Un aperçu de l'histoire de la Sécurité des systèmes d'information*

Général Jean-Louis DESVIGNES

D'éminents spécialistes et historiens se sont déjà penchés sur l'histoire de la cryptographie, du chiffre, bref de tout ce que l'on qualifie communément de codes secrets et qui contribue à la préservation de la confidentialité d'informations que l'on ne souhaite pas partager. Les références ne manquent pas d'ailleurs, qui montrent l'importance de la maîtrise de ces techniques dont la force ou les faiblesses ont été jusqu'à changer le cours de l'Histoire.

Cependant, la sécurité des systèmes d'information dépasse le cadre de la confidentialité puisqu'elle englobe aussi bien la fiabilité du système lui-même qui doit garantir la disponibilité des informations qu'il traite, que l'authenticité des informations transmises, l'authentification des correspondants ou encore la non répudiation d'une transaction. En outre, les technologies modernes utilisées ont elles-mêmes engendré de nouvelles vulnérabilités d'ordre logique ou physique. De plus, l'interconnexion à outrance de tous les réseaux et systèmes que l'on observe aujourd'hui a ajouté une dimension nouvelle à la lutte traditionnelle que défenseurs de l'information et attaquants se livrent depuis la nuit des temps : le temps réel. La réactivité face aux attaques, que celles-ci soient ciblées ou massives, est la vertu principale que l'on demande aujourd'hui aux responsables informatiques.

Enfin, les enjeux se sont considérablement étendus. Si autrefois déjà, la divulgation d'une information pouvait avoir des conséquences fâcheuses sur le déroulement d'un conflit ou dans le cadre de négociations, aujourd'hui l'une des principales menaces qui planent sur nos sociétés tellement « techno dépendantes » est celle d'une opération de déstabilisation des rouages essentiels au bon fonctionnement d'un pays par le biais d'une attaque informatique conduite par des pirates chevronnés.

Dans la grande compétition mondiale, la SSI est devenue un des critères de discrimination entre les États. Face à la politique d'« information dominance » affichée ouvertement par nos grands alliés, il importe de ne pas perdre pied dans ce domaine capital.

*Cette communication a été donnée en introduction à la session sur la cryptologie lors du Colloque sur l'histoire de l'informatique, Rennes-Cesson, en 2004. Mais, elle n'a pu être insérée dans les *Actes* imprimés. Les numéros de page donnés ici sont ceux qui suivraient les dernières pages imprimées.

Bref historique de la cryptologie et de son contrôle par les États

Il existe dans l'antiquité de nombreux témoignages de l'usage de moyens visant à dissimuler le sens de certaines écritures aux yeux indiscrets. Le terme *cryptographie*, a d'ailleurs longtemps été le terme consacré pour désigner la science du secret, même lorsque celle-ci vint à être utilisée pour dissimuler autre chose que du texte (de la voix, des images, des données de toute nature …). Le plus connu des procédés antiques, en tous cas celui qui est traditionnellement enseigné aux apprentis chiffreurs, est la scytale, cette espèce de bâton de maréchal utilisé par les Lacédémoniens plus de cinq cents ans avant Jésus Christ. Le procédé consistait à enrouler de manière hélicoïdale un ruban de papyrus autour du fameux bâton et d'écrire le message dans le sens de sa matrice : une fois déroulé, le ruban ne présentait plus qu'une suite de caractères sans signification.

Bien que plus rudimentaire que le procédé antérieur de l'écrivain grec Polybe, le chiffre de César constitue la deuxième référence en terme de notoriété : celui-ci avait eu l'idée de décaler l'alphabet de trois lettres pour désorienter ceux qui auraient eu l'audace de s'attaquer à ses messagers. La scytale « transposait » les lettres d'un message tandis que César leur « substituait » d'autres caractères. Ces deux principes restent encore aujourd'hui à la base de la plupart des systèmes cryptologiques.

Le procédé de transformation constituait une convention secrète entre les correspondants. Celle-ci était composée, d'une part, de l'astuce elle-même (ex. le décalage des lettres ou la façon d'écrire sur le papyrus de la scytale), on parle aujourd'hui d'« algorithme » et d'un élément susceptible de varier (la valeur du décalage de l'alphabet de César ou le diamètre de la scytale) qui constitue ce que l'on appelle la clef.

Autrefois naturellement, l'astuce comme la clef devaient rester secrètes : une fois le principe connu, un « Jules César » est décryptable par un enfant sachant lire et écrire ; la scytale, sous réserve de ne pas être grosse comme un baobab, peut être attaquée en quelques minutes. Nous verrons plus loin qu'aujourd'hui, les algorithmes sont publiés et la résistance des procédés réside essentiellement dans la préservation de la confidentialité de la clef qui doit elle-même pouvoir résister aux essais systématiques.

Tout au long de l'Histoire, les procédés n'ont cessé d'évoluer. Les cryptologues, généralement des mathématiciens, des diplomates, des ecclésiastes et des militaires, déployèrent leur génie pour rendre les procédés plus résistants mais aussi plus simples d'emploi : le reproche maintes fois formulé par les chefs militaires impatients à l'encontre du chiffre résidait dans la lenteur des opérations de chiffrement et de déchiffrement. Il est intéressant de noter que, en cryptographie, la sophistication n'a pas toujours été un gage d'herméticité. Bien au contraire, elle a parfois

conduit à des régressions en matière de sécurité mais surtout, elle occasionnait des erreurs d'exploitation, des répétitions malencontreuses, voire des négligences, toujours propices à l'attaquant.

