 :
AU NOM DE LIBERTE D'EXPRESSION, LA DIFFAMATION N'EST PAS UN DELIT

La diffamation est un fait pénal relativement mal connu dans son mécanisme bien que pourtant souvent cité à tout propos par ceux qui se trouvent pris dans les rets du débat public. Prévue par l'article 29 de la loi de 1881 sur la presse, l'infraction de diffamation repose essentiellement sur l'intention de son auteur d'attenter à l'honneur ou à la considération de la personne visée. Elle se rencontre communément dans toutes les conversations, quel qu'en soit le sujet, quels qu'en soient les participants. Si le législateur s'est pourtant emparé de la question au sujet de la presse, c'est qu'un propos mal calibré livré au cours d'une conversation animée ne recèle pas le même danger lorsqu'il est imprimé – donc fixé – et par voie de conséquence accessible à un plus grand nombre et sur une plus longue période. La ruine d'une réputation, la destruction potentielle d'une vie, d'une famille, d'une institution apporte un désordre social que le législateur doit corriger en apportant une restriction à la liberté d'expression.

Cette liberté d'expression, si chère aux constituants de 1789, semble l'être encore plus à tous les adeptes pratiquants de l'internet. Suivant un raisonnement que n'aurait pas renié Karl Marx, la combinaison de la technologie numérique et la libre accession à l'information et à « la culture » permettrait enfin de pouvoir exercer pleinement cette liberté restée formelle avant l'avènement des réseaux internet. Ce double pari s'appuyant toujours invariablement sur la technique (rapidité de la diffusion, de la duplication, de la reproduction) pour soit échapper au juge soit le placer devant le fait accompli.

La diffamation sur internet se rencontre essentiellement dans les forums, les newsgroups, les « sites communautaires 2.0 ».

En France, on peut parler de matrice diffamatoire avec l'affaire dite « Altern » ou encore « Estelle Halliday » en 1998. Bien que traitant de la protection de la vie privée (article 9 du code civil français), cette affaire mis en lumière ce que la liberté de publication puis de parole (cf. les propos tenus pour justifier la mise en ligne puis pour critiquer l'ordonnance rendue par le TGI de Paris) pouvaient avoir de destructeur. La présentation d'un mannequin célèbre dans son plus simple appareil assorti de commentaires à vocation masturbatoire plantait le décor d'une controverse qui déborda bientôt le cadre de la diffamation pour atteindre celui du statut de l'hébergeur (encore mal résolu à ce jour).

Le web2.0 se développe assez largement sur le mythe de l'impuissance du juge sur internet, incapable de « censurer » la liberté d'expression ou seulement d'appliquer une loi plutôt qu'une autre.

Ce mythe se fracassa notamment en 2002 avec l'emblématique affaire « Père-Noël.fr » et le forum « défense-consommateur.org » qui vit les propos outranciers tenus censurés par le juge et son auteur sévèrement condamné. La technique du constat d'huissier avait facilement permis de surmonter la prétendue difficulté du numérique.

Reste que la diffamation a encore de beaux jours devant elle sur internet. La nécessité de supprimer toute contrainte dans l'expression de la parole rencontrant la nécessité de trouver des financements pour les sites 2.0 (par la publicité notamment et donc par la l'affichage de pages vues) fait peser une nouvelle menace sur l'application de ce régime injustement accusé d'être censeur alors qu'il n'est qu'un prolongement de l'article 11 de la Déclaration Universelle des Droits de l'Homme et du Citoyen de 1789.

6° PARTIE : ASPECTS METIERS

MYTHES ET LEGENDES SUR LES HACKERS

Mauro Israel, Expert sécurité BIOOS

Eh oui, il faut bien l'admettre : je suis un hacker ! Mais qu'est ce que ça veut dire au juste ? Est-ce mal ? Est-ce illégal ?

MYTHE N° 1 :
LES HACKERS SONT DES DELINQUANTS…

Non, les hackers sont en fait des esprits curieux

Revenons à la source : Dans les années 60, un groupe d'ingénieurs du MIT (Massachusetts Institute of Technology) de Boston désigne ainsi les personnes qui essaient de « hacker » c'est-à-dire « d'analyser » (ce qui vient du grec « découper en plus petites parties ») un système complexe. L'idée du hacker est de comprendre le fonctionnement d'un système – dans ce cas informatique-afin d'en repérer les failles et autres dysfonctionnements.

La *Request for Comments* RFC 1392 (les RFC sont les règles écrites d'Internet) décrit même le hacker comme «*[une] personne qui se plaît à avoir une connaissance intime du fonctionnement interne d'un système, les ordinateurs et les réseaux informatiques en particulier.* »

Aujourd'hui, l'usage courant du mot «hacker» se réfère principalement à des cyber-délinquants dû à une déformation de ce terme de la part des médias. Pour faire de l'audience ou du tirage, les « exploits » des hackers –ainsi nommés parce que les failles du système « cible » sont divulguées-sont relatés dans la presse, voire à la télévision.

Il y a également différents types de hackers, par exemple les «*script kiddies*», qui sont en général des adolescents utilisant des programmes de hacking trouvés sur Internet, avec en fait très peu de connaissances sur le sujet. Un peu comme des « apprentis sorciers » qui utiliseraient une formule magique sans la comprendre…

Il y a également des variantes liées au positionnement éthique du hacker suivant qu'il respecte la loi ou pas: Le « *Black Hat* » est un hacker « du côté obscur de la Force » c'est-à-dire qu'il effectue des intrusions dans un système sans l'accord de l'intéressé. Le « *White Hat* » est au contraire un « hacker éthique » c'est à dire **qu'il intervient à la demande explicite de l'intéressé notamment sous forme de « tests d'intrusion »** qui consistent à vérifier la résistance d'un système vis-à-vis des meilleures techniques de hacking du moment. Cette approche volontariste et pragmatique permet de colmater les brèches de sécurité sans perdre de temps dans des analyses de risque, puisque la menace est avérée et formalisée : *« que peut faire un hacker depuis internet de dommageable à mon système et comment y remédier ? »*. Une variante de ces tests d'intrusion permet également de vérifier la résistance du système depuis l'intérieur, par exemple par la tentative d'intrusion d'un informaticien, mais ceci est une autre histoire… On raconte que les termes *« Black Hat »* et *« White Hat »* proviennent du feuilleton en noir et blanc *« Eliott Ness »* où les « gentils » avaient des chapeaux blancs et les « méchants » des chapeaux noirs, afin que le téléspectateur puisse les distinguer notamment dans les scènes de fusillade ! Il existe également une population de hackers intermédiaire dite « Grey Hat », qui tantôt effectue des actions d'intrusion illégales, tantôt des actions commanditées.

Ne me demandez pas dans quelle catégorie je me situe ! En fait si on reprend le jargon naval, les « pirates » des uns étaient les « corsaires » des autres et inversement… Tout est donc une

question de point de vue et de respect de la Loi. Mais est-ce éthique ou non de contourner les filtres d'un système d'information d'un dictateur afin de montrer au monde ses exactions ? De Gaulle était considéré comme un « terroriste » par le régime de Vichy… **Pour moi un hacker doit agir avant tout dans l'intérêt de la vérité et contre l'hypocrisie d'une fausse sécurité étayée par des affirmations gratuites et non démontrées.**

Mon premier hacking a été relaté dans beaucoup de medias y compris à la télévision. Je m'étais rendu compte alors que les 3614, 3615, 3616 du Minitel étaient des PAD accessibles directement par leur numéro. Comme j'habitais dans le « 92 », j'ai essayé « 192000001 »… Et je tombe sur la page d'accueil d'une base de données EDF. Le système était sous GCOS 6 – que j'avais appris à l'Armée quelques mois auparavant-et me demandait tout simplement un login-mot de passe. Avec le Minitel inutile de vous dire que c'était un peu lent d'essayer des millions de mots de passe, donc je commence avec une lettre, et je tape « A » puisque c'était le début de l'alphabet… C'était le bon mot de passe !!! J'ai vu défiler tous les « *little links* » de la base de données, en fait les comptes de tous les clients EDF !

J'en ai alors parlé à quelques ingénieurs du « *Solex Crack Band* », dénommé ainsi puisque nous travaillions pour les carburateurs Solex à essayer de mettre au point le « carburateur idéal » avec les premiers micro-ordinateurs… A l'époque le terme de « hacker » n'existait pas, alors nous étions plutôt des « *crackers* » (des casseurs) ou des « *phreakers* », le « ph » début de « *phone* » étant lié au craquage des systèmes téléphoniques et notamment des cabines (essentiellement pour ne pas payer l'accès à l'international). Notre « vocation » provenait du film « *Wargames* » où un adolescent compose tous les numéros de téléphone pour finir par pénétrer par hasard dans l'ordinateur du Pentagone qui simule une guerre nucléaire…

Visiblement l'un d'entre nous en a parlé à quelqu'un, qui connaissait quelqu'un, qui connaissait… un journaliste, puisqu'au final Paris-Match a fait un article, puis la télévision (le « France Télévisions » de l'époque) est venue tourner un double reportage : « D'un côté on voyait un Minitel qui défilait tous les comptes EDF des clients (floutés), et de l'autre la réaction de l'hébergeur –*Telesystemes*-qui dans un premier temps prend cela à la rigolade et dit que « c'est impossible », puis blêmit et finalement demande l'arrestation des ces « délinquants pubères» ! Un grand moment de télévision ;) Heureusement que nos visages étaient floutés et que les journalistes n'ont pas divulgué nos adresses…

Encore faudrait-il qu'il y ait eu « délit » : en effet la Loi Godfrain qui institue le crime informatique « *intrusion ou tentative d'intrusion dans un système de traitement de données* » ne date que de 1985… **Avant cette date les hackers n'étaient pas juridiquement des délinquants.**

Est-ce que éthiquement c'est mal de dénoncer une faille patente d'un système d'information ? Si on en croît la Loi et les jugements issus des affaires de hacking en France, j'en déduis qu'au contraire **c'est faire preuve de civisme**. Par exemple dans l'affaire KITETOA contre TATI, le hacker a été relaxé parce que TATI et son hébergeur **n'avaient pas suffisamment protégé leur système** et notamment les données de leurs clients. Il suffisait d'utiliser un simple navigateur pour le prouver, en ajoutant à la fin de l'URL l'accès à une métadonnée comme « :$DATA » ; Par exemple : *http://www.tati.fr:$data*

Cette simple commande était accessible à n'importe qui sans outil spécialisé de piratage, ce qui permettait de visualiser l'intégralité de la base de données clients… Cette faille était bien connue à l'époque et cet « exploit » était à la portée de n'importe quel curieux du fonctionnement d'Internet. Le problème c'est que « KITETOA » l'a publié sur son site (en masquant les coordonnées des clients) et s'est ainsi attiré les foudres de TATI et de la justice.

Cet exemple montre bien la problématique du « *full disclosure* » autrement dit : doit-on exposer les failles de sécurité sur internet ou dans les medias ? Serge Humpich en sait quelque chose lorsqu'il a voulu dénoncer les failles de l'algorithme B0' de la carte bancaire… Garde à vue, saisie de ses ordinateurs, prison avec sursis… ça ne donne pas envie de s'exposer ! Et pourtant les hackers ne peuvent pas s'en empêcher, ça fait partie du personnage : **il s'agit d'une envie irrépressible de montrer qu'on a trouvé une faille**. Plus la faille est grosse et plus elle touche une entité « respectable », plus la jouissance est forte !

MYTHE N° 2 :
LES HACKERS SONT BIEN DES DELINQUANTS…

La réalité est que les mises en garde des hackers ne sont pas écoutées

Voici un exemple qui illustre bien ce phénomène et aussi les réactions incroyables des institutions concernées : Deux hackers Italiens – Andrea Barisani et Daniele Bianco …. ont montré en 2007 comment avec quelques euros de matériel radio on pouvait injecter du trafic TMC-RDS dans les GPS des voitures, et **créer ainsi potentiellement un désordre total en annonçant des fausses nouvelles** et éventuellement en détournant le trafic ou bien en créant la panique en indiquant un attentat ou un crash aérien…

La démonstration était ponctuée de clips vidéo, où l'on voyait, en vrai, nos deux acolytes l'un au volant de sa voiture, et l'autre en train de lui envoyer de faux messages à travers le récepteur RDS. A un moment, il y avait une annonce de « *combat de taureaux* », pour bien montrer que cette annonce était complètement farfelue et erronée !

Ce qui pose problème, est que **n'importe qui capable d'émettre un signal radio, est capable d'injecter ces informations sur les GPS embarqués des voitures**, et que l'on peut également imaginer injecter d'autres informations dans cette même voiture puisque le « bus » est commun à plusieurs fonctions dont le GPS.

Croyez-vous que les autorités compétentes (à Genève) ont rectifié ou crypté ou protégé les communications TMC ? Pas du tout ! Andréa m'a montré la lettre de réponse de TMC suite à leur missive qui leur exposait le problème avant même que celui-ci ne soit divulgué… Ils ont balayé leurs arguments de dangerosité en estimant que « *personne ne le fera puisque… c'est illégal* » !!!

On imagine alors **des terroristes en train de polluer les informations du trafic TMC pour amplifier les effets d'un attentat en désorganisant les secours** par des embouteillages monstres… Vous pensez qu'il s'agit d'un délire paranoïaque ? Au moment où j'écris ces lignes, plus de trois ans après la divulgation de la faille, rien n'a été modifié : Pourquoi prendre ce risque insensé ? Pourquoi ne pas en parler dans les medias pour faire réagir les autorités ?

Richard Clarke – ex conseiller spécial à la sécurité à la Maison Blanche des présidents Clinton et Bush – complète bien cela. Les menaces pesant sur le cyberespace ne sont pas évaluées correctement par les gouvernements actuels : *« **they did not get it** » -Ils n'ont pas pigé…*

En fait, ni les gouvernements, ni les entreprises n'évaluent correctement les risques informatiques et comptent sur la chance de n'être pas visés par une attaque : « *on n'a rien de confidentiel chez nous* », ou bien cherchent à étouffer ou à décrédibiliser l'information de la faille avérée.

Un exemple patent est celui de HSBC à Genève. Un informaticien dénommé Hervé FALCIANI, par une simple commande SQL SELECT, en tant qu'administrateur système, « pompe » le fichier des clients de la banque. Ce qui se passe ensuite est confus (tentative de

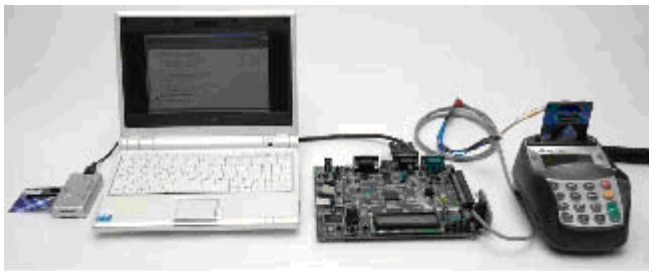
revente du fichier, saisie par le fisc Français ?) mais il est clair que le fichier des clients d'une banque où le secret est la base même du métier s'est fait pirater en quelques minutes ! Il y a visiblement un défaut majeur de protection ! Est-ce que les autres banques se sont intéressées au problème ? *« Est-ce possible chez nous ?, Comment se protéger de ce type de consultation par les administrateurs informatiques qui ont tous les droits sur les fichiers ?».* En vérité, **la plupart des entreprises et administrations « jouent les autruches »** ou bien affirment de manière péremptoire que « *ce n'est pas réalisable chez nous parce que nos moyens de sécurisation sont bien meilleurs…*»

MYTHE N° 3 :
LES HACKERS SONT TOUJOURS DES DELINQUANTS…

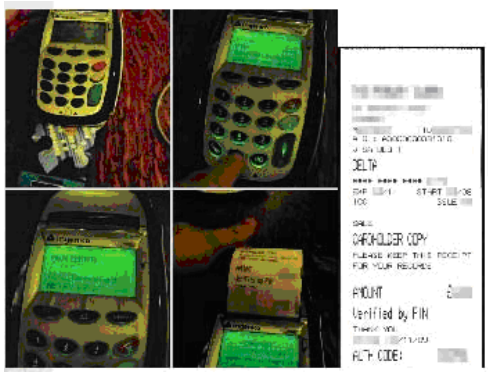
La réalité est que les entreprises –en particulier les banques- cherchent à minimiser et à relativiser toute information sur la facilité avec laquelle on peut les pirater

Un autre exemple, qui nous touche tous, est celui, récent, de la faille de sécurité sur les cartes bancaires à puce. Pas les anciennes B zéro', les nouvelles ! Cela fait plusieurs mois que des chercheurs de l'Université de Cambridge ont démontré que l'on pouvait avec un matériel basique – un PC portable, un lecteur de cartes, un terminal de paiement, un peu d'électronique-fabriquer un système *« Man in the middle »* qui permet de taper n'importe quel code et obtenir une transaction validée de type *« YES CARD »* (pourvu que la transaction ne déclenche pas d'appel au central) :

Voici le matériel utilisé et la séquence modifiée par l'insertion d'un PIN code « forcé » :



Et la preuve de la transaction sous forme de ticket de caisse valide :



En exposant ces faits à la conférence CARDS 2010 à Rome je me suis attiré les remarques acides suivantes : *« Il ne faut pas parler de choses mauvaises sur les cartes à puce au moment même où les banques Italiennes envisagent de passer à la carte à puce »*, ou bien *« En vrai, ce n'est pas réalisable car les hackers se feraient repérer dans une boutique avec ce matériel… »* ou alors *« Les cartes de notre banque ne sont pas affectées par cette faille ».* Toutes ces affirmations sont fausses : Primo, une banque ne va pas adopter un nouveau système sans un minimum de vérifications, donc les banques Italiennes vont corréler ces informations avant de prendre une décision. Ce rapport se trouve

sur Internet depuis mai 2010, donc quelqu'un aurait de toute manière fini par le remonter. Aujourd'hui on peut difficilement dissimuler une information il y aura un jour ou l'autre une fuite, un *« leak »*, pardon un *« wikileaks »* !

Deuxio, si le commerçant est complice « passif » et fournit le terminal de paiement le fraudeur aura tout loisir de le faire… Ah bon, vous affirmez contrôler et tracer les terminaux de millions de commerçants dans le monde, notamment en Amérique du Sud, en Asie et en Afrique ?!

Tertio, l'exploit a été réalisé avec une carte à puce d'une banque Française et un terminal Français, les deux totalement à jour au niveau du *firmware*. Pour des raisons de standardisation il est peu probable que certaines cartes soient affectées et d'autres pas, en tous les cas cela doit être vérifié.

Le véritable problème soulevé par le hacker n'est donc pas l'exploit proprement dit, voire même sa légalité, mais le fait de le divulguer sur Internet et les medias: le *« full disclosure »*.

MYTHE N° 4 :

LES SYSTEMES ACTUELS SONT PARFAITEMENT SECURISES, MEME SI CERTAINS HACKERS DELINQUANTS (ET MYTHOMANES) CHERCHENT A NOUS FAIRE CROIRE LE CONTRAIRE…

Les failles de sécurité sont béantes et les dirigeants s'en fichent : « business first » !

L'histoire de « Hacker-Croll » est une illustration de la sous-estimation des problèmes de sécurité par nos dirigeants.

« Un pirate informatique français de 25 ans, qui était en mesure de contrôler le réseau social Twitter, a été interpellé mardi dans le Puy-de-Dôme au terme d'une enquête franco-américaine de plusieurs mois. "Hacker-croll", selon son surnom, était parvenu à obtenir les "codes administrateurs" de Twitter et pouvait y naviguer à l'aise, en créant et supprimant des comptes. Il avait notamment piraté un compte Twitter au nom de Barack Obama. Il a été libéré mercredi soir à l'issue de sa garde à vue.

Ce pirate sévissait aussi sur le réseau social Facebook ou des messageries électroniques telles que G-mail.

Quand Obama se fait pirater son compte Twitter...

Twitter, Barack Obama, Britney Spears, hacker, Web, Faits-divers

Info publiée par la rédaction du Post

Par La rédaction du Post
le 25/03/2010 à 09:07, vu 15656 fois, 20

Montage Le Post

On ne rigole pas avec les données informatiques de l'homme le plus influent du monde.

Pour avoir piraté le compte Twitter de Barack Obama, un jeune Auvergnat de 25 ans risque maintenant 2 ans de prison.

Le hacker en herbe a aussi réussi à pirater le compte de la chanteuse Britney Spears et ceux d'autres personnalités non révélés. Plusieurs centaines, précise *RTL*, car le pirate avait réussi à devenir administrateur du réseau de microblogging. Et récupérer au passage des coordonnées bancaires, dont il n'aurait a priori pas fait

Ce pirate informatique sans profession avait créé son propre blog pour faire partager ses trouvailles. Il était déjà connu pour des faits d'escroqueries sur internet, de « petites escroqueries qui lui avaient rapporté 15.000 euros ». En revanche, il n'a "jamais tenté de monnayer ni tirer un profit quelconque" du piratage de Twitter. " source – La redaction du POST".

On se demande lequel des deux piratages était le plus grave – celui du Président des Etats-Unis ou celui de la « chanteuse »- pour motiver l'intervention musclée et combinée de la

gendarmerie et du FBI au petit matin dans la chambre que ce jeune homme occupe chez sa maman dans les environs de Clermont-Ferrand…

Qu'a-t-il donc fait de si mal ? Comment quelqu'un en plein cœur de la France avec un simple ordinateur connecté à internet peut-il s'introduire dans la base de données d'un des sites les plus connus au monde et certainement des plus sécurisés ? Je vais vous le révéler dans les lignes qui suivent : en fait c'est à la portée de n'importe qui et il suffisait juste d'y penser.

Au moment où j'écris ces lignes la faille n'est bien entendu toujours pas été corrigée… **Il n'y a pas besoin de compétences informatiques particulières, juste du bon sens**. On appelle cette « technique » le *Google hacking,* c'est-à-dire s'aider de Google pour aider à analyser les failles d'un système.

Tapez par exemple :

On obtient la liste de tous les députés qui ont une boite email à la « poste.net »

Ensuite on va sur le site de l'Assemblée Nationale pour obtenir toutes sortes d'infos sur notre « cible », par exemple sa date de naissance ou sa ville de naissance.

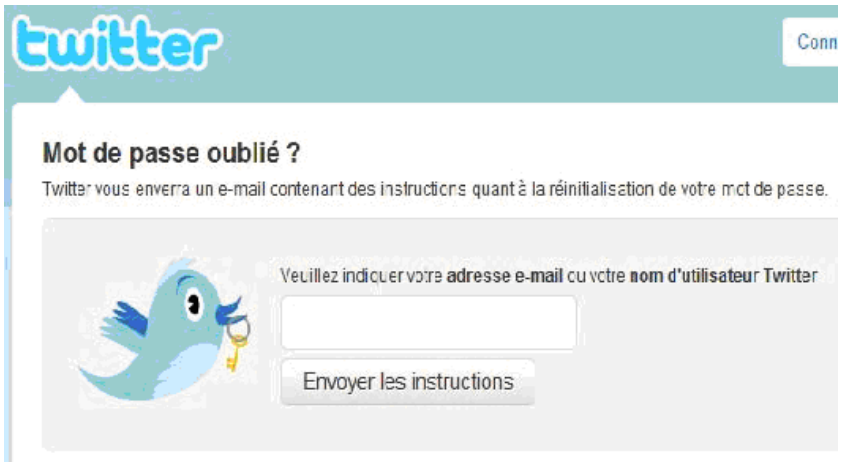
On se rend ensuite sur le site de la « poste.net ». Vous noterez au passage que le site est en « http », c'est-à-dire que le mot de passe circule en clair. Vous noterez aussi qu'en aucun cas il y a piratage, puisque ces infos sont disponibles de n'importe où avec Google. De plus, si vous vous connectez dans un lieu public, par exemple en wifi, votre login et mot de passe sont interceptables par n'importe qui. Gardez ceci en mémoire pour comprendre un autre hacking exposé plus bas.

BSSID	Last seen	Vendor	Signal	SSID	Enc	Mode
000352F432E0	22/01/2009 - 11...	Colubris Net...	-80 dBm	Neuf WiFi	No	Infrastructure
000352E09560	22/01/2009 - 11...	Colubris Net...	-82 dBm	Adael-Gratuit	No	Infrastructure
0016B601750E	22/01/2009 - 11...	Cisco-Linksys	-90 dBm	wirelessAP	Yes	Infrastructure
5EA6FB67F7C8	22/01/2009 - 11...		-90 dBm	freeboxdam	Yes	Infrastructure
5EA6FB67F7C9	22/01/2009 - 11...		-90 dBm		Yes	Infrastructure
5EA6FB67F7CA	22/01/2009 - 11...		-90 dBm		Yes	Infrastructure
0021863E1724	22/01/2009 - 11...		-84 dBm	Livebox-1d6d	Yes	Infrastructure
0003C9435F6B	22/01/2009 - 11...	TECOM Co....	-90 dBm	Wanadoo_c094	Yes	Infrastructure
4AC26158E591	22/01/2009 - 11...		-89 dBm		Yes	Infrastructure
4AC26158E590	22/01/2009 - 11...		-90 dBm	Pidmo	Yes	Infrastructure
000352F432E1	22/01/2009 - 11...	Colubris Net...	-77 dBm		Yes	Infrastructure
020508F70EFC	22/01/2009 - 11...		-92 dBm	print server 0EA...	No	Peer
5EA6FB67F7CB	22/01/2009 - 11...		-90 dBm	freephonie	Yes	Infrastructure

La clé de voute de ce hacking est la compréhension du système des « mots de passe oubliés ». Que se passe-t-il si notre député à oublié son mot de passe ? Il clique sur la boite de dialogue « mot de passe oublié » :

Dans de nombreux cas, y compris Twitter, ce mot de passe est expédié… à une boite aux lettres électronique. Hacker-Croll a donc piraté la boite mail d'un des administrateurs de Twitter ce qui lui a permis de réinitialiser le mot de passe et donc d'accéder à tous les messages de l'administrateur en question et donc de lui dérober tous les mots de passe de tous les sites qui vous envoient un email pour renouveler votre « mot de passe oublié », c'est-à-dire la quasi-totalité des sites, y compris certaines banques….

La clef de voute du système est donc l'accès à la boite mail de la « cible ». Mais alors comment réinitialiser un mot de passe d'une boite mail puisque l'on y a plus accès ? C'est alors que rentre en compte une autre méthode, celle de la *« challenge phrase »*. On vous pose une ou plusieurs questions personnelles auxquelles vous avez préalablement donné la réponse lors de votre enrôlement. Et savez-vous quelle était la *challenge phrase* choisie par l'administrateur de Twitter ? *« Quelle est la ville de naissance de votre mère ? »*. D'où l'intérêt de « votre ami Google » ci-dessus ! De nombreuses personnes choisissent des questions triviales (date de naissance) ou mettent des réponses que l'on peut trouver dans Google, sur les réseaux sociaux etc… **Cela a été le cas pour deux députés Français** qui utilisent des messageries publiques en plus de la messagerie de l'Assemblée Nationale. Ils n'utilisent pas de pseudo ce qui fait que leur nom indique leur email… Leur boite aux lettres a été piratée et leur mot de passe réinitialisé. Des réactions dans les medias ? Aucune ou presque. Des améliorations de la sécurité ? Pas que je sache.



Est-ce une intrusion dans un système de données ? Est-ce un délit ? L'utilisation d'un simple navigateur et l'utilisation du moteur de recherche le plus répandu sur la planète indique plutôt qu'on a réussi un hold-up avec un pistolet à eau… Et encore, on n'a même pas la forme d'un pistolet, disons, avec juste un téléphone portable… Il vaudrait mieux sécuriser l'accès à la messagerie de la Poste à laquelle font confiance des millions de Français, plutôt que de « tuer le messager de la mauvaise nouvelle ». C'est toute la problématique du hacker. Lorsqu'il se vante de son exploit, la seule réponse des autorités c'est de lui envoyer la police et de l'embastiller.

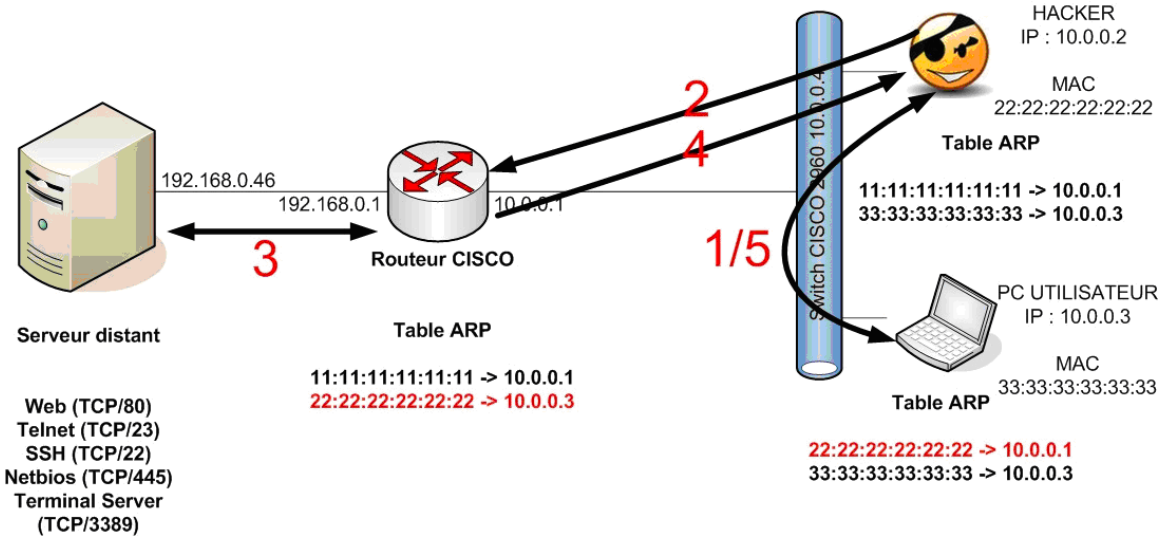
MYTHE N° 5 :
LES HACKERS SONT DEFINITIVEMENT DES DELINQUANTS…

Les hackers sont en fait des « messagers de mauvaises nouvelles »

Un autre exemple vient de ma propre expérience à la Black Hat 2008. Tous les ans aux USA depuis près de 25 ans, les hackers du monde entier se réunissent, comparent leurs exploits et apprennent de ceux des autres. Les plus grandes agences américaines comme la CIA, le FBI ou la NSA participent et cherchent même à recruter les meilleurs hackers. Les medias couvrent l'évènement qui a lieu notamment à Las Vegas. En 2008 donc je participe au challenge du *« wall of sheep »* qui consiste à épingler sur un mur électronique, visible des congressistes, les pseudos et mots de passe des participants qui utilisent des mots de passe en clair dans leurs connexions. Dans une conférence sur les meilleures pratiques d'attaque et de sécurité, c'est la moindre des choses que de se comporter en donnant l'exemple…

Les journalistes, dont je faisais partie pour un magazine de sécurité bien connu, avaient été dûment prévenus par un email quelques jours avant, du challenge et **clairement instruits de ne pas se connecter en clair**. (donc utiliser *https* au lieu de *http*). Mon esprit curieux de

hacker m'a poussé à vérifier cela dans la salle de presse… Et là je m'aperçois que de nombreux journalistes se connectent au back office de leur journal –en mode administrateur qui plus est-sans aucune précaution de chiffrement. Je récupère en quelques minutes des dizaines de mots de passe qui me permettraient de me connecter aux bases d'articles des plus grands medias américains… J'en vérifie au hasard deux, notamment celui de CNET. Je me connecte avec un simple navigateur et je vois défiler tous les articles du magazine ainsi que les archives, la possibilité de modifier ou d'effacer des articles…



Pour cela j'ai utilisé la technique du *« man in the middle »* qui permet d'intercepter les flux wifi ou réseau et de lire le contenu des paquets qui circulent sur un réseau. Il faut bien comprendre qu'il n'y à aucun génie là-dedans. Il suffit d'avoir un logiciel en téléchargement libre sur Internet et une carte wifi ou réseau. Autrement dit, dans n'importe quel lieu public, aéroport, gare, restaurant, café etc… quelqu'un peut « renifler » vos flux wifi pourvu que ceux-ci soient en clair (http), comme on écouterait la conversation de quelqu'un qui parlerait fort….