On ne peut citer tous ceux qui, durant ce qu'on appelle l'âge artisanal de la cryptologie qui s'étend de l'antiquité à la première guerre mondiale, ont contribué à faire progresser cette science ou cet art. Je mentionnerai néanmoins l'abbé allemand Trithème (1462-1516) dont le nom sera donné à une filiale de Thomson qui constitua en 1998 le premier tiers de confiance, le physicien mathématicien italien Porta (1534-1616) qui institua la notion de chiffre bigrammique, Vigenère (1523-1596) dont le procédé – le célèbre « carré de Vigenère » – inspiré de Trithème, ne fut décrypté qu'au milieu du XIX^{e} siècle et que l'on retrouve encore aujourd'hui dans certains systèmes informatisés ; Rossignol l'auteur du grand chiffre de Louis XIV, dont les compétences furent hélas rapidement perdues. Louis XVI, bien qu'honnête serrurier ne s'intéressa pas au chiffre ; il prononça la dissolution du cabinet « secret » créé par son père et négligea son « cabinet noir ». Une vague d'angélisme accompagna la révolution la constituante ayant institué le secret des correspondances et le niveau général de la cryptologie européenne s'affaissa. Pourtant, dans le même temps, un inventeur moins connu pour ses travaux de cryptologue que parce qu'il allait devenir un grand président des États-Unis, mérite d'être cité : Thomas Jefferson. Ce grand démocrate avait inventé en 1795 un petit cylindre à roues parfaitement apte à protéger des secrets d'État. Le commandant Bazerie réinventera, près d'un siècle plus tard, un dispositif très ressemblant.

On aborda le premier conflit mondial, il faut bien le reconnaître, avec des moyens cryptologiques qui n'avaient pas suivi l'évolution prodigieuse des télécommunications intervenues au dix neuvième siècle. Il s'en trouva un décalage entre la rapidité d'acheminement des dépêches transmises désormais à la vitesse de la fée Electricité et la lenteur des opérations manuelles et fastidieuses de chiffrement et déchiffrement.

Si le chiffre était manuel, les méthodes d'attaque l'étaient tout autant. Le décryptement relevait à la fois de l'analyse des textes chiffrés interceptés ou cryptogrammes (fréquence d'apparition des caractères selon la langue, particularités de celle-ci, nature du texte : diplomatique, militaires, commercial), de méthodes de prédilection de l'attaquant (intuition ou force brute) et d'actions plus traditionnelles des services de renseignement visant à s'assurer les confidences d'un responsable des service du chiffre adverse. À ce jeu plusieurs pays excellaient et les Français n'étaient pas les derniers. Mais ce sont les Allemands qui, au début du conflit, remportèrent les plus grands succès notamment à Tannenberg contre les Russes, non pas tant grâce à leur service de décryptement qu'en raison de la défaillance du chiffre des armées du Tsar : pour des raisons d'ordre logistique, les réseaux de chiffrement qui devaient être renouvelés furent inopérants et les ordres de mouvement furent communiqués en clair par radio HF par des généraux qui ignoraient

sans doute que les ondes ne s'arrêtaient pas sur la ligne de front. On peut s'interroger à juste titre sur le rôle de cette défaillance du chiffre russe sur la révolution bolchevique …

Sur le front de l'Ouest, les Allemands s'appliquaient à chiffrer leurs propres communications, mais c'était sans compter sur le génie du lieutenant puis capitaine Painvin qui, durant presque tout le conflit, réussit à percer les systèmes allemands ADFGX puis ADFGVX jusqu'à ce fameux télégramme dit « radiogramme de la Victoire », qui donna ou confirma les indices relatifs à la dernière offensive allemande. La confrontation filmée cinquante ans plus tard entre les deux principaux protagonistes Painvin, l'attaquant, et Fritz Nebel, le défenseur, est passionnante et parfois pathétique : on y voit le Français impitoyable décrire par le menu comment il s'est joué des perfectionnements que le pauvre Nebel s'épuisait à inventer et l'on assiste à l'effondrement de ce dernier, lorsqu'il découvre qu'il a sans doute contribué à la défaite de son pays.

De leur côté, les Britanniques, qui avaient été un peu pris de court dans cette forme de lutte, se rattrapèrent vite sous l'impulsion de Churchill (déjà). C'est à eux que l'on doit le décryptement du fameux télégramme « Zimmermann » qui entraîna l'engagement des États-Unis dans le conflit.

Avec l'entre deux guerres commença la deuxième époque du chiffre, celle de sa mécanisation, puis les machines – les « cryptographes » – devinrent électo-mécaniques et enfin électroniques. La plus célèbre des machines est certainement l'ENIGMA utilisée d'abord à des fins commerciales et dont seront dérivées différentes versions au profit du commandement allemand et notamment de la Kriegsmarine. Son principe reposait sur une série de disques ou tambours chiffrants dont la position relative et la rotation assuraient, par contact électrique, le caractère pseudo aléatoire de la substitution d'un caractère par un autre. L'opérateur appuyait sur la touche de la lettre qu'il voulait chiffrer ce qui provoquait après le positionnement des tambours, l'éclairage du caractère à lui substituer. Idem au déchiffrement. Les Polonais les premiers s'attaquèrent à cette machine, ils en vinrent même à la re-fabriquer en série.