Muni de ces éléments je me présente au *« wall of sheep »* -le mur des moutons- pour leur faire part de ma découverte et pour qu'ils publient les pseudos (avec les mots de passe partiellement cachés pour montrer qu'on les a, mais pour empêcher qu'on les utilise). Il y avait des centaines de noms déjà affichés (le hacker Dan Kaminski le célèbre découvreur de la faille DNS en faisait partie…). Les organisateurs du challenge vérifient sur mon ordinateur, sont amusés, mais m'expliquent gentiment **qu'on ne publiera pas ces pseudos là car la presse est sponsor de l'évènement !**

Un photographe prend une photo de mon écran à mon insu à ce moment là et publie les pseudos et mots de passe sur internet !!!

La journaliste de CNET est prévenue ensuite comme « victime » de ce piratage et demande immédiatement à l'organisation de la Black Hat de nous exclure. Ceci dit elle utilisait le login d'un homme, qui plus est le directeur de la rédaction, qui plus est administrateur de la base complète du journal… Ce qui est une fois de plus démontre le fait de « tuer le messager » au lieu de reconnaître son propre comportement laxiste et dangereux. Ce qui est incroyable c'est que les media américains puis mondiaux se sont emparés de l'affaire, et nos noms, qui avaient été divulgués par l'organisation avec nos badges, défilaient en boucle sur CNN : *« three french journalists have been expelled from Black Hat conference… »*. Des dizaines d'agences de presse ou des media appelaient sur nos téléphones portables (dont le numéro à priori privé et

confidentiel avait été également dûment divulgué par l'organisation…). **Tout d'un coup notre séjour s'est transformé en enfer**. Quand je dis « nous » c'est parce que par amalgame mes deux collègues ont été inquiétés, alors qu'ils ne savaient même pas de quoi il en retournait !

Après une pression énorme de la part des organisateurs qui nous sommaient de tenir une conférence de presse pour nous expliquer (oh le joli coup de pub sans dépenser un centime !), ainsi que des délires de journalistes qui nous ont traités «d'espions» sans aucune référence, ni vérification des faits, nous avons finalement quitté les USA deux semaines de vacances plus tard, sans être inquiétés le moins du monde. Pourquoi cela ? Parce que d'autres media « alternatifs » comme « Wired » ont commencé à soutenir les « hackers » (c'est-à-dire nous) en expliquant que c'était une honte qu'une journaliste qui couvre un évènement de sécurité, qui plus est qui réunit près de 5000 hackers, ne prenne aucune précaution pour se connecter à son journal… **Donc que son comportement irresponsable exposait la sécurité de ses sources et permettrait à des intrus de rentrer dans le système d'information d'un des plus grands media américain…** De même l'autre journaliste qui avait été « piraté » à publié un article faisant son « mea culpa » en expliquant qu'il se connectait avant en « https » mais qu'il avait laissé tomber pour des questions de compatibilité sur certains points d'accès (le certificat était obsolète).

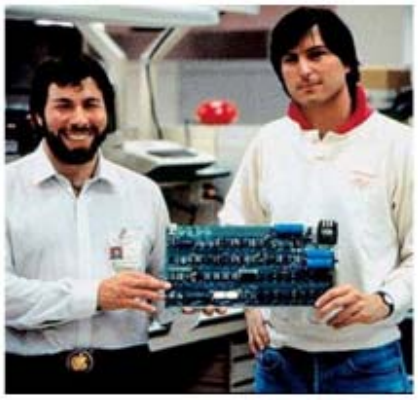
Au final, à part en France-où nous avons été laminés par des journaleux jaloux et donneurs de leçons, l'expérience a été positive et mon esprit « hacker » en a été renforcé. Oui, hacker est un état d'esprit voire un mode de vie.

MYTHE N° 6 :
LES HACKERS SONT DES DELINQUANTS QUI N'ONT AUCUN CONTACT AVEC LA VIE REELLE (DES « NO LIFE »)

Non, les hackers sont bien intégrés dans la vie réelle et organisés en « tribus du monde libre»…

Les hackers sont organisés en « tribus », comme un mouvement alternatif. D'ailleurs le monde du logiciel libre est directement lié aux hackers, et des personnages comme Steve Jobs, Steve Wozniak « Woz », et même Bill Gates ont commencé comme hackers avant de créer l'industrie des ordinateurs personnels.


Philip Zimmermann


Steve Wozniak


et Steve Jobs Bill Gates

D'autres se sont directement opposés au système du logiciel payant comme mon ami Phil Zimmermann, qui a publié un logiciel de chiffrement PGP *« Pretty Good Privacy »* qui enfreignait la limite de taille de clef fixée par le gouvernement Américain et qui surtout le

diffusait gratuitement aux internautes. Presque tous –de ma génération-sont « rentrés dans le rang » en vendant leur logiciel à de grands éditeurs, ou en faisant fortune comme pour Apple ou Microsoft.

MYTHE N° 7 :
LES HACKERS SONT TOUS DES GENIES DE L'INFORMATIQUE

En fait le maillon faible de tous les systèmes de sécurité est l'être humain, qui ne nécessite aucun génie pour le duper…

Le plus célèbre des hackers Kevin Mitnick –non pas uniquement par ses exploits, mais surtout par les 170 années de prison auxquelles il a été condamné, les peines aux USA étant cumulables-est aujourd'hui consultant en sécurité –libéré sous caution-et a commis deux livres qui expliquent le *« social engineering »*. Comme il explique dans *« The art of deception »* (l'art de la manipulation) Il s'agit d'utiliser la ruse pour persuader un utilisateur de lui donner son mot de passe.

Tout commence avec un repas au restaurant à Washington, où, par hasard, il est assis à côté de la belle Alice, secrétaire du patron du FBI qui lui fait face. Il entend juste *« Alice je vais aller aux iles Grenadines à l'hotel habituel la semaine prochaine »*… La semaine suivante, il demande à parler au directeur du FBI au téléphone et après moult barrages franchis (dans son livre il explique comment) il parvient non pas au Directeur –puisqu'il n'est pas là-mais à sa secrétaire, ce qui était en fait son véritable but. En utilisant un truqueur de voix, il dit à Alice : *« C'est Bob, je suis aux Grenadines et je n'arrive pas à me connecter à mon f… e-mail ». « Le mot de passe à changé ou quoi ?!! »*. Et là Alice qui ferait tout pour que son patron Bob ne s'énerve pas plus, lui « redonne » le mot de passe… En fait lui « donne », puisque c'est Kevin Mitnick et non le patron du FBI à l'autre bout du téléphone !

Mitnick se connecte alors à la messagerie du FBI, lit tous les emails et commence une incroyable farce qui va durer plusieurs années où il imite le style et les textes de différents contacts de cette personne et où il obtient au final l'accès à la plupart des sites et messageries sensibles américains, comme la CIA, la NSA ou le Pentagone au total 17 sites. (Ce qui explique les 170 ans de prison requis: 17 x 10 ans, peine maximum pour le piratage aux USA). En utilisant des systèmes de proxy anonymes il masque sa véritable adresse IP en la changeant toutes les 10 secondes (voir le réseau TOR pour cela). Alors qu'il n'habite pas très loin de la Maison Blanche, la CIA le recherche partout dans le monde… C'est finalement un autre hacker –un japonais-émoustillé par la prime de plusieurs millions de dollars, ou par désir de vengeance personnelle, qui finira par l'attirer dans un faux site –un *honey pot*, site «

pot de miel »-et remontera à son adresse IP d'origine… La suite est comme dans les feuilletons à la télé : des dizaines de policiers armés jusqu'aux dents défoncent la porte et dans une débauche de gaz lacrymogènes et d'aboiements d'ordres brutaux arrêtent le sieur Kevin…

C'est à ce moment que l'on comprend mieux la notion de « tribu de hackers ». Après son arrestation, la caution a été fixée à 1 million de dollars, une somme évidemment impossible à payer pour un quidam. Sur internet –avec Paypal-des milliers de hackers on donné 10 ou 20 dollars, et la caution a été réunie et payée en quelques mois, et Kevin libéré !

Le même cas s'est produit récemment en France avec le hacker « Guillermito » qui avait démontré des failles patentes dans le logiciel anti-virus *« V-Guard »* de TEGAM, mais qui avait été condamné à plusieurs milliers d'euros d'amende pour « contrefaçon » et avait entraîné indirectement la disparition de cet éditeur en publiant ses résultats sur internet. Comme aux USA des centaines de hackers solidaires se sont cotisés, car cet enseignant en biologie à Harvard n'avait évidemment pas les moyens de payer une telle somme…

MYTHE N° 8 :
LES HACKERS N'ONT QU'UN PAUVRE PC POUR EFFECTUER LEURS EXPLOITS DEPUIS LEUR CHAMBRE.

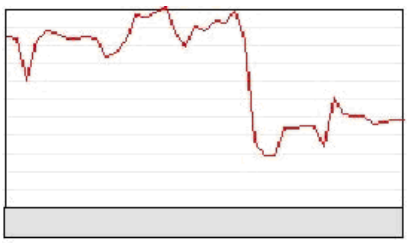
En fait, les hackers disposent de l'ordinateur le plus puissant au monde…

Une nouvelle génération de hackers à remplacé l'ancienne : cette génération là, est très technique et dispose de moyens informatiques sans précédent : Quel est l'ordinateur le plus puissant du monde ? Celui du Pentagone ? Celui des Russes ? Des Chinois ? Non, celui des hackers !!!

1 Tianhe-1A – (Chine) 2 Jaguar -Cray 3 Nebulae -Dawning TC3600 4 TSUBAME 2.0 5 Hopper -Cray XE6 6 Tera-100 -Bull 7 Roadrunner -BladeCenter 8 Kraken XT5 -Cray 9 JUGENE -Blue Gene/P Solution 10 Cielo -Cray XE6 8 *(10 ordinateurs les plus puissants au monde – source top500.org – janvier 2011)*

Tous ces ordinateurs ont un point commun : ils sont basés sur des microprocesseurs du commerce (Xeon Intel ou Cray) mais montés de manière massivement parallèle. Un système de refroidissement liquide permet « d'empiler » les processeurs et de dissiper la gigantesque chaleur générée. La vitesse est mesurée en Teraflops (mille milliards d'instructions par seconde) voire en PetaFlops (1000 Tflops). Ces calculateurs servent surtout aux simulations et aux cassage d'algorithmes de chiffrement de manière à ce qu'un pays dispose d'un outil pour voir « en clair » ce qui transite comme information chez lui.

L'idée des hackers est la même : casser les algorithmes de chiffrement afin de lire les flux cryptés.



Stats

Active machines	1333
Online machines	834
Current CPU power	4786 GIOPS
Last 24 hours	3788 million chains
Current speed	2.63 bil links/second
Data growth	63.5 GB
Cracked hashes	291197
MD5	270016
NTLM	11715
LM	8808
SHA1	658
Uncracked hashes	226809
MD5	198058
NTLM	16825
LM	9144
SHA1	2782
Success rate	56.21%
MD5	57.69%
NTLM	41.05%
LM	49.06%
SHA1	19.13%
Last password cracked	lyafxdtm

Grâce à Internet on peut regrouper des centaines de milliers, voire des millions d'ordinateurs à travers le réseau en leur faisant effectuer à chacun une part minuscule du travail en tâche de fond, sans même que l'utilisateur de l'ordinateur en soit affecté. En effet, le CPU d'un ordinateur est utilisé à quelques % de ses possibilités, un peu comme notre cerveau…

De là est né le projet BOINC *(Berkeley Open Infrastructure for Network Computing)*,à l'université de Berkeley. Il s'agit d'installer un programme en tâche de fond sur son ordinateur et celui-ci va procéder à des calculs de décodage scientifique ou autres… Ce programme est largement utilisé par la communauté scientifique pour, par exemple, le décodage du génome humain ou bien la tentative de décodage des bruits radio éventuellement extra-terrestres (ex programme SETI)…

Mais les hackers l'utilisent pour un tout autre but : la plupart des accès aux ordinateurs étant protégés par un mot de passe, celui-ci est *craquable* en « brute force » en essayant toutes les combinaisons possibles, comme pour ouvrir la serrure d'un coffre. Plus le mot de passe est long et compliqué, plus l'attaque est longue proportionnellement. Une approche mathématique consiste à prendre toutes les combinaisons de caractères (lettres+chiffres+caractères spéciaux) et à fabriquer une table qui donne la résultante codée pour chacune des combinaisons. Ensuite il suffit de regarder dans cette table si la combinaison chiffrée correspond et de remonter ainsi au mot de passe qui l'a générée.

Plus le mot de passe est long, plus le nombre d'entrées de la table est grand et ceci de manière exponentielle. Cette table « qui résout tout » est appelée *« rainbow table »* ou « table arc-en-ciel ». Plus d'un demi-million de hackers se sont donc « fédérés » autour de ce logiciel et ce réseau *« rainbowcrack.net »* de manière à constituer des tables de plus en plus puissantes, en se partageant la tâche immense de calcul.