Le tournant de la guerre

Les Français bénéficiant de la trahison d'un chiffreur allemand ne furent pas en reste et purent communiquer aux Anglais des informations importantes sur la manière d'attaquer la version militaire. Mais ce sont ces derniers qui mirent tout en œuvre pour venir à bout du chiffre allemand en construisant à Bletcheley Park leur fameuse « BOMBE » sous la direction du mathématicien Turing avec les conséquences que l'on sait sur le déroulement de la bataille de l'Atlantique. Certains affirment que c'est à Bletchley Park que fut réellement inventée l'informatique pour

répondre au besoin du décryptement. Même s'il fut plus discret que celui qu'il rendit aux pilotes de la RAF qui avaient gagné la bataille d'Angleterre contre la Luftwaffe, l'hommage de Churchill à ses cryptologues fut celui d'un homme parfaitement initié et conscient de la valeur inestimable des services que ceux-ci avaient rendus, dans l'ombre. N'avait-il pas accepté la tragédie de Coventry pour ne pas risquer de révéler aux Allemands que leur chiffre était cassé ?

Dans le Pacifique également, à la base des grands échecs des Japonais ou des grandes victoires des Américains, la domination de ces derniers en matière cryptologique s'est révélée déterminante. Vernon Walter, ancien ambassadeur US auprès des Nations unies et ayant eu une intimité certaine avec la plupart des grands, affirmait quelques mois avant sa mort lors d'une conférence en janvier 2003 à Coëtquidan que l'attaque de Pearl Harbour n'avait pas été contrée, seulement pour entraîner le peuple américain dans la guerre selon une version souvent entendue, mais aussi pour ne pas révéler aux Japonais que leur chiffre était percé. Midway, tournant de la guerre dans le Pacifique, est avant tout, même si cela n'entame en rien le génie stratégique de l'Amirauté, la valeur et le courage des marins et des pilotes qui y ont participé, une victoire du service du chiffre de la Marine américaine.

Un black-out sur la crypto

Lorsque quelques années plus tard, pour cause de guerre froide, des responsables allemands furent informés des exploits de Bletchley Parc, ils objectèrent : « si vous nous décryptiez si bien, vous auriez du gagner la guerre un an plus tôt ». « C'est ce que nous avons fait » ont répliqué les Alliés ! Inutile de dire que lorsqu'on dispose d'un avantage aussi substantiel, on ne va pas le clamer sur les toits et au contraire tout faire pour éviter de le perdre.

C'est pourquoi dès la fin de la guerre, toutes les questions portants sur la cryptologie vont faire l'objet de mesures d'embargo. Les moyens cryptologiques vont être étroitement contrôlés, les travaux des chercheurs et les publications surveillés tandis qu'une lutte intense va s'engager sur ce domaine entre les deux blocs. Une agence va être créée aux États-Unis, la célèbre NSA *(National Security Agency)* spécialisée en particulier dans le renseignement d'origine technique : les interceptions et le décryptement. C'est elle qui va en outre assurer le développement et/ou l'évaluation de tous les procédés de chiffrement du gouvernement américain et de ceux de l'OTAN. Au sein de cette agence qui comporte des dizaines de milliers d'employés est en effet installée une enclave particulière, appelée SECAN, chargée de contrôler la solidité de tous les moyens permettant de protéger les documents classifiés de l'Alliance.

Pourtant, le black out souhaité sur la cryptologie par les services de renseignement va être mis à mal en raison de la pression des milieux économiques qui eux aussi ont besoin de protéger la confidentialité de leurs échanges.

Une véritable révolution

C'est au milieu des années soixante dix que le Bureau national de standardisation des États-Unis, au terme d'une compétition remportée par la firme IBM décide de retenir, pour sécuriser les transactions financières, le fameux DES *(Data Encryption Standard)* et … de le publier. Bien que la suspicion demeure encore sur la solidité effective de ce procédé qui a reçu, avant qu'elle ne l'approuve, quelques modifications de la NSA, cette publication suscita quelque émoi dans la communauté du renseignement : le DES utilise des clefs qui, bien que ramenées de 64 à 56 bits, étaient pratiquement impossibles à attaquer par force brute, à l'époque, du moins dans des délais raisonnables.

De plus, cette compétition avait stimulé la recherche et c'est dans ces circonstances qu'intervint une autre découverte qui allait véritablement révolutionner la science du secret : Diffie et Hellmann eurent en effet l'idée géniale de s'affranchir du principe datant de l'antiquité consistant à partager, entre correspondants, le même secret, c'est-à-dire la même clef. L'idée était d'avoir une clef pour chiffrer qui pouvait être révélée (d'où le nom de système « à clef publique » donné à ce type de procédé) et une clef pour déchiffrer qui était privée et devait rester secrète. Tout le problème consistait à trouver une fonction mathématique irréversible liant les deux clefs. Plusieurs procédés furent proposés dont un par Diffie lui-même, mais c'est le trio Rivest, Shamir et Adleman, qui proposa deux années après cette idée lumineuse une solution qui reste encore aujourd'hui l'un des principaux standards asymétriques : le RSA (les initiales du trio) fondé sur la quasi-impossibilité de retrouver deux grands nombres premiers si l'on ne connaît que le produit de ceux-ci.

Ce procédé résolvait le problème le plus épineux des chiffreurs : celui de la mise en place des fameuses clefs qu'il fallait changer régulièrement et avec force précautions. Cependant, les calculs nécessaires sur les nombres premiers étant pénalisant en termes de débit, on ne se servira de ce procédé que pour transmettre de courts messages, par exemple, la clef d'un système symétrique performant.