Aujourd'hui grâce à ces tables en téléchargement sur Internet, n'importe quel mot de passe de moins de 2x7 caractères est cassé instantanément (ce qui correspond à la totalité des ordinateurs sous Windows XP). Ce « net-ordinateur » virtuel, composé de plus de 500.000 ordinateurs personnels est infiniment plus puissant que n'importe lequel du top 10 des ordinateurs « nationaux ». Les millions d'ordinateurs qui composent le réseau BOINC ont plus de puissance de calcul qu'aucun Etat n'a jamais osé rêver et le tout en mode « gratuit » !

MYTHE N° 9 :
LES HACKERS SONT DESINTERESSES.

Alexander Tereshki Joanna Rutkowska Rafal Wojtczuk

Non, la nouvelle génération en a fait un business…

Cette nouvelle génération comporte déjà ses « vedettes » comme Alex Tereshki, Rafal Wojtczuk et Joanna Rutkowska de *Invisible Things Lab* (qui a démonté et fracturé le système d'accès à Vista avec sa fameuse *« Blue Pill »*), les Italiens Andrea

Barisani et Daniele Bianco dont j'ai parlé plus haut.

Andrea Barisani Ankit FADIA

Ces hackers sont plutôt d'Europe de l'Est ou d'Inde –comme mon ami Ankit Fadia -se décrivent comme des « chercheurs en sécurité » et ont souvent une entité commerciale pour « rentabiliser » leurs travaux. Ils participent largement à des conférences ou interviennent sur des missions de *« forensics »* pour aider les entreprises, les éditeurs de logiciel ou les gouvernements à comprendre ce qui s'est passé en cas d'intrusion ou de faille de sécurité. L'exemple de DAN Kaminsky illustre bien ce phénomène : au lieu de divulguer sur Internet l'énorme faille de sécurité qu'il avait découverte sur les serveurs DNS du monde entier, il a contacté en secret les éditeurs –y compris les développeurs du libre, premiers concernés par cette faille, les serveurs DNS BIND étant essentiellement sous Linux-et a ainsi permis de corriger la faille 11 jours avant que les hackers de METASPLOIT ne publient le programme d'attaque et que les *script kiddies* se jettent dessus pour l'essayer.

Avec Dan Kaminsky à la BH 2008

Puisqu'on parle de METASPLOIT, voici l'exemple typique de la facilité pour porter une attaque aujourd'hui vers un site ou vers un ordinateur connecté à Internet. METASPLOIT analyse la faille publiée, écrit un code d'attaque et le publie aussitôt sur son site :

Mais H.D. Moore le fondateur de METASPLOIT vient de vendre sa société, et lui avec, à un éditeur de sécurité Américain. **Tout le travail collaboratif du libre a donc été récupéré par une société privée…**

MYTHE N° 10 :
LES HACKERS SONT DES PROGRAMMEURS CHEVRONNES

En fait tous les programmes de hacking sont disponibles sur Internet

A part quelques exceptions, la plupart des hackers reprennent les sources de programmes existants ou utilisent des programmes tout faits.

Il existe plein de sites « alternatifs » comme Goolag.org, Backtrack, secuser.org, etc… qui permettent à l'apprenti hacker de « faire son marché ». Voici la page d'accueil de goolag.org. Vous avez bien entendu saisi le clin d'œil à Google :

Ou rfidiot.org qui indique tous les éléments pour pirater les badges RFID des autoroutes, transports en commun ou stations de ski :

MYTHE N° 11 :
IL EXISTE DES « HACKERS D'ETAT ».

La nouvelle génération chinoise est indépendante, impatiente et nationaliste…

Il existe également un mythe de hackers d'Etat, désignant notamment la Chine. Ces hackers seraient rémunérés par le gouvernement Chinois afin de récupérer les secrets industriels dans nos sites à travers des piratages par Internet. Alors que l'attaque de l'intérieur –par un stagiaire par exemple-me parait plausible et simple, autant l'attaque concertée depuis internet est un mythe : De par leur nature les hackers –même les Chinois-sont «anti-establishement », et pour avoir été plusieurs fois en Chine, j'ai vu que les jeunes ingénieurs informaticiens aspirent essentiellement aux même valeurs matérielles qui nous ont porté depuis la fin de la 2eme guerre mondiale : avoir une (belle) voiture, un appartement, un frigo plein, une télé avec 300 chaines, et bien entendu un smartphone et une connexion internet à haut débit…

« Chinese Cyber-Army »

La seule différence notable avec « nos hackers » est qu'ils ont un sens nationaliste hyper-aigü généré par les humiliations que les occidentaux leur ont fait subir pendant des centaines d'années quand ils n'étaient que l'ombre de l'ancien « Empire du Milieu ».

Alors quand *Jin Jing*, athlète Chinoise paralympique, portant la flamme olympique à Paris se fait asperger par des imbéciles fanatiques (pour dénoncer les atteintes aux droits de l'homme au Tibet) avec des extincteurs, pour éteindre la flamme et se fait renverser son fauteuil, les hackers Chinois le prennent pour une grave offense et se vengent en attaquant les sites Français en déni de service, comme d'ailleurs ils ont boycotté les magasins Carrefour sur place…

Jin Jing sur son fauteuil,
lors du passage de la flamme à Paris

Il est clair que la Chine forme actuellement la plupart des ingénieurs dans le monde et que qualitativement ils n'ont rien à envier aux nôtres : Par exemple, deux jeunes femmes de l'Université de Shanghai ont partiellement cassé l'algorithme MD5 en août 2004, et comme tous les chercheurs ont publié leurs travaux sur Internet. Cet algorithme étant constitutif du protocole https qui chiffre nos flux web sur Internet il y a de quoi s'inquiéter…

Peu de temps après, malgré les dénégations des « experts », les Chaos Computer Club allemand et également EPFL de Lausanne confirmaient les « collisions » dans certains cas

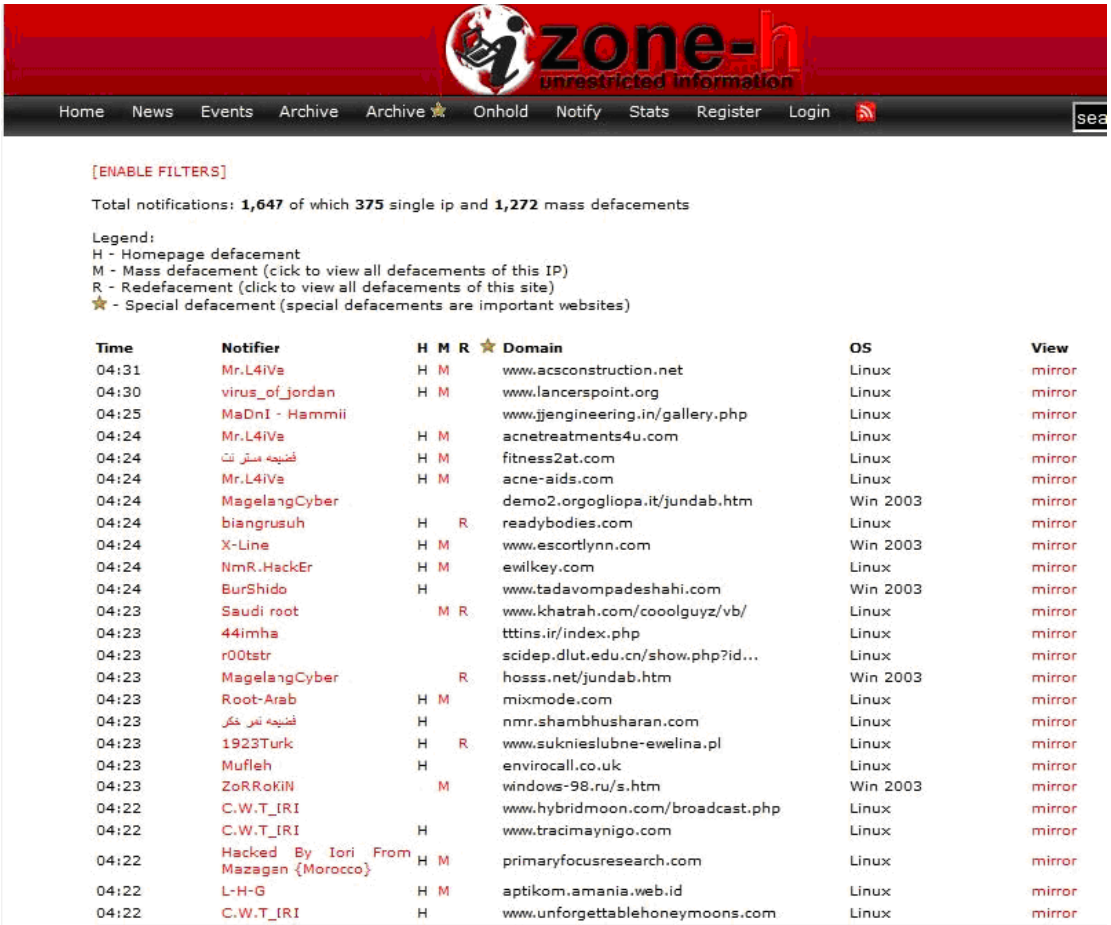
permettant la réversibilité du hash : autrement dit on peut « retrouver le steak initial avec la viande hachée », ou bien on peut retrouver par cryptanalyse le mot de passe… Plus besoin de « rainbow table » ou de puissants supercalculateurs…

On dirait que les hackers sont pratiquement le « R&D » de la sécurité !

MYTHE N° 12 :
LES HACKERS ADORENT SE VANTER DE LEURS EXPLOITS

Ils ont même un site web qui les recense… sans les encenser !

A propos de R&D est-ce que les sites web sont sécurisés ? A entendre les banques et autres sites de e-commerce : « tout est sous contrôle ». Mais est-ce vrai ? En vérité il y a des failles à la fois dans les systèmes et dans le code applicatif. Certains hackers les trouvent mais comment le prouver et surtout s'en vanter ? Le site *« zone-h.org »* a été créé comme un *« Guiness des records »* des hackers. Ceux-ci peuvent faire une copie d'écran de la page piratée et la poster sur le site pour preuve avec le lien pour aller sur le site.



Time	Notifier	H	M	R	Domain	OS	View
04:31	Mr.L4iVe	H	M		www.acsconstruction.net	Linux	mirror
04:30	virus_of_jordan	H	M		www.lancerspoint.org	Linux	mirror
04:25	MaDnI - Hammii				www.jjengineering.in/gallery.php	Linux	mirror
04:24	Mr.L4iVe	H	M		acnetreatments4u.com	Linux	mirror
04:24	فضيحه ستر نت	H	M		fitness2at.com	Linux	mirror
04:24	Mr.L4iVe	H	M		acne-aids.com	Linux	mirror
04:24	MagelangCyber				demo2.orgogliopa.it/jundab.htm	Win 2003	mirror
04:24	biangrusuh	H		R	readybodies.com	Linux	mirror
04:24	X-Line	H	M		www.escortlynn.com	Win 2003	mirror
04:24	NmR.HackEr	H	M		ewilkey.com	Linux	mirror
04:24	BurShido	H			www.tadavompadeshahi.com	Win 2003	mirror
04:23	Saudi root		M	R	www.khatrah.com/cooolguyz/vb/	Linux	mirror
04:23	44imha				tttins.ir/index.php	Linux	mirror
04:23	r00tstr				scidep.dlut.edu.cn/show.php?id...	Linux	mirror
04:23	MagelangCyber			R	hosss.net/jundab.htm	Win 2003	mirror
04:23	Root-Arab	H	M		mixmode.com	Linux	mirror
04:23	فضيحه نمر خكر	H			nmr.shambhusharan.com	Linux	mirror
04:23	1923Turk	H		R	www.sukrieslubne-ewelina.pl	Linux	mirror
04:23	Mufleh	H			envirocall.co.uk	Linux	mirror
04:23	ZoRRoKiN		M		windows-98.ru/s.htm	Win 2003	mirror
04:22	C.W.T_IRI				www.hybridmoon.com/broadcast.php	Linux	mirror
04:22	C.W.T_IRI	H			www.tracimaynigo.com	Linux	mirror
04:22	Hacked By Iori From Mazagan {Morocco}	H	M		primaryfocusresearch.com	Linux	mirror
04:22	L-H-G	H	M		aptikom.amania.web.id	Linux	mirror
04:22	C.W.T_IRI	H			www.unforgettablehoneymoons.com	Linux	mirror

On appelle ce phénomène le « defacing ». Il s'agit de montrer que l'on a pris le contrôle du site en changeant sa page d'accueil ce qui prouve que l'on est capable d'écrire ce qu'on veut sur l'ordinateur « cible » qui héberge le site. La tribu des hackers nationalistes ou idéologues en « …istes », qui attaquent les sites d'un pays « inamical » en profitent pour mettre un message politique. Par exemple ci-dessous le *défacement* (le mot n'existe pas, mais vous avez compris) de la page d'accueil de Baidu qui est … le Google chinois !

Un autre exemple de déni de service distribué est celui récent de la tribu des *« anonymous »* qui en utilisant le programme LOIC (Low Orbit Ion Cannon) attaquent les sites des banques en les inondant, donc en empêchant les transactions normales avec leurs clients, parce que ces banques refusent d'encaisser les dons vers Wikileaks, tentant ainsi d'asphyxier ces derniers et les contraindre à fermer leur site.
Les polices du monde entier, y compris en France, traquent les *anonymous* et viennent par exemple d'arrêter un adolescent de 15 ans qui n'a pas trouvé plus malin que d'utiliser le programme LOIC depuis chez ses parents avec l'adresse IP de sa Freebox… Les « vrais » *anonymous* utilisent bien entendu des proxy avec des rebonds comme dans le réseau TOR dont j'ai déjà parlé :

MYTHE N° 13 :
LES HACKERS SONT DECIDEMENT DES DELINQUANTS ET DOIVENT ETRE TRAITES COMME TELS (LES MYTHES ONT LA VIE DURE)…

Les hackers sont les messagers de la vérité même si elle n'est pas bonne à entendre !

Mais revenons au commencement de l'affaire *Wikileaks* : Le site par lui-même ne fait que collecter des informations que n'importe quel internaute peut « poster » et ceci depuis plusieurs années. Des dons -comme pour Wikipedia-lui permettent de payer les hébergements dans les différents pays. Tout le monde s'en fiche jusqu'au jour un informaticien « gay » de l'Armée Américaine (le fait qu'il soit homosexuel est déterminant dans l'histoire), décide de pomper tous les messages échangés par les ambassades US dans le monde et de les poster sur *Wikileaks*… Il est en Irak, et naturellement l'armée Américaine concentre là-bas toutes les informations nécessaires au déroulement des opérations. Donc cet informaticien entre dans la salle informatique, copie toutes les données de la base en quelques minutes et en ressort sans être inquiété !!!

Il les publie sur *Wikileaks* et là c'est un déchainement médiatico-politique contre, une fois encore, le « messager » Julian Assange. On déterre même une affaire de viol en Suède, alors qu'il est Australien et il est incarcéré au Royaume Uni. Les banques américaines, VISA, Mastercard, Paypal, Bank of America sont priées de lui bloquer ses comptes et les hébergeurs de résilier leur contrat ; Idem en Europe…

Au lieu de se demander comment un simple soldat-informaticien avait pu dérober 250.000 câbles classés secrets en quelques minutes en plein territoire de guerre qui plus est (donc que des ennemis pourraient réaliser aussi) et comment y remédier pour que cela ne se reproduise plus, on s'attaque à celui qui ose en parler…

Comment cet informaticien a-t-il procédé et pourquoi ? Il a utilisé un disque DVD-RW (réinscriptible) qui contient 4Go de données - ce qui est énorme pour stocker du texte-et lors de la fouille en sortie à prétendu qu'il s'agissait d'une copie de chansons de Lady Gaga ! Le garde responsable de la fouille – qui cherchait des clefs USB ou des disques durs en suivant scrupuleusement sa procédure-n'y a vu que du feu…

Le soldat à fait cela et surtout publié ces informations par vengeance. Il en avait assez d'être maltraité comme homosexuel dans l'armée US. *« Don't ask, don't tell»* suivant la doctrine. *« Ne posez pas la question et ne le dites pas »*. Du coup, c'est le facteur humain qui a causé la trahison, comme souvent en sécurité…

Au final, les hackers sont à l'informatique ce que les écologistes sont à l'économie de marché : un contrepoids d'idées et de pouvoir. En ce sens ils ont toute leur place pour contrer des éditeurs de logiciels qui n'ont pas forcement l'objectif unique d'améliorer la sécurité de leurs clients, mais probablement surtout l'objectif de s'enrichir massivement sur un marché colossal. Les hackers aident les entreprises à boucher leurs trous de sécurité en leur faisant subir le challenge de la réalité des attaques. Les hackers défient les états totalitaires en les empêchant de censurer l'information.

S'il n'y avait pas les hackers, « Big Brother » aurait déjà gagné !

MYTHES ET LEGENDES DU CORRESPONDANT INFORMATIQUE ET LIBERTES

Bruno Rasle
Délégué général de l'AFCDP

Le 6 août 2004, à l'occasion de la transposition de la directive européenne 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, la France s'est dotée d'un dispositif qui dispense de l'obligation de déclaration auprès de la CNIL les responsables de traitements qui ont procédé à la désignation d'un «*détaché à la protection des données à caractère personnel* ».

Cette personne – plus connue sous le nom de CIL (pour Correspondant Informatique & Libertés) – est « *chargée d'assurer, d'une manière indépendante, l'application interne des dispositions nationales* » et « *de tenir un registre des traitements […] garantissant de la sorte que les traitements ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées* ». La fonction a été définie par le décret n°2005-1309 du 20 octobre 2005. Toutes les entités procédant au traitement automatisé de données à caractère personnel sont concernées quelque soit leur secteur, leur statut ou leur taille.

Issue largement d'une pratique allemande, cette mesure a été introduite dans la Loi dite « Informatique et Libertés » sur l'initiative d'Alex Türk, sénateur du Nord et Président de la CNIL. Cette fonction de « délégué à la protection des données à caractère personnel » a été transposée chez plusieurs de nos voisins : Allemagne, Estonie, Luxembourg, Hongrie, Pays-Bas, Slovaquie et Suède.

Le Correspondant Informatique et Libertés a vocation à être un interlocuteur spécialisé en matière de protection de données à caractère personnel, tant pour le responsable des traitements, que dans les rapports de ce dernier avec la CNIL. Le CIL occupe ainsi une place centrale dans le développement maîtrisé des nouvelles technologies de l'information et de la communication.

Au-delà du simple allègement de formalités, le Correspondant à un rôle primordial à jouer pour s'assurer que l'informatique se développera sans danger pour les droits des usagers, des clients et des salariés. C'est aussi pour les responsables des fichiers le moyen de se garantir de nombreux risques vis-à-vis de l'application du droit en vigueur.

Au sens strict de la nouvelle loi et de son décret d'application relatif au correspondant, les missions de ce dernier sont de tenir la liste des traitements et de veiller à l'application de la loi. Mais d'autres missions peuvent être confiées au Correspondant, comme la préparation des demandes d'autorisation, l'élaboration d'une politique de protection des données à caractère personnel, la sensibilisation du personnel aux dispositions de la loi, l'extension de la tenue de la liste aux traitements non dispensés ou encore le contrôle de l'application des règles prédéfinies.

MYTHE N°1 :
LE CORRESPONDANT INFORMATIQUE ET LIBERTES (OU CIL) EST LE REPRESENTANT DE LA CNIL AU SEIN DE L'ORGANISATION QUI L'A DESIGNE.

Le CIL est le plus souvent un collaborateur de l'entité (entreprise, association, collectivité, etc.), recruté spécialement ou désigné parmi le personnel. Bien qu'il soit effectivement l'interlocuteur privilégié de la Commission Nationale Informatique et des Libertés, il n'est en rien son représentant. Il est financièrement à la charge de l'entité qui l'a désigné et conseille dans ses choix le responsable de traitement au regard de la conformité à la loi Informatique et Libertés et du droit des personnes concernant leurs données à caractère personnel.

Le CIL doit particulièrement veiller à ne pas apparaître comme un *Mister No*, évoquant à la moindre dérive les risques juridiques qui pèsent sur le responsable de traitement. Il doit s'imprégner des objectifs opérationnels poursuivis par les directions métier et – dans la limite de ce que permet le cadre légal – porter conseil pour trouver les équilibres adéquats.

MYTHE N°2 :
LE CORRESPONDANT INFORMATIQUE ET LIBERTES EST NECESSAIREMENT UN EMPLOYE DE L'ORGANISATION.

Dans une limite précisée par le décret d'application n°2005-1309 du 20 octobre 2005 (dans son article 44), certaines entités peuvent désigner une personne étrangère à leur personnel. Lorsque moins de cinquante personnes participent à la mise en œuvre du traitement ou y ont directement accès, l'organisme est libre de désigner un CIL externe. Il peut s'agir d'un consultant spécialisé, d'un avocat, d'un expert comptable, d'une société de conseil en informatique … pour autant que la personne dispose des compétences nécessaires. Sont comptabilisées pour pouvoir procéder ainsi toutes les personnes chargées d'exploiter, de développer et d'assurer la maintenance de l'application, tous les utilisateurs chargés notamment de saisir les données ou de les consulter ainsi que toutes les personnes qui, en raison de leurs fonctions ou pour les besoins du service, accèdent aux données enregistrées.

Lorsque le seuil des cinquante personnes est dépassé, le recours à une personne externe est strictement encadré : le CIL peut être un salarié d'une des entités du groupe de sociétés auquel appartient l'organisme, un salarié du groupement d'intérêt économique dont est membre l'organisme, une personne mandatée à cet effet par un organisme professionnel, une personne mandatée à cet effet par un organisme regroupant des responsables de traitement d'un même secteur d'activité. On parle alors de CIL externe et de CIL mutualisé (comme au sein du Notariat, ou chez les huissiers).

A noter que, parmi les états membres qui ont opté pour la formule du Délégué à la protection des données personnelles, seule la France restreint le champ des possibles. Aucun de nos voisins n'impose un seuil, laissant le responsable de traitement prendre ses responsabilités en choisissant ce qui lui semble correspondre le mieux aux objectifs poursuivis.

MYTHE N°3 :
LE CIL ENDOSSE LES RESPONSABILITES PENALES QUI PESAIENT, AVANT SA DESIGNATION, SUR LE RESPONSABLE DE TRAITEMENT.

Le CIL n'est pas un paratonnerre. Son rôle est de conseiller le responsable de traitement sur les mesures à prendre pour respecter le droit et il n'y a pas de transfert de la responsabilité

vers le CIL. Le responsable de traitement conserve la pleine et entière responsabilité vis-à-vis des traitements mis en œuvre et de leur conformité à la loi.

Pour autant on peut imaginer que la responsabilité propre du CIL pourrait être recherchée en cas de complicité d'infraction (par exemple s'il a connaissance d'une non-conformité grave au regard de la loi Informatique et Libertés, commise sciemment par le responsable de traitement ou ses commettants, mais qu'il ne la traite pas), voire de négligence patente.

Si le CIL ne peut être tenu pénalement responsable des manquements de son responsable de traitement, seuls ses propres manquements peuvent lui être imputables. En conclusion, le risque de mise en cause de la responsabilité du CIL semble très faible, sans être pour autant inexistant.

MYTHE N°4 :
LE CORRESPONDANT INFORMATIQUE ET LIBERTES EST UN SALARIE PROTEGE.

C'est le cas en Allemagne mais pas en France, au sens où on l'entend pour des représentants du personnel ou des délégués syndicaux. Même si la loi Informatique et Libertés précise que le CIL ne peut faire l'objet de sanctions de l'employeur du fait de l'exercice de ses missions, il peut être déchargé en cas de manquements graves dûment constatés et qui lui sont directement imputables au titre de ses fonctions de CIL. Pour assurer l'effectivité de cette protection, la CNIL doit être avertie de toute modification affectant sa fonction.

La décharge du CIL peut être initiée par la CNIL, lorsqu'un manquement grave aux devoirs de ses missions est directement imputable au Correspondant. Après avoir recueilli les observations de ce dernier, la Commission Nationale Informatique et des Libertés peut demander au responsable des traitements de relever le CIL de ses fonctions.

La décharge du CIL à la demande du responsable de traitement ne peut être envisagée qu'en raison de manquements à l'exécution de sa mission par le CIL : Le responsable des traitements doit saisir la CNIL pour avis et informer son Correspondant en même temps, afin que celui-ci puisse présenter ses observations. Les manquements invoqués doivent être directement imputables au Correspondant et relever directement de l'exercice de ses missions telles que définies dans la désignation notifiée à la CNIL.

La CNIL fait alors connaître son avis dans le délai d'un mois.

Ce n'est qu'une fois le CIL mis en mesure d'exposer son point de vue et à l'expiration du délai que la décision de le décharger peut être prise par le responsable des traitements. Pour continuer à bénéficier de la dispense de déclaration, le responsable de traitement doit notifier à la CNIL les coordonnées et fonctions de son nouveau Correspondant. A défaut, le responsable de traitement devra déclarer l'ensemble des traitements exonérés.

MYTHE N°5 :
LE CIL A UNE OBLIGATION DE DENONCER SON EMPLOYEUR OU CLIENT A LA CNIL S'IL CONSTATE DES IRREGULARITES.

Dans son article 49, le décret n°2005-1309 du 20 octobre 2005 dispose que le CIL « *informe le responsable des traitements des manquements constatés avant toute saisine de la Commission nationale de l'informatique et des libertés* ». *L'article 51 précise que « La Commission nationale de l'informatique et des libertés peut être saisie à tout moment par le correspondant à la protection des données à caractère personnel ou le responsable des traitements de toute difficulté rencontrée à l'occasion de l'exercice des missions du correspondant. L'auteur de la saisine doit justifier qu'il en a préalablement informé, selon le cas, le correspondant ou le responsable des traitements* ».

Ce pouvoir de saisine doit donc être utilisé en dernier recours (une fois seulement que toutes les autres voies ont été exploitées, après que le Correspondant a effectué les démarches nécessaires auprès du responsable de traitements et que celles-ci sont demeurées infructueuses) et lorsque cela se justifie réellement, quand le CIL rencontre de notables difficultés dans l'exercice de ses missions, par exemple en l'absence systématique de consultation avant la mise en œuvre de traitements sensibles, ou devant l'impossibilité d'exercer ses fonctions du fait de l'insuffisance des moyens alloués.

Avant d'utiliser ce pouvoir, le CIL et le Responsable de traitement peuvent s'entretenir avec la CNIL, notamment devant certaines difficultés d'application des dispositions législatives et réglementaires.

Si le Correspondant doit utiliser son pouvoir de saisine dans les cas extrêmes, il doit veiller également à ses propres intérêts, car nous avons vu que sa responsabilité propre pourrait être recherchée en cas de complicité d'infraction.

MYTHE N°6 :
SI LE RESPONSABLE DE TRAITEMENT DESIGNE UN CIL, IL EVITE LES CONTROLES SUR PLACE DE LA CNIL ET ECHAPPE A TOUTE SANCTION.

Des entités ayant désigné un CIL ont d'ores et déjà fait l'objet de contrôles sur place. Dans son rapport annuel pour l'année 2009, la CNIL indique même qu'elle compte profiter des prochains contrôles sur place qu'elle va effectuer pour « évaluer l'efficacité des CIL ». La désignation d'un Correspondant n'est donc pas un facteur direct permettant d'échapper aux contrôles et aux éventuelles sanctions. Par contre c'est indubitablement un facteur de réduction de l'exposition à ces risques.

De plus le CIL est à même de préparer son entité à faire l'objet d'une mission de contrôle de la CNIL. L'AFCDP, association qui représente les CIL, a publié un livre blanc qui permet de gérer une telle situation.

MYTHE N°7 :
SI LE RESPONSABLE DE TRAITEMENT DESIGNE UN CIL, IL N'A PLUS AUCUNE FORMALITE A EFFECTUER VIS-A-VIS DE LA CNIL.

Seuls les traitements de données à caractère personnels soumis au régime de la déclaration sont exonérés de formalité en cas de désignation d'un Correspondant Informatique et Libertés. Les traitements soumis à demande d'autorisation ne le sont pas.

Lors de la désignation de son CIL, le responsable de traitement doit indiquer s'il attend également de son Correspondant qu'il apporte son aide dans la préparation des demandes d'autorisation.

Enfin, même si le décret n°2005-1309 du 20 octobre 2005 n'oblige le CIL qu'à mettre dans son registre les traitements exonérés de déclaration, il est recommandé de garder sous son « radar » les traitements bénéficiant de dispense, ne serait-ce que pour vérifier qu'ils restent bien sous ce périmètre.

MYTHE N°8 :
LE CIL EST FORCEMENT UN JURISTE.

Clarifions immédiatement un point : il n'existe pas de « profil » idéal du candidat CIL. Les correspondants actuels viennent d'horizons très divers : informatique, juridique, qualité, contrôle interne, audit, record management, etc.

Actuellement, aucun agrément n'est demandé, aucune exigence de diplôme n'est fixée, la loi prévoit que le Correspondant est « *une personne bénéficiant des qualifications requises pour exercer ses missions* » : l'une des priorités d'un nouveau CIL est donc de compléter ses connaissances.

Les compétences et qualifications du CIL doivent porter tant sur la législation relative à la protection des données à caractère personnel (Informatique & Libertés, LCEN, Code du travail, etc.) que sur l'informatique et les standards technologiques (cybersurveillance, géolocalisation, biométrie, chiffrement, cookie, etc.), sans oublier le domaine d'activité propre du responsable des traitements.

Le Correspondant doit également avoir connaissance des législations particulières au secteur d'activité concerné (commerce électronique, marketing direct, assurances, collectivités territoriales ...) et des règles spécifiques au traitement de certaines données (données couvertes par exemple par le secret médical ou le secret bancaire). Le CIL doit aussi avoir ou acquérir des compétences en conseil et management pour pouvoir assurer pleinement son rôle d'information et d'audit.

Une qualité est souvent oubliée, celle de communiquant, car il faut garder à l'esprit le facteur organisationnel et humain. Afin de diffuser une culture de protection des données, le CIL doit savoir écouter, sensibiliser, et favoriser les remontées d'informations : Il sera aussi amené dans l'exercice de ses fonctions à permettre un dialogue entre le responsable du traitement, les personnes faisant l'objet du traitement, et la CNIL.