Mais un autre avantage, qui allait se révéler d'une utilité extrême, fut découvert en inversant le procédé : si je chiffre cette fois, avec ma clef secrète, un court message, par exemple un identifiant, mon correspondant peut vérifier avec ma clef publiée que c'est bien moi qui l'ai envoyé. Je vais donc pouvoir « signer » mes messages. Si de plus, à mon identifiant j'ajoute un condensé de mon message obtenu par une fonction dite de « hachage » qui garantit que cette image réduite ne peut être

obtenue qu'à partir de mon texte, mon correspondant sera assuré de « l'intégrité » de celui-ci.

Cette sorte de mécano cryptologique est aujourd'hui à la base de toutes les transactions sans lesquelles le commerce électronique ne pourrait se développer.

Vers une libéralisation de la cryptologie

Evidemment, face à l'intérêt de ces développements, les règles de contrôle de la cryptologie par les États devaient évoluer : en France jusqu'en 1986, les moyens cryptologiques étaient assimilés à des matériels de guerre régis par un décret de 1939. C'était un peu gênant au moment où la France était pionnière en matière de paiement électronique grâce à l'invention des cartes à puce. Un premier assouplissement intervint qui permettait de faire sortir de ce régime certains équipements destinés à un usage commercial ou à des applications industrielles. Puis la loi de réglementation des télécommunications de 1990 se vit ajouter un article consacré à la cryptologie. Celui-ci était cependant toujours rédigé dans une optique de préservation des intérêts de la Défense nationale et les récriminations des industriels et des internautes de tendance majoritairement libertaire redoublèrent tandis que les exigences de la police, de maintien de ses capacités d'écoute, s'intensifiaient. C'est la loi de 1996 qui entama le processus de libéralisation. Elle rendit libre l'utilisation de moyens de cryptologie de force modérée (attaquable par force brute raisonnable : typiquement des systèmes à clef symétriques de 40 bits) et celle de moyens robustes à condition que ceux-ci utilisent des clefs gérées par un organisme agréé. C'était les fameux « tiers de confiance », une solution jugée comme le meilleur compromis pour, à la fois satisfaire les besoins de protection légitimes des utilisateurs et maintenir les capacités d'investigation de la police et de la justice. Ce dispositif original qui faisait reposer l'essentiel des contraintes sur les fournisseurs de moyens ou de prestation de cryptologie n'eut pas le temps de faire ses preuves et fut balayé par la libéralisation quasi totale de l'utilisation des moyens cryptologiques en 1999. Le gouvernement qui avait contribué au gonflement de la bulle Internet se laissa persuader que toute restriction à l'usage de la cryptologie nuisait au développement du commerce électronique. Les arguments sécuritaires furent balayés par la promesse du ministre des finances de fournir aux services ce qu'il faudrait pour casser ce qu'on aurait libéré, quand bien même il avait été démontré par le professeur Stern que c'était rigoureusement impossible …

La cryptologie toujours une arme de guerre

Après le 11 septembre, il y eut un moment de panique, et l'on vit des apôtres de la libéralisation « ramer » en sens inverse. Même M. Phil Zimmermann, qui avait

mis en libre circulation sur Internet son redoutable PGP *(pretty good privacy)* eut quelques frayeurs en imaginant que son système avait peut-être aidé Al Quaeda à commettre son horrible attentat. Les craintes émises avant la libéralisation étaient bien fondées : les criminels qu'ils soient des trafiquants, des pédophiles ou des terroristes savent utiliser les nouvelles technologies et celles qui peuvent dissimuler leurs méfaits particulièrement.

Aujourd'hui c'est « la loi pour la confiance dans l'économie numérique » de juin 2004 qui affirme, cette fois, la responsabilité de l'utilisateur (et non plus celle de son fournisseur), et lui impose de remettre à la justice les clefs qu'il aurait éventuellement utilisées pour commettre un crime ou un délit sous peine d'une aggravation sensible de sa condamnation … Mais le juge peut également faire appel aux services spécialisés pour décrypter les fichiers saisis ou les communications interceptées sans que ces services n'aient à fournir la preuve de la relation biunivoque entre le cryptogramme et le clair. À la lecture des batailles d'experts autour du décryptement du message de l'attaché italien dans l'affaire Dreyfus, on imagine les dérives que pourrait engendrer ce type de dispositif dans un contexte où la démocratie aurait un tant soit peu reculé.

Quoiqu'il en soit, aujourd'hui plus que jamais, les services doivent traiter avec les industriels pour contourner le problème cryptologique. C'est le règne des portes dérobées, des « *back doors* », ces mécanismes qui permettent d'accéder soit aux clefs utilisées, soit directement aux documents clairs avant que ceux-ci ne soient chiffrés.

Mais comme la plupart des industriels de l'informatique se trouvent aux États-Unis, il est facile de comprendre quels sont les services les mieux placés et les plus favorisés :ldots Inutile de dire que la sécurité apportée par les produits dont la seule garantie est la taille de leur clef est toute relative.

C'est pourquoi, en matière de SSI, il est important de ne pas se polariser sur une seule de ses composantes.

Les vulnérabilités nouvelles, nées des évolutions technologiques

Tant que les procédés de chiffrement restèrent manuels ou purement mécaniques, les seules vulnérabilités de ceux-ci résidaient dans la faiblesse de l'algorithme, celle de la longueur de la clef, et … les faiblesses humaines : erreurs, négligences ou trahison. Avec l'utilisation de l'électricité, une nouvelle source de fuite avait été introduite mais on s'en aperçut fort tard : les parasites. En effet, toute machine électrique comportant des contacts s'ouvrant et se fermant périodiquement génère des parasites. Un moulin à café comme une machine à écrire. Si vous vous rasez le matin en écoutant la radio et que soudain, votre réception est brouillée, vous vous direz : tiens ! le voisin n'a pas encore pris son petit déjeuner. Rien de très

compromettant. Mais si, lorsque vous frappez sur votre clavier, votre voisin peut, en utilisant un récepteur adéquat, recueillir et reconstituer le code à cinq ou huit moments que vous utilisez, et lire ainsi votre correspondance, c'est déjà plus gênant. Et si vous êtes un fonctionnaire des affaires étrangères en train de taper les dépêches de votre ambassadeur, cela devient carrément dramatique. C'est pourtant ce qui est arrivé à nos ambassades à Moscou et dans d'autres pays, pas seulement de l'Est, durant la guerre froide. Le colonel Cattieuw, ancien chef du service central du chiffre, estime que les Soviétiques nous ont ainsi espionnés pendant plus de six ans. Pour faciliter l'interception, ils piégeaient durant le transit de la valise diplomatique nos téléimprimeurs en introduisant dans un condensateur un micro émetteur qui amplifiait le phénomène de rayonnement compromettant. Pourtant sans être amplifiés, ces signaux se propageaient déjà très loin : durant les années quatre vingt, l'équipe de mesure de l'EMA réussissait régulièrement des captures d'écran à plusieurs centaines de mètres.

Pour l'anecdote, je voudrais vous rapporter l'histoire suivante. En 1985, j'étais affecté à l'EMA lorsqu'on nous livra la première station destinée à mesurer ces fameux signaux parasites. J'ai demandé au technicien à qui j'en avais confié la mise en œuvre : « allez donc faire le tour du ministère pour voir si vous captez quelque chose ». Il y est allé, il a vu et il n'a pas été déçu : « je ne savais pas que vous aviez décidé de m'envoyer à … la semaine prochaine … J'ai vu ça en interceptant la console du bureau des missions ! » a-t-il commencé par me dire. Certes, cette indiscrétion n'était pas dramatique, sauf que, sur le même ordinateur défilaient également les prévisions de voyage du CEMA … C'était l'époque de l'attentat contre le DC10 d'UTA. Sauf que, dans la foulée il avait réussi à capturer en se plaçant de l'autre côté du boulevard St Germain tous les écrans de l'EMAT alors équipé de micro-ordinateurs de marque GOUPIL particulièrement rayonnants. Ceux-ci firent pendant quelques années la joie des équipes de mesure qui se livrèrent alors à un concours de distance de capture … Si ce technicien avait réussi en moins d'une heure à visiter la plupart des bureaux, je me prenais à imaginer ce qu'un agent confortablement installé dans une chambre de bonne de l'autre côté du boulevard pouvait recueillir à longueur d'année. Bah ! « on a sans doute contribué à la saturation du KGB et à la victoire de 1989 » diront les officiers traitants de l'époque …

Dans le jargon de l'OTAN, on a appelé ce phénomène la menace « TEMPEST ». Elle concerne tous les équipements de traitement de l'information et naturellement les équipements de chiffrement. Ainsi, un équipement mal conçu transmet certes, un cryptogramme mais en même temps peut émettre, sous forme atténuée, le signal clair. Celui-ci peut se propager très loin pour peu qu'il bénéficie d'un support conducteur fortuit (un tuyau de chauffage, une ligne électrique,...) ou d'un couplage favorable avec un moyen de télécommunication (un téléphone, un émetteur radio,...). Dès que cette menace fut identifiée, les Américains imposèrent à

l'OTAN des normes très sévères touchant d'une part les matériels, d'autre part les installations. Ces normes, au passage, contribuèrent à éliminer des compétitions industrielles un bon nombre de pays. Ce n'était peut-être pas l'objectif au départ, mais ces normes hautement classifiées, difficiles à atteindre, contribuèrent à leur manière à la lutte contre la prolifération cryptologique... En France il fut relativement facile de convaincre les états-majors d'adopter des mesures pour contrer cette menace car les démonstrations étaient très spectaculaires. Pourtant, la parade, extrêmement coûteuse, car elle aboutissait à faire doubler, voire quadrupler le prix des matériels et des installations, fut prise en compte au moment où une menace d'une tout autre ampleur apparaissait : celle qui résultait de la vulnérabilité des systèmes informatiques. Pourtant, cette menace, même si elle a perdu de son importance en particulier parce que les ordinateurs rayonnent peu, reste d'actualité car elle doit englober d'autres vulnérabilités liées aux facilités offertes aujourd'hui comme les systèmes sans fil. Mais le danger principal se situe surtout au niveau des installations et des plates-formes qui favorisent le couplage entre différents équipements de traitement et/ou de communication.