MYTHE N°9 :
LE CIL EST FORCEMENT UN INFORMATICIEN.

D'après les sondages effectués par l'AFCDP auprès de ses membres et les informations divulguées par la CNIL, les informaticiens viennent en première position : plus du tiers des CIL sont de profil informatique (principalement Chefs de projet, RSSI et DBA). La plus forte représentation s'observe au sein des collectivités territoriales et au sein des Universités, dont les CIL sont à plus de 95% des informaticiens.

Mais une nouvelle fois, il n'existe pas de profil idéal pour cette fonction.

Le nom de la loi (Informatique et Libertés) a peut-être assimilé un peut vite, aux yeux des responsables de traitement, la fonction à la seule sphère du système d'information ? Il convient de ne pas oublier que les fichiers sur support papier sont également concernés (comme ceux du périmètre Ressources humaines, par exemple), du moment qu'il existe un ordre permettant un tri ou une entrée sélective.

MYTHE N°10 :
NOUS N'AVONS PAS BESOIN D'UN CIL, NOUS AVONS DEJA UN RSSI.

Si le Responsable de la Sécurité des Systèmes d'Information est chargé de la protection des actifs immatériels de l'entreprise, la mission du CIL est centrée sur la conformité à la loi Informatique et Libertés. Outre le fait que son périmètre d'action est focalisé sur les données à caractère personnel, sa tâche ne se limite pas à s'assurer de leur bonne sécurité, mais s'étend à bien d'autres aspects : information des personnes, tenue du registre des traitements et publicité de celui-ci, organisation des processus de réception et de gestion des demandes de droits d'accès, vérification de l'adéquation des données collectées et de leur durée de conservation au regard de la finalité, etc. En ce qui concerne les données à caractère personnel, le *Privacy By Design* englobe le *Security by Design*.

Mais d'autres missions peuvent être confiées au Correspondant, comme la préparation des demandes d'autorisation de certains traitements auprès de la CNIL (notamment lors de flux transfrontières), l'élaboration d'une politique de protection des données à caractère personnel, la sensibilisation du personnel aux dispositions de la loi, l'extension de la tenue de la liste aux traitements non dispensés ou encore le contrôle de l'application des règles prédéfinies.

MYTHE N°11 :
IL EST IMPOSSIBLE D'ETRE CIL ET RSSI SIMULTANEMENT.

Observons pour commencer que de nombreux RSSI ont été désignés CIL.

Cette simultanéité de pose pas de problèmes particuliers, à deux réserves près. La première provient de l'article 46 du décret n°2005-1309 du 20 octobre 2005 qui précise que « *Le correspondant ne reçoit aucune instruction pour l'exercice de sa mission* » et que « *Les fonctions ou activités exercées concurremment par le correspondant ne doivent pas être susceptibles de provoquer un conflit d'intérêts avec l'exercice de sa mission* ». Concernant spécifiquement les mesures de protection des données personnelles, il faut donc s'assurer qu'il n'y a pas un tel conflit : la même personne peut-elle bien, simultanément, être en charge de cette sécurisation et du contrôle de cette bonne sécurisation ?

La seconde réserve porte sur la délicate gestion des relations hiérarchiques. Le CIL exerce ses missions de manière indépendante, dispose d'une autonomie d'action reconnue par tous et est directement rattaché au responsable de traitement à qui il peut apporter conseils, recommandations et alertes si nécessaires. Ces particularités ne sont pas le fait de la plupart des RSSI qui, dans cette mission, rapporte à un supérieur hiérarchique qui n'est pas le responsable de traitement.

Si la fonction est dévolue à un autre professionnel que le RSSI, le CIL contribue à améliorer la politique de sécurité informatique de l'organisation : en cela CIL et RSSI sont des alliés objectifs et ont de nombreux points communs. Outre le fait qu'ils sont parfois perçus à tort comme des « improductifs » et des « empêcheurs de tourner en rond », ils éprouvent les mêmes difficultés pour être impliqués en amont (et non pas la veille de la mise en œuvre d'une nouvelle application), pour faire passer l'idée que « mieux vaut prévenir que guérir », pour sensibiliser utilisateurs et direction, pour faire appliquer les décisions, politiques, charte, et pour valoriser leurs actions (en l'absence d'incident, avions nous réellement besoin de faire des efforts ?).

Cette coopération (qui doit être élargie au *Risk Manager*, aux spécialistes de l'Intelligence économique et à ceux de la Conformité, de l'Audit et de la Déontologie) va se renforcer dans l'éventualité d'une future obligation de notifier les violations aux traitements de données à caractère personnel, envisagé dans le cadre de la révision de la Directive européenne 95/46 CE et à laquelle les Opérateurs et FAI sont tenus dans le cadre de la transposition du Paquet Telecom.

MYTHE N°12 :
IL N'Y A FINALEMENT PAS GRAND AVANTAGE A DESIGNER UN CIL

En matière de protection de données à caractère personnel, la loi, à elle seule, ne suffit pas. La fonction de Correspondant Informatique et Libertés, créée par le décret n°2005-1309 du 20 octobre 2005, est un élément clé de régulation, par la pratique.

Au-delà du simple allègement de formalités, le Correspondant à un rôle primordial à jouer pour s'assurer que l'informatique se développe sans danger pour les droits des usagers, des clients, des patients, des salariés, des citoyens. C'est aussi pour les responsables des traitements le moyen de se garantir de nombreux risques vis-à-vis de l'application du droit en vigueur.

Au sens le plus strict, la fonction de Correspondant exonère de l'obligation de déclaration préalable des traitements les plus courants. Une lecture superficielle de la loi pourrait laisser croire que l'unique portée de la désignation d'un correspondant serait de bénéficier de cet allègement des formalités déclaratives… ce qui représente une économie de quelques timbres.

Ce serait sous-estimer l'aide précieuse que le CIL apporte au responsable du traitement. C'est, pour ce dernier, le moyen de se garantir de nombreux risques vis-à-vis de l'application du droit en vigueur, d'autant que de lourdes sanctions sont encourues en cas de non-respect de ces obligations. Le Correspondant a donc un rôle de conseil et de suivi dans la légalité de déploiement des projets informatiques et, plus largement, de la gestion de données à caractère personnel. Il propose les solutions permettant de concilier protection des libertés individuelles et intérêt légitime des professionnels. En l'absence de CIL, ces tâches sont souvent négligées alors qu'elles sont essentielles au regard de la protection des droits des personnes.

La désignation d'un Correspondant Informatique et Libertés contribue à réduire les coûts de gestion client (exercice du droit d'accès, gestion des litiges, rationalisation des traitements, suppression des données obsolètes) et permet de développer la collaboration et les synergies entre services (juridique, informatique, marketing, etc.). Enfin, pour les entreprises globales, la désignation d'un CIL s'impose face au *Chief Privacy Officer* des groupes multinationaux. En outre, la désignation d'un Correspondant Informatique et Libertés permet à une organisation de bénéficier d'une relation privilégiée avec la CNIL, qui a mis en place un service qui leur est entièrement consacré.

Le Correspondant, s'il est d'ores et déjà un personnage-clé dans le paysage de la protection des données personnelles, est amené à prendre de l'importance. De plus, que la fonction reste facultative ou qu'elle devienne obligatoire, comme c'est le cas en Allemagne, la désignation d'un CIL va immanquablement être perçue comme un label de qualité et de bonnes pratiques en ce qu'elle rassure le consommateur, l'usager, le collaborateur ou le citoyen : un élément à ne pas négliger quant il s'agit d'instaurer la confiance. Il ne faudrait pas paraître en retard par rapport à ses homologues, confrères et compétiteurs.

MYTHE N°13 :
NOUS SOMMES FORCEMENT EN CONFORMITE CAR NOUS AVONS DESIGNE UN CIL

De la même façon qu'une entité qui n'a pas fait le choix de désigner un CIL peut parfaitement être en conformité avec la loi Informatique et Libertés, rien n'assure qu'un organisme qui a désigné un Correspondant Informatique et Libertés est en complète conformité. Encore faut-il que le CIL ait les qualités et connaissances nécessaires, encore faut-il lui donner les moyens de mener à bien ses missions.

Parmi les facteurs d'efficience, on peut citer : une désignation préparée en mode projet, un rattachement au Responsable du traitement ou *a minima* à une personne faisant partie de l'équipe de direction, une certaine « mise en scène » de la désignation pour bien montrer

qu'une telle décision est un geste fort, une réelle affectation de moyens (temps alloué à la mission, budget, soutien, formation initiale, veille).

D'une façon générale il faut mieux considérer la conformité comme une démarche que comme un état : la désignation d'un CIL par le responsable de traitement n'est pas un aboutissement, mais bien le début de cette démarche.

CONCLUSION

En quelques années, le CIL s'est imposé comme un personnage-clé dans le paysage de la protection des données personnelles. Son absence ne veut pas dire que l'entité n'a pas déployé tous les efforts nécessaires pour être en conformité, mais la désignation d'un Correspondant rassure le consommateur, l'usager, le collaborateur, le patient ou le citoyen : un élément à ne pas négliger quant il s'agit d'instaurer la confiance.

De plus, que la fonction reste facultative ou qu'elle devienne obligatoire comme c'est déjà le cas en Allemagne et comme la proposition de loi Détraigne-Escoffier (votée au Sénat le 23 mars 2010) le prévoit, la désignation d'un CIL peut être perçue comme un label de qualité et de bonnes pratiques. Dans l'attente, le volontariat donne l'occasion à certaines entités de se démarquer.

La révision de la Directive européenne de 1995, qui a donné naissance à notre loi Informatique et Libertés actuelle et au CIL, est en marche, pour adapter le cadre légal aux récents développements technologiques comme le *Cloud Computing*, les réseaux sociaux, les applications mobiles et la géolocalisation, le marketing comportemental, les puces RFID, la vidéoprotection, la biométrie ou les nanotechnologies. Dans sa communication du 4 novembre 2010 la Commission européenne introduit de nouvelles contraintes, comme l'*Accountability* (l'obligation, pour le Responsable de traitement de prouver qu'il a pris des mesures pour assurer la conformité), l'analyse d'impact et de risques en amont de tout projet manipulant des données personnelles, la notification des violations aux traitements de données à caractère personnelles, la mise en œuvre du concept de *Privacy By Design* et la désignation d'un délégué à la protection de ces mêmes données.

Pour s'y préparer, les professionnels concernés se sont regroupés au sein d'une association qui les représente, l'AFCDP (Association Française des Correspondants à la protection des Données à caractère Personnel), qui a déjà eu l'occasion de faire connaître ses positions et d'influer sur certaines orientations.

La fonction de correspondant doit être tirée vers le haut. Certains voient le CIL du futur comme un véritable « Commissaire aux données », ou « Commissaire Informatique et Libertés », par analogie avec les commissaires aux comptes. De toute façon, il faut avoir de l'ambition pour ce nouveau métier, passionnant, qui se fonde sur la primauté de la personne comme le dit l'article premier de la Loi Informatique et Libertés : « *L'informatique doit être au service de chaque citoyen […] Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ».

ACRONYMES

MYTHES ET LEGENDES D'INTERNET

ATM : Asynchronous Transfer Mode

ETSI : European Telecommunications Standards Institute

ICANN : Internet Corporation for Assigned Names and Numbers

IETF : Internet Engineering Task Force

IPsec : Internet Protocol Security

IPv6 : Internet Protocol version 6

ISO : International Organization for Standardization

NAT : Network Address Translation

P2P : Peer-to-Peer

RINA : Recursive Inter-Network Architecture

ToIP : Telephony over IP

UIT : Union Internationale des Télécommunications (ITU)

MYTHES ET LEGENDES DE LA SECURITE DE L'INFORMATION

CERT : Computer Emergency Response Team

MYTHES ET LEGENDES DU CHIFFREMENT

3DES : Triple Data Encryption Standard

AES : Advanced Encryption Standard

RSA : Rivest Shamir Adleman, algorithme de cryptographie asymétrique du nom de ses inventeurs

MYTHES ET LEENDES DE LA SIGNATURE ELECTRONIQUE

MD5 : Message Digest 5, fonction de hachage

PIN : Personal Identification Number

SHA1,2,3 : Secure Hash Algorithm

MYTHES ET LEGENDES DE LA CERTIFICATION CRITERES COMMUNS

ANSSI : Agence nationale de la sécurité des systèmes d'information

EALn : Evaluation Assurance Level n

ITSEC : Information Technology Security Evaluation Criteria

VPN : Virtual Private Network

MYTHES ET LEGENDES DU PAIEMENT MOBILE

NFC : Near Field Communication

GLOSSAIRE

Audioconférence

Une *téléconférence* dans laquelle les participants sont en communication téléphonique chacun avec tous les autres. Elle permet la transmission de phonie et éventuellement de télécopie.

Communications unifiées

Un ensemble de services destinés aux entreprises qui permet d'unifier les moyens de communications interpersonnelles temps réel (téléphonie fixe et mobile, visiophonie, etc.), les outils de travail collaboratif, ainsi que l'environnement informatique et les applications bureautiques de l'entreprise.

CTI *Computer Telephony Integration*

Un ensemble de techniques, de matériels et de logiciels qui réalisent des applications informatiques couplées avec des services téléphoniques. Il est utilisé notamment pour le télémarketing et dans les *centres d'appels*.

Interopérabilité

La possibilité donnée à des services ou des équipements de technologies différentes à fonctionner ensemble.

NFC

Communication en champ proche (Near Field Communication), technologie de communication sans-fil à courte portée et haute fréquence, permettant l'échange d'informations entre des périphériques jusqu'à une distance d'environ 10 cm.

Extension des mécanismes RFID (Radio Frequency IDentification), permettant notamment d'interagir avec un téléphone mobile dans le cadre du paiement électronique.

Présence

Une fonctionnalité utilisée dans les solutions de collaboration pour connaître l'état de présence (téléphonique, calendrier, PC) des collaborateurs. Les utilisateurs peuvent ainsi communiquer de manière efficace selon la situation du moment et le média le plus approprié.

SI *Système d'Information*

Un ensemble organisé de ressources (personnel, données, procédures, matériel, logiciel…) dont le but est d'acquérir, stocker, structurer et communiquer des *données* (texte, images, phonie, sons, données informatiques, vidéo…).

Softphone

Un logiciel qui émule un poste téléphonique sur un ordinateur. L'ordinateur, équipé d'interfaces audio (microphone + haut-parleur ou micro casque) est utilisé pour recevoir ou émettre des communications téléphoniques avec les services associés.

Téléconférence

Une conférence durant laquelle les participants sont répartis dans plusieurs lieux reliés entre eux par des moyens de télécommunications.

Vidéoconférence

Une *téléconférence* dans laquelle les participants sont reliés par des circuits qui permettent la transmission d'images animées et de phonie.

Web Social

Une optique dans laquelle l'Internet est considéré comme un espace de socialisation, un lieu dont une des fonctions principales est l'interaction entre les personnes.

Web2.0

Un ensemble de technologies et d'usages qui ont suivi la forme initiale du *Web*, en particulier les interfaces permettant aux internautes d'interagir de façon simple à la fois avec le contenu et la structure des pages mais aussi entre eux. Le Web2.0 a donné naissance au *Web Social*.