Les vulnérabilités nouvelles, nées avec l'informatique et les réseaux

Comme on l'a vu, l'informatique s'était développée avec Turing durant la Guerre pour casser le chiffre allemand. Mais très rapidement elle a trouvé ou retrouvé sa place dans tous les domaines nécessitant de grosses capacités de calcul. Du reste les premières applications de traitement automatique des données réalisées avant guerre à des fins de statistiques ou de comptabilité avec des machines plus mécaniques qu'électronique, furent privilégiées. Il y eut d'abord l'époque des gros ordinateurs centraux : on se préoccupait alors plus du bon fonctionnement de ces machines que d'une quelconque possibilité d'en corrompre la logique. Très rapidement cependant, nos très chers informaticiens eurent à cœur de relier ces ordinateurs entre eux, à la demande des chercheurs souhaitant partager leurs travaux. C'est effectivement sur des crédits du DOD américain que furent reliés entre eux les centres de recherche et centres de calcul travaillant à son profit à travers un réseau d'un genre nouveau. Le réseau ARPANET, c'est son nom, peut être considéré comme l'ancêtre d'INTERNET. Ce réseau « à commutation de paquets » était maillé et reposait sur le principe du « datagram » : chaque paquet ou élément d'un message circule de manière indépendante de ses congénères, en empruntant le chemin qui lui semble le plus rapide. À l'arrivée, la machine du destinataire se charge de recoller les morceaux du message ou du fichier dans le bon ordre. Ce réseau était censé, en principe, résister à la destruction par atomisation de plusieurs de ses nœuds.

En France dans le même temps, se développait le réseau Transpac reposant sur un autre principe, celui du circuit virtuel défini par la norme X25 du CCITT : le premier

paquet, appelé paquet d'appel, se chargeait de tracer la route, et les suivants se dépêchaient de lui emboîter le pas. Il se trouve que j'eus à choisir entre les deux principes pour réaliser le réseau de l'armée de terre RETINAT. J'optai rapidement pour le second, d'abord parce que d'un point de vue économique il valait mieux coller au plus près à ce que faisait TRANSPAC, à l'époque l'opérateur le plus en pointe au niveau mondial, ensuite parce que je craignais moins le risque de perdre une partie de message pour cause de vitrification que de voir le réseau auto-saturé par des boucles de paquets fous ne trouvant pas la sortie. Les tares congénitales d'ARPANET n'ont pas totalement disparu avec Internet bien au contraire. Elles sont heureusement compensées par la puissance informatique dont disposent aujourd'hui les utilisateurs pour rattraper les erreurs du réseau. D'ailleurs, on tente tant bien que mal de réintroduire sur Internet certains mécanismes éprouvés des réseaux X25 et du minitel tant décrié.

C'est surtout quand les ordinateurs furent ainsi en réseau que les problèmes de sécurité informatique furent médiatisés, les mésaventures touchant un grand nombre de gens : la détresse du pauvre informaticien solitaire ne pouvait émouvoir les masses. En revanche, quand en 1978, un des premiers virus contamina plus de six mille ordinateurs en moins de 24 heures, cela fit quelque bruit.

Pourtant bien au paravent, quelques pirates en col blanc s'étaient déjà livrés à des détournements de technologie sur des systèmes centraux bien isolés du reste de la planète. On cite souvent parmi les premiers cas, celui de cet informaticien qui avait imaginé ouvrir un compte qu'il était le seul à connaître en l'approvisionnant avec tous les centimes récupérés sur les arrondis résultant des opérations de la banque qui l'employait. Au bout du compte il s'était constitué un petit magot.

Le télégraphe de Chape et le délit d'initié

De tout temps les technologies nouvelles ont stimulé l'imagination des aigrefins. Imaginez que le télégraphe de Chape lui-même a servi à deux employés de la ligne qui reliait Paris à Bordeaux pour boursicoter avec succès : ils profitaient de la séquence des messages de service (les répétitions de messages erronés par exemple) pour se communiquer les cours du vin à Bordeaux anticipant ainsi de 24 heures les fluctuations annoncées le lendemain à Paris par voie de presse. Pris de remords, l'un d'eux se dénonça sur son lit de mort. Le cocasse dans cette histoire fut que son complice survivant ne put être condamné le délit n'ayant pas encore été codifié. En tout cas c'est certainement un exemple historique de l'utilisation de ce qu'on appelle les « canaux cachés » dans un système informatique. C'est d'ailleurs le mode de pénétration de prédilection des pirates (ou de leurs agents logiciels) qui s'introduisent dans votre ordinateur pendant que vous vaquez à vos occupations sur la toile. Parfois avec votre consentement, souvent sans, de petits programmes accompagnent les emplettes que vous êtes allés faire sur le réseau. Ce

sont les « *cookies* », souvent bienveillantes, facilitant vos recherches ou servant à renseigner vos fournisseurs sur votre profil, vos goûts, vos petites habitudes, etc. Mais il y a aussi les cadeaux du stroumpf farceur qui vont vous polluer l'existence ou pire, détruire ou voler vos données.

Comment mesurer la confiance ?

Les Américains les premiers ont tenté de codifier des critères permettant de noter les systèmes informatiques en fonction de la confiance qu'on pouvait leur accorder sur une échelle comprenant cinq niveaux. Ils ont en particulier défini un certain nombre de mécanismes à implanter pour instaurer la confiance. L' « *orange book* » diffusé au sein de l'OTAN au début des années quatre vingt a constitué longtemps la seule référence en matière de sécurité informatique. Cependant, quatre pays européens (AL, R.U, P.B et FR) ont compris que ces normes allaient devenir une arme économique et ont répliqué, d'abord en ordre dispersé, avec un livre de couleur chacun, puis ensemble avec ce qui est devenu la référence européenne : les ITSEC *(information technology security evaluation criteria)*. Ces critères enrichirent les travaux américains en cherchant en particulier à mesurer non seulement la présence mais la pertinence et l'efficacité des mécanismes de sécurité. Enfin les cinq pays se sont mis au travail pour rédiger des « critères communs » qui sont devenus en 1999 une norme ISO. Une notion originale a été introduite dans ceux-ci : celle de « profil de protection ». Il s'agit de définir, pour un type de ressource informatique donné (un système d'exploitation, une carte à puce, un pare-feu, un dispositif de contrôle d'accès, etc.) et un type ou une communauté d'utilisateurs (les médecins, les banques …) face à un ensemble de menaces identifiées, une cible de sécurité générique auquel les industriels doivent se conformer. Des laboratoires agréés procèdent à la vérification de ces profils au cours d'une évaluation. Si celle-ci est positive, le produit peut lors être certifié au niveau requis par l'État (c'est aujourd'hui la Direction centrale de la sécurité des systèmes d'information qui délivre ces certificats). Ce dispositif est complété par des accords de reconnaissance mutuelle des certificats signés entre un certain nombre de pays.

Des cyber-SAMU

Cependant, si l'on a aujourd'hui un bon thermomètre permettant de connaître le niveau de sécurité d'un outil informatique, le niveau le plus élevé est très difficilement atteint et pour ainsi dire jamais. C'est pourquoi il est nécessaire de combiner des mesures techniques et des mesures organisationnelles : aucun système ne peut être à l'abri d'une attaque en particulier si celle-ci est conduite de l'intérieur. La sécurité absolue n'existant pas, des mesures curatives doivent être envisagées

pour compléter les mesures préventives. En matière de technologie de l'information et de la communication, on est passé d'une politique d'élimination du risque à une politique de gestion de celui-ci. Pour cela, des cellules de veille ont été instituées pour monter la garde sur les réseaux et venir en aide aux victimes des pirates. C'est l'expérience de 1978 qui a permis de faire prendre conscience de ce besoin : en effet face à une attaque d'une ampleur inédite furent rapidement réunis les meilleurs experts. Ceux-ci, conjuguant leurs compétences, découvrirent en moins de vingt quatre heures le virus et le remède pour l'éradiquer en le transmettant lui aussi par le réseau. Devant le succès de cette contre attaque, il fut décidé de créer une, puis plusieurs cellules sur le modèle de celle qui avait réussi. C'est ce qu'on appelle un CERT *(computer emergency response team)* sorte de SaMU ou de caserne de pompiers capables de déceler une attaque, de l'analyser, puis de diffuser l'alarme et les remèdes. La France dispose ainsi depuis 1999 d'une telle cellule pour les besoins de l'Administration et les armées d'une organisation de veille, d'alerte et de réponse qui lui est reliée.

Des puces inquiétantes

Sommes-nous protégés pour autant ? Il faudrait être bien optimiste pour le penser car nous ne maîtrisons que rarement les technologies sur lesquelles reposent nos systèmes d'information. Les Américains ont aujourd'hui des objectifs de sécurité qui les conduisent à lutter dans le cyberespace avec les moyens que peuvent leur offrir les grandes firmes informatiques. Heureuse coïncidence : les techniques antipiratage mises au point conjointement par les fabricants de puces et les éditeurs de logiciels pour lutter contre les copies illicites des logiciels ainsi que des oeuvres cinématographiques ou musicales permettent bien d'autres choses en matière d'espionnage, comme s'en alarme un universitaire britannique, Ross Anderson. S'est ajouté depuis le 11 septembre 2001 à ces ouvertures techniques, un arsenal juridique permettant de mener les investigations policières dans le domaine des technologies de l'information et de la communication dans des conditions que n'osaient plus, au paravent, espérer les services de sécurité.

Aussi, combien de Fritz Nebel y-a-t il dans notre pays, certains qu'ils sont d'avoir tout mis en oeuvre pour mettre leurs petits secrets à l'abri des yeux indiscrets et qui pourtant, découvriront un jour que ceux-ci étaient en accès libre ?

Les enjeux de la SSI au XXI^{e} siècle

À travers ce que nous avons déjà vu, il semble évident que la sécurité des systèmes d'information revêt une importance capitale pour un pays qui a un tant soi peu le souci de rester maître de son destin ou pour une entreprise soucieuse de

renforcer sa compétitivité surtout à l'international. Même s'il est concerné à un moindre degré, l'individu lui-même exprime aujourd'hui un besoin de confiance dans les technologies qu'il choisit d'utiliser ou qui lui sont imposées dans ses rapports avec l'administration et la société. À ce besoin de confiance s'ajoute le souci de protection de ses libertés individuelles et de sa vie privée.

Les enjeux pour l'État

Un État doit assurer la protection de ses citoyens. C'est sa mission originelle et pour ce faire il doit en premier lieu être en mesure d'apprécier lui-même les situations et ne pas se laisser guider par des informations orientées. Des exemples récents montrent à quel point l'État, surtout s'il affiche haut et fort son indépendance, doit posséder son propre système d'information et sa propre capacité d'analyse. Naturellement ce système d'information exige le plus haut niveau de garantie quant à sa disponibilité, sa résistance à toute forme de pollution et de corruption et, bien sûr, sa confidentialité. Ne serait-ce que pour satisfaire ce besoin de confiance dans son système d'information, l'État doit disposer des compétences et des ressources propres à lui assurer la fourniture de moyens hors de tout soupçon.