POUR ALLER PLUS LOIN DANS LA CONNAISSANCE DES TIC

Les contributeurs de cet ouvrage collectif ont également écrit, ou participé à l'écriture de livres dans leurs domaines d'expertises. Voici, sans être objectif, loin s'en faut, quelques uns de ces livres qui peuvent vous permettre d'aller plus loin dans la connaissance des TIC.

.

Christian Aghroum :

Auteur de :

- « Les mots pour comprendre la cybersécurité et profiter sereinement d'Internet », collection Dico Dékode, 2010, éditions Lignes de Repères.

Contributeur de :

- « Identification et surveillance des individus ». Editions de la Bibliothèque publique d'information (Centre Pompidou) Juin 2010
- « Cybercriminalité, une guerre perdue ? » Editions Choiseul « Sécurité Globale » Dossier numéro 6 - Hiver 2008
- « La criminalité numérique ».Editions INHES : « Les cahiers de la sécurité » Cahier numéro 6 – Octobre 2008
- « Cybercriminalité et cybersécurité en Europe ». Les Dossiers Européens n°14 April 2008
- « La lutte contre la contrefaçon, enjeux, nouveaux moyens d'action, guide pratique ». Editions du Ministère de l'Economie, Ministère du Budget 1995

Jean-Pierre Archambault

Auteur de :

- De la télématique à Internet aux éditions du CNDP

Michel Elie

Auteur de divers articles sur l'histoire et la prospective de l'internet.

Il a coordonné le dossier « le fossé numérique l'internet facteur de nouvelles inégalités ? » publié par La Documentation Française en août 2001

Franck Franchin

Co-auteur de :

- « Le business de la cybercriminalité ». Collection Management et informatique. Editions Hermes Science.

Jean-Denis Garo

Auteur de :

- « Mon papa travaille dans l'Informatique et les Télécoms » - 2007
- « Anita & Béatrix – Le sens caché du vocabulaire des IT » - 2010

Co-Auteur des livres collectifs :

- « Sécurité des Systèmes d'Information » Les Guides ECOTER, Edition Mission Ecoter – 2002
- « Guide TIC des petites et moyennes collectivités », Edition Ficome – 2004
- « La sécurité à l'usage des décideurs ». Edition etna France- 2005
- « La sécurité à l'usage des PME et des TPE », Edition Ténor – 2006
- « La Sécurité à l'usage des collectivités locales et territoriales », Edition Forum ATENA- 2009
- « Lexique des TIC », Edition Forum ATENA – 2010
- « L'Internet à l'usage ....de l'écosystème numérique de demain », Edition Forum ATENA - 2011

Responsable éditorial de :

- « L'Off-Shore et les centres de contacts Cap sur l'île Maurice », Edition 1Angle2Vues - 2007

Thierry Gaudin,

- Voir l'imposante quantité d'oeuvres écrites en

http://www.2100.org/gaudin/1/publications/

Daniel Guinier,

Auteur de :

- « Sécurité et qualité des systèmes d'information – Approche systémique -*"La part de l'homme"* ». Editions Masson, 1992.
- « Catastrophe et management - Plans d'urgence et continuité des systèmes d'information ». Editions Masson, 1995.
- « Le courrier électronique et l'archivage légal ». Livre blanc, édité par IBM France, 2005.

Contributeur de :

  - « Systèmes d'information - Art et pratiques ; Ch. 5 : Sécurité et cybercriminalité ». Editions d'Organisation (Eyrolles), 2002.
- « Tableaux de bord pour diriger dans un contexte incertain ; Ch. 13 : La sécurité des tableaux de bord ». Editions d'Organisation (Eyrolles), 2004.
- « Encyclopédie de l'informatique et des systèmes d'information ; Section II/4 : La politique de sécurité ». Editions Vuibert, 2006.
- « Le guide pratique du chef d'entreprise face au risque numérique ». Guide édité par la gendarmerie nationale, préface du ministre de l'intérieur, 2009, 2010.

Mauro Israel

Auteur de :

- Aide mémoire Netware de NOVELL –DUNOD TECH
- Guide PSI Netware de NOVELL – DUNOD TECH

Contributeur de :

- La sécurité à l'usage de PME-TPE collection TENOR

Sophie de Lastours

Auteur de :

- La France gagne la guerre des codes secrets, 1918 chez Tallandier, et de nombreux articles sur l'histoire du chiffre dont les plus récents :
- La section du chiffre pendant la Première Guerre Mondiale
- A travers les travaux du colonel Henry Olivari et du capitaine Georges-Jean
- Painvin, Université de Saint Denis Paris VIII. Journée d'Etudes sur les enjeux de la cryptologie. 2008.
- La cryptologie est elle misogyne ? Bulletin de l'ARCSI 2009.
- Diplomatie, renseignement et codes secrets au cours de la longue vie du général Charles-François Dumouriez (1739-1823) Actes du colloque de Cambrai. Journée Dumouriez sous le patronage du Sénateur Jacques Legendre et Bulletin de l'ARCSI 2011

Elle a pris en charge avec Gilbert Eudes sous le titre « Mission d'un cryptologue en Russie (1916) » et publié dans la collection qu'elle dirige, le manuscrit du colonel Henry Olivari qui lui avait été confié par son petit-fils.

Fabrice Mattatia,

Auteur de :

- "An Overview of Some Electronic Identification Use Cases in Europe", in *Practical studies in e-government*, S. Assar, I. Boughzala et I. Boydens (dir), Springer, 2011.

Gérard Peliks

Auteur de :

- "Le World Wide Web: Création de serveurs sur Internet". Éditions. Addison-Wesley France 1995

Contributeur et synchroniseur des les livres collectifs :

- « La sécurité à l'usage des décideurs ». Edition etna France – 2005
- « La sécurité à l'usage des PME et des TPE », collection Ténor – 2006
- « La Sécurité à l'usage des Collectivités locales et territoriales », Forum ATENA – 2009

Bruno Rasle

Co-auteur de :

- « Halte au spam ». Editions Eyrolles – 2003
- « La Sécurité à l'usage des Collectivités locales et territoriales », Forum ATENA – 2009
- « La physique selon Albert Ducrocq » Edition Vuibert - 2006

Yvon Rastetter

Auteur de :

- « Le logiciel libre dans les entreprises ». Editions Hermes – 2002
- « La fusion de la téléphonie dans l'internet ». Editions Hermes – 2005
- « Le logiciel libre dans la mondialisation ». Editions Hermes – 2006
- « Le logiciel libre dans les PME ». Editions 2008

Philippe Vacheyrout

Maitre d'œuvre pour :

- «Mediam » le site intranet de la branche maladie de la Sécurité Sociale www.mediam.ext.cnamts.fr/cgi-ameli/aurweb/ACI RCC/MULTI
- « Ameli » le site extranet de la branche maladie de la Sécurité Sociale www.ameli.fr/
- Pionnier de la carte Sésam Vitale www.sesam-vitale.fr/index.asp

Auteur de :

- Contribution de C@pucine.net au Sommet à Tunis 12/2005 www.capucine.net/article.php?id_article=8
- Contribution au Forum sur la Gouvernance d'Internet à Genève 02/2006 www.capucine.net/article.php?id_article=10
- Charte du « Réseau de Confiance Numérique » Capucine.net *6 www.capucine.net/article.php?id_article=15

A PROPOS DES AUTEURS

Par ordre alphabétique :

Christian AGHROUM est diplômé de l'Ecole Nationale Supérieure de la Police et titulaire d'un DESS en "politique et gestion de la sécurité". Responsable central de la sécurité des systèmes d'information de la Direction Centrale de la Police Judiciaire, il a dirigé durant quatre années l'OCLCTIC, l'office de lutte contre la cybercriminalité, jusqu'en juin 2010. Il a représenté la France dans des instances internationales et enseigné à l'ENSP, à l'ISEP et donné des conférences à l'ENA, l'ENM, l'IHEDN et l'INHES. Il vit dorénavant en Suisse où il exerce les fonctions de Chief Security Officer dans une grande entreprise internationale. *chrisagh (at) hotmail.fr*

Jean-Pierre ARCHAMBAULT, professeur agrégé de mathématiques, est chargé de mission veille technologique au CNDP-CRDP de Paris, où il assure notamment la responsabilité du dossier des logiciels libres, coordonnant le pôle de compétences logiciels libres du SCEREN. Il a participé au pilotage du développement des TICE dans l'académie de Créteil. Il est l'auteur de nombreux articles sur les usages pédagogiques et les enjeux des TIC. Il est président de l'association EPI (Enseignement Public et Informatique) et administrateur de la Société européenne de l'Internet. *jp.archambault (at) laposte.net*

Luc BARANGER a trente ans d'expérience dans le domaine de la sûreté. Il a créé et dirigé sa société d'installation en sûreté et communication dans le secteur industriel, tertiaire et le monde de la grande distribution, avant de devenir responsable des pôles techniques sûreté et communication à la F.F.I.E. (Fédération Française des Installateurs Électriciens) où il est responsable des Affaires Techniques et Expertise. *l.baranger (at) ffie.fr*

Jacques BAUDRON, spécialiste en architecture de réseau de transmission, dirige la société iXTEL qu'il a créée en 1998. Auparavant au sein des équipes d'architecture d'Alcatel il a travaillé sur la définition des réseaux et a contribué et animé des groupes de travail au sein de l'ITU-T et de l'ETSI pour la définition des architectures de protection dans les réseaux. Il est à l'origine de la gamme d'outils d'ingénierie de trafic et d'audit de réseau RetiTools tant sur les aspects routage, protection ou synchronisation. Jacques Baudron est également chargé de cours dans des écoles d'ingénieurs et universités et anime des séminaires auprès de professionnels : opérateurs, équipementiers, institutions. : *jacques.baudron (at) ixtel.fr*

Eric BOURRE est ingénieur IAM au sein du Cyber Security Customer Solutions Centre de EADS où il travaille sur des sujets tels que la PKI, la fédération des identités ou encore le contrôle d'accès. Diplômé de l'école nationale supérieure d'informatique et de mathématiques appliquées de Grenoble (ENSIMAG), il est également titulaire d'un master en cryptologie et sécurité des systèmes d'information. *eric.bourre (at) cassidian.com*

Jean Pierre CABANEL est Professeur à l'Institut National Polytechnique (INP / ENSEEIHT) de Toulouse et membre du laboratoire IRIT (Institut de Recherche en Informatique de Toulouse), équipe Université. Il anime un groupe de recherche sur le futur des télécommunications. Ses travaux récents traitent de l'autonomie des vecteurs aériens et spatiaux. Docteur d'état de l'Université Paul Sabatier à Toulouse,. il anime avec le Professeur Guy Pujolle le « Working Group » 6.4 de l'IFIP sur les LAN et PABX et organise plusieurs congrès au sein de Sup Telecom. Paris. Il travaille sur la problématique de la sécurité des systèmes de communication : PKI :, et Tiers de Confiance. *jeanpierre.cabanel (at) free.fr*

Ladji DIAKITE est diplômé de l'INSA de Lyon et de Télécom Paris Tech il a fait partie des projets de l'INRIA qui ont introduit UNIX en France (projets SOL et CHORUS sous les directions respectives de Michel GIEN et Hubert ZIMMERMAN). Il a ensuite mis son expertise UNIX et systèmes ouverts au service tour à tour de la banque, du génie logiciel, de l'imagerie médicale puis des télécommunications en dirigeant des projets ou départements R & D ou encore des services d'assistance aux opérateurs de réseaux. Il est actuellement responsable des secteurs data et télécom du syndicat professionnel des fabricants de fils et câbles énergie et télécom : *ladji.diakite (at) sycabel.com*

Michel ELIE, ingénieur ESE, chargé de projets de télématique à la CII à partir de 1965, a participé en 1969-70 comme assistant de recherche au groupe réseau NWG de l'Université de Californie à Los Angéles (UCLA), chargé de la conception du réseau Arpanet devenu par la suite Internet.. Il a ensuite été responsable de l'architecture de réseau de CII et de Bull jusqu'en 1988 puis associé à la direction de la recherche et du développement avancé de Bull.. A partir de 1995, il s'intéresse à la prospective de l'internet, particulièrement concernant ses usages à fort potentiel social et sociétal. En 1997 il participe à la création à Montpellier d' une association à but non lucratif , l'Observatoire des Usages de l'Internet (OUI) et aide plusieurs associations de terrain à utiliser l'internet comme vecteur de communication et de développement..

michel.elie (at) wanadoo.fr

Jean Christophe ELINEAU est responsable informatique dans une mutuelle. Président du pôle Aquinetic (pôle Aquitain de compétences en Logiciels Libres) et des Rencontres Mondiales du Logiciel Libre 2008 (Mont de Marsan). Il a fondé en 2005, Landinux, le Groupe d'Utilisateurs de Logiciels Libres (G.U.L.L.) pour le département des Landes.

jc.elineau (at) aquinetic.org

Franck FRANCHIN, travaille à la Direction de la Sécurité Groupe de France Telecom. Spécialiste depuis 20 ans en architectures sécurisées de systèmes civils ou militaires et en cybercriminalité, il est ingénieur diplômé de Supélec et de l'ENSEEIHT et titulaire d'un MBA de l'ESCP. Il mène aussi des recherches sur la résilience des infrastructures vitales dans l'équipe de la Professeure Solange Ghernanouti-Hélie de la Faculté des Hautes Etudes Commerciales de l'Université de Lausanne : *franck.franchin (at) bbox.fr*

Laura GARCIA VITORIA a été enseignante à l'Ecole Nationale d'Administration, à Paris IV -Sorbonne et à l'Institut National des Télécommunications. Elle dirige aujourd'hui, la Fondation des Territoires de Demain - dont elle assure par ailleurs la direction scientifique -. Elle dirige la Revue en ligne ARENOTECH et intervient régulièrement dans des rencontres internationales et livre ses chroniques à des portails internationaux.. Auteur de nombreux libres, articles et conférences, elle est régulièrement consultée par divers organismes internationaux sur le développement de stratégies basées sur l'innovation, la recherche et la créativité. *laura.garcia (at) arenotech.org*

Jean-Denis GARO, Directeur Communication et Marketing Support d'Aastra, est Titulaire d'un DEA Science et Technologie du CSTS, complétant un DUE à la Faculté de droit de Bordeaux et une école de Commerce dans la même ville.

Il a effectué sa carrière dans les IT, Matra Communication, Nortel Networks, EADS Telecom et Aastra. Administrateur du Forum ATENA, il est auteur de plusieurs ouvrages spécialisés. Il intervient dans les domaines touchant à l'évolution des usages dans les centres de contacts, les communications unifiées et collaboratives, la téléphonie IP, les solutions de vidéoconférence et les réseaux sociaux d'entreprises. *jgaro(at) aastra.com*

Gérard GAUDIN est Consultant indépendant en Sécurité des Systèmes d'Information, initiateur du Club R2GS (Recherche et Réflexion en Gestion opérationnelle de la Sécurité) créé au début de l'année 2009. Cette association, dont l'objectif premier est de mettre au point et de diffuser des pratiques de référence en matière de démarches SIEM et LID, regroupe au début 2011 une trentaine d'organisations et d'entreprises de différents secteurs d'activités parmi les plus avancées en France dans le domaine SIEM et LID. Diplômé de l'École Supérieure d'Électricité, Il a une longue expérience du marketing stratégique et du management de centres de profits importants au sein de grandes entreprises. : *gerard.gaudin2 (at) wanadoo.fr*

Thierry GAUDIN est Ingénieur Général des Mines, président de « Prospective 2100" (http://2100.org). Polytechnique (promotion 1959), Ecole des Mines de Paris, Docteur en Sciences de l'information et de la communication, Université de Paris X Nanterre (2008) : Thèse sur travaux : « Innovation et prospective : la pensée anticipatrice ». Fondateur et directeur du Centre de Prospective et d'Evaluation du Ministère de la Recherche et de la Technologie. Prospective 2100 est une association internationale ayant pour objectif de préparer des programmes planétaires pour le 21° siècle. Thierry Gaudin est vice-président de la Société européenne d'Internet : *gaudin (at) 2100.org*

Jean-Marc GREMY, **a**près une formation militaire dans la Marine Nationale débute sa carrière civile au sein de la R&D d'Alcatel Business Systems puis se tourne vers les TIC au sein d'Alcatel puis du Groupe Synthélabo. Entrepreneur, il participe en 1997 à l'éclosion de Cyber Networks et fonde en 2002 Ipelium. Fort de cette expérience réussie de 18 années dans la technologie, le management et l'entreprenariat, il créé en 2007 un cabinet de conseil indépendant CABESTAN CONSULTANTS.résolument tourné vers le conseil et la formation. Il est instructeur européen pour le cursus CISSP® et conférencier pour le Centre de Formation de l'ANSSI. *jmgremy (at) cabestan-consultants.com*

Jean-Yves GRESSER, X62, ENST 67, MSEE MIT ('68) a un passé de chercheur puis de directeur de recherches au CNET, de responsable informatique dans les télécom. et la finance (banque, banque centrale, assurance) puis de « dircom » et de mercatique sur la toile du premier groupe mondial d'assurance crédit (1998-2002).

Depuis, il continue de parrainer de jeunes innovateurs en Europe et aux Etats-Unis, dans le numérique et le cinéma, et d'inventer. Il est vice président du Black Forest Group Inc. (NY), membre fondateur de la Société française de terminologie, membre de plusieurs commissions spécialisées de terminologie et de néologie du dispositif d'enrichissement de la langue française et d'autres associations dont le Stéréo-Club de France, fondé en 1903. : *jgresser (at) noos.fr*

David GROUT est responsable avant vente chez McAfee. Titulaire d'un master en Informatique eBusiness, il est également titulaire de plusieurs certifications comme CISSP, Comptia Security +. Il est aujourd'hui à la tête d'une équipe de 5 personnes et gère l'ensemble du marché entreprise en France. Présent dans le domaine de la sécurité depuis plus de 7 ans il intervient aussi lors de séminaires ou de parutions dans la presse informatique : *David_Grout (at) McAfee.com*

Daniel GUINIER est expert en cybercriminalité près la Cour Pénale Internationale de La Haye. Docteur ès sciences, certifié CISSP, -ISSMP, -ISSAP, MBCI, expert judiciaire honoraire près de la Cour d'Appel de Colmar, Lieutenant-colonel (RC) de la gendarmerie nationale. Il est chargé de cours dans plusieurs universités. Il est l'auteur de plusieurs livres et de nombreuses publications. Il est Senior member de l'IEEE et de l'ACM, Emeritus member de la New York Academy of Sciences, membre du BCI et de l'AFSIN. *guinier (at) acm.org*

Daniel HAGIMONT est Professeur à l'Institut National Polytechnique de Toulouse et membre du laboratoire IRIT (Institut de Recherche en Informatique de Toulouse), où il anime un groupe de recherche autour des systèmes d'exploitation, des systèmes répartis et des intergiciels. Ses travaux plus récents concernent les systèmes d'administration autonomes. Il a obtenu un doctorat de l'Institut National Polytechnique de Grenoble. Après une année postdoctorale à l'Université de Colombie Britannique (Vancouver), il a rejoint l'INRIA en 1995 comme Chargé de Recherche. Il est Professeur depuis 2005. *daniel.hagimont (at) enseeiht.fr*

Bruno HAMON est fondateur et gérant de la société MIRCA, cabinet de conseil en sécurité du patrimoine informationnel. Avant de créer sa première entreprise EXEDIS, qui a rejoint le Groupe LEXSI, il a travaillé dans de grands groupes (SAGEM, SIEMENS, ZIFF DAVIS). Il a participé au lancement du site RueduCommerce.com. Il préside au sein de l'AFNOR le groupe de travail œuvrant sur les Plans de Continuité d'Activité. Il est chargé de cours à l'ISEP dans différents mastères. Avec 30 années d'expériences dans les NTIC, il participe à de nombreuses conférences. *bhamon (at) mirca.fr*

Mauro ISRAEL, en chinois **魔术师的净**, en leet, le langage des hackers 13^/37\/\/1≥≥, est expert en sécurité des systèmes d'information depuis plus de 25 ans. Il enseigne la sensibilisation à la sécurité, et effectue du hacking éthique et de nombreux audits de sécurité. Diplômé de l'Institut Supérieur du Commerce de Paris, Il a été programmeur de l'Armée Française, Master CNE Novell, Microsoft Certified Professional, ProCSSI de l'INSECA Pôle Universitaire Léonard de Vinci ainsi que ISO27001 Certified Lead Auditor. Il se concentre maintenant sur les aspects pratiques de la sécurité des systèmes d'information, les processus d'audit et de certification, et les plans de continuité d'activité. Auteur de livres et articles dans des revues spécialisées sur la sécurité, il est un expert international reconnu de la sécurité, blogueur et conférencier. *lenetwizz (at) gmail.com*

Dominique LACROIX a une formation initiale de lettres classiques (latin, grec, sanscrit) et de pédagogie. Après avoir travaillé dans l'édition, le cinéma et le journalisme, elle a été happée depuis plus de 15 ans par la micro-informatique, d'abord comme développeur de bases de données, puis de sites Internet et de réseaux sociaux. Elle se définit comme scribe. Elle se consacre aussi à l'animation de communautés Internet et à l'analyse des enjeux sociétaux internationaux de la généralisation de l'usage du web. Elle préside depuis 2010 la Société européenne d'Internet (http://ies-france.eu) qui a pour objet la pédagogie des questions soulevées par la gouvernance d'Internet. : *dl (at) panamo.eu*

Michel LANASPEZE est Directeur Marketing et Communication de Sophos pour l'Europe de l'Ouest. Diplômé de Télécom Paris (ENST) et du MBA de l'INSEAD, il contribue depuis 1996 à l'élaboration et la diffusion de solutions de sécurité pour le Web et les réseaux au sein de Bull, Evidian, UBIqube puis Sophos, après avoir participé à la conception de solutions d'administration pour SITA/Equant et Atos Origin. *michel.lanaspeze (at) sophos.fr*

SOPHIE de LASTOURS est docteur en Histoire militaire de la Sorbonne, possède un DESS de droit de la Défense et est ancienne auditrice du Chear, de l'IHEDN et de l'INHES. Elle dirige la collection Histoire de la Défense aux Editions l'Harmattan et écrit des scénarios sur l'Histoire du renseignement pour plusieurs sociétés de production. Elle a été désignée en juin 2010 comme expert de l'histoire du chiffre au sein du Conseil Supérieur de la Formation et de la Recherche Scientifique. Elle est membre de l'ARCSI : *sophiedelastours (at) hotmail.com*

François LETELLIER, est spécialisé dans l'innovation et l'entrepreneuriat dans les NTIC. Il a rejoint l'INRIA pendant quatre ans pour assurer le développement du consortium international ObjectWeb et la fondation de l'association OW2, dédiés au middleware open-source. Expert technico-économique auprès d'institutions de support à l'innovation au niveau français et européen, il conseille les sociétés sur leurs démarches d'innovation ouverte et leurs politiques logiciel libre et open source. Il dispense des cours sur l'économie du logiciel dans l'enseignement supérieur. Au cours de ses vingt années d'expérience, il a créé et édité des progiciels médicaux et été associé fondateur d'un cabinet de conseil et d'ingénierie informatique. *fl@flet.fr*

Fabrice MATTATIA est ancien élève de l'Ecole polytechnique, ingénieur de Télécom Paris, ingénieur en chef des mines, ainsi que docteur en droit, spécialisé dans le droit du numérique. Il a participé au projet français de carte d'identité électronique de 2004 à 2008, avant de devenir conseiller de la secrétaire d'Etat à l'économie numérique en 2009-2010. Il intervient dans plusieurs établissements d'enseignement supérieur et est l'auteur de plusieurs articles et contributions dans des publications aussi bien techniques que juridiques.

Fabrice.Mattatia (at) m4x.org

Jean PAPADOPOULO, Ingénieur en automatismes de l'Institut Supérieur de Mécanique et d'Electricité à Sofia (Bulgarie) est titulaire d'un doctorat de la Faculté de Paris. Il a développé chez Bull, une expertise en architecture et développement de systèmes informatiques de gestion ou scientifiques, microprocesseurs et de systèmes d'exploitation. Il a été Vice-Président du SIEPS (Syndicat des Industries Exportatrices de Produits Stratégiques) et architecte du projet qui a abouti à Tera10, le système le plus puissant d'Europe en son temps. Il a été conseiller relations industrielles au laboratoire PriSM, Université de Versailles et coordonnateur du projet ANR PARA (Parallélisme et Amélioration du Rendement des Applications). Actuellement il gére la SARL JP Etudes & Conseil. *jean.papadopoulo (at) gmail.com*

Jean-Claude PATIN dirige la société Juritel – qu'il a fondée avec ses associés – en 1995. Il est en charge du recouvrement et des nouvelles technologies.

Il a accompagné son premier client internet en 1995 dans le domaine de l'hébergement (hosting, housing, infogérance, cloud). Il intervient aujourd'hui essentiellement dans le cadre de mission de coordination et d'expertise pour de nombreux clients internet (publicité, data-center, applications, jeux en ligne, ...)

Gérard PELIKS est expert sécurité dans le Cyber Security Customer Solutions Centre de Cassidian, filliale d'EADS. Il préside l'atelier sécurité de l'association Forum ATENA, participe à la commission sécurité des systèmes d'Information de l'AFNOR et anime un atelier sécurité dans le cadre du Cercle d'Intelligence Économique du Medef de l'Ouest Parisien. Il est membre de l'ARCSI et du Club R2GS. Gérard Peliks est chargé de cours dans des écoles d'Ingénieurs, sur différentes facettes de la sécurité. *gerard.peliks (at) cassidian.com*

Guy PERROT est responsable normalisation corporate de la société Nexans pour les produits télécoms. Il participe aux travaux de normalisations sur les produits fibres optiques et haute fréquence et sur les protections électromagnétiques. Responsable normalisation pour les produits télécoms de Alcatel Câble, puis de la normalisation du secteur câble télécom, pour la société NEXANS, poste élargi aux câbles énergie. Il est président de plusieurs comités CEI, Cenelec et CEF. *Guy.Perrot (at) nexans.com*

Sadry PORLON est avocat au barreau de Paris

Docteur en droit, il est également chargé d'enseignements, au sein d'une école de commerce, notamment, en droit des médias et de la communication, en droit du commerce électronique et du multimédia ainsi qu'en droit des marques.

avocat (at) porlon.net

Philipe POUX est directeur au sein du cabinet Ellipsa

Spécialiste des nouvelles technologies et de la relation client, président de l'atelier Solutions Vocales de Forum Atena, fondateur des salons VocalExpo et MobilePaymentExpo, chargé de cours à l'Ecole Centrale d'Electronique.

philippe (at) vocalnews.info

Bruno RASLE est délégué général de l'AFCDP (Association Française des Correspondants à la protection des Données à caractère Personnel). Il a participé à la création de la première entité française dédiée à l'optimisation des réseaux et à la gestion des performances en environnement IP et s'est consacré ensuite à la protection des données stratégiques. Membre du groupe de contact anti-spam mis en place par la DDM (Direction du Développement des Médias, services du Premier ministre). Il intervient dans le cadre du Mastère Spécialisé « *Management et Protection des Données à caractère personnel* » de l'ISEP. *bruno.rasle (at) halte-au-spam.com*

Yvon RASTTETER est fondateur et gérant de la société Arts.Soft, start-up qui conduit des projets trans-disciplinaires dans lesquels coopèrent des artistes, des architectes, des spécialistes des TIC, des enseignants, des formateurs. Il a fait carrière dans de grandes entreprises en France et aux USA. Depuis 2009, il exerce une veille technologique sur le logiciel libre dans l'association Forum Atena.

rasteter (at) free.fr

Guillaume REMBERT est ingénieur de Télécom Lille 1. Il a effectué des stages puis des emplois : dans l'industrie métallurgique, la restauration, la communication, les télécommunications spatiales et terrestres. Il travaille actuellement à mi-temps au CNRS et réalise une formation entreprenariale à l'IAE. Il créera prochainement une entreprise de télécommunications (Systèmes d'Information et Systèmes de Communications Spatiales).

grembert (at) gmail.com

Guillaume RIBORDY dirige la société ID Quantique, qu'il a cofondée à Genève en 2001. Il a participé en 2007 au premier déploiement pratique d'une solution de cryptographie quantique pour le compte du gouvernement genevois. Avant de se lancer dans cette aventure commerciale, il a étudié la physique à l'Ecole Polytechnique Fédérale de Lausanne et obtenu son doctorat de l'Université de Genève. Ses travaux de recherche ont porté sur les applications pratiques des technologies quantiques de l'information, comme la cryptographie quantique et les

générateurs quantiques d'aléas. Grégoire Ribordy a étudié et travaillé en Allemagne, au Canada, aux Etats-Unis et au Japon.

Nicolas RUFF est chercheur au sein de la société EADS.

Il est l'auteur de nombreuses publications sur la sécurité des technologies Microsoft dans des revues spécialisées telles que MISC. Il dispense régulièrement des formations sur le sujet et participe à des conférences telles que SSTIC, les Microsoft TechDays ou la JSSI de l'OSSIR.

nicolas.ruff (at) eads.net

Yanis TAIEB est spécialiste des média et réseaux sociaux. Diplomé de l'ESG, puis chef d'entreprises, il forme les dirigeants et les cadres dirigeants à la mise en œuvre stratégique des média sociaux et accompagne les entreprises dans leur déploiement sur ces nouveaux média. Il anime des conférences et des tables rondes ainsi que des ateliers sur le sujet. Il est l'auteur du Blog : www.mediasociaux.net, source d'analyses sur ce phénomène qui connaît un développement spectaculaire. *yanis.taieb (at) winesight.fr*

Philippe VACHEROUT est président de Capucine.net

Entré à la Cnamts en 1975, il est à l'initiative de la création des Centres de traitements électronique inter-caisses et des Centres de traitement informatique de Saint-Etienne, Troyes et Rouen. La carte à puce citoyenne Capucine est une carte sans contacts, acoustique. Le son émis est différent à chaque fois, donc impossible à décrypter.

phvacheyrout (at) capucine.net