Or, sur ce plan notre pays, même s'il se situe dans le peloton de tête en matière de technologies de l'information, se trouve dans une position de grande dépendance vis à vis de son grand allié au plan informatique, notamment pour l'informatique d'usage courrant, la bureautique, que l'on retrouve jusque dans les systèmes opérationnels de nos forces armées. À ce titre, les risques que l'on évoquait précédemment sont bien réels. Sans être paranoïaque, il est pour le moins hasardeux de confier sa correspondance à un automate programmé pour rendre compte à un autre maître.

Bien sûr il existe des parades à ce danger et l'on peut réussir à bâtir des forteresses malgré l'existence de mines et de sous-terrains traversant les fondations. Mais les travaux de consolidation sont toujours lourds et coûteux et imposent des règles d'utilisation qui font perdre une bonne partie des avantages de l'informatique. Ainsi, la procédure de nettoyage imposée sur un terminal pour passer d'un traitement d'information d'un niveau de confidentialité supérieure à celui d'information d'un niveau inférieur a-t-elle été suffisamment pénalisante pour entraîner le rejet de certains systèmes.

Une échappatoire à cette dépendance pourrait résider dans le recours au développement de produits sous licence libre. Il est regrettable que l'État français, tellement attaché à son indépendance dans d'autres domaines, comme l'espace ou le nucléaire, ne se soit pas fait le champion de cette démarche au niveau européen. L'échec du plan calcul a sans doute contribué à l'inaction de notre pays dans ce domaine. Il n'est cependant pas trop tard. On voit d'ailleurs des pays qui ont compris

qu'on ne pouvait pas laisser à l'industrie américaine et accessoirement, à son gouvernement, le monopole des technologies de l'information, consentir des efforts gigantesques pour voler de leurs propres ailes en développant leurs propres outils. Le Japon, la Chine et l'Inde ont de tels programmes. L'Europe serait bien inspirée de les imiter.

Il convient de saluer l'initiative de la DGA qui avec le projet SINAPSE vise à disposer d'un système de confiance fondé en particulier sur l'utilisation du « logiciel libre » LINUX.

Conserver son autonomie de décision et de réaction en toutes circonstances c'est bien. Mais il faut également assurer le fonctionnement de ce qu'on appelle aujourd'hui les infrastructures vitales du pays. C'est à dire, ses réseaux de transport d'énergie, de distribution dont le fonctionnement peut être gravement perturbé par les actions de « cyber terroristes ». Le recensement des réseaux critiques a été entrepris et des exercices d'alerte et de simulation d'attaque sont aujourd'hui pratiqués pour vérifier l'aptitude des responsables informatiques à rétablir une situation dégradée.

L'État, ensuite, doit, sur le plan de la sécurité intérieure, donner à la police et à la justice les moyens de lutter contre l'utilisation délictueuse et criminelle des technologies de l'information. À ce titre, il dispose aujourd'hui de l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication qui peut faire appel en outre aux compétences d'autres services étatiques.

Sur le plan économique, l'État doit également permettre à nos entreprises de se battre à armes égales dans la grande compétition internationale dans laquelle la bataille informationnelle ne joue pas le rôle le moins important.

Enfin, dans la recherche d'une amélioration de sa productivité administrative, l'État doit veiller à instaurer la confiance dans les téléprocédures qu'il met en place.

Les enjeux pour les entreprises

Longtemps, la SSI dans les entreprises, a été traitée comme dans l'administration : une contrainte à laquelle on ne se plie que par obligation. De nos jours tout de même, des efforts ont été consentis parce que l'outil informatique devenu indispensable est parfois rendu indisponible par les attaques virales. Ces attaques, non ciblées en général, qui perturbent parfois gravement le fonctionnement d'une entreprise, ont permis de sensibiliser les responsables à la problématique plus large de la SSI : « Si un programme malicieux est capable de s'introduire dans mon système pour m'empêcher de travailler que peut-il faire d'autre ? ». Les entreprises ont donc rapidement assimilé les risques qu'elles encouraient : cela va de l'attaque de l'image de la société jusqu'à la disparition de celle-ci, en passant par des pertes de

parts de marché, la perte de confiance ou le refus de coopérer d'autres sociétés plus averties. Un progrès décisif sera accompli lorsque les banques et les assureurs de ces sociétés exigeront des certificats garantissant que leur système d'information est protégé à un niveau suffisant.

Pour certaines professions impliquant des règles de protection du secret professionnel, des négligences dans le traitement de données personnelles peuvent conduire les responsables devant les tribunaux.

Naturellement je ne parlerai pas des entreprises travaillant sur des domaines sensibles comme ceux de la Défense puisque la protection de leur système est une condition sine qua non de l'exercice de leur activité.

Les enjeux pour les individus

Le citoyen est entré, bon gré mal gré, dans la société de l'information. Si tous ne sont pas encore des accros de l'Internet, la plupart utilisent déjà des technologies dont certaines possèdent des fonctions de sécurité : les cartes bancaires ou de santé, les serrures électroniques de voiture, la télévision à péage, etc. De plus en plus l'Administration s'informatise et remplace les échanges sous forme de papier avec les administrés par des « télé procédures ». Ainsi pouvons-nous déclarer nos revenus et payer nos impôts par Internet. De même le secteur bancaire a-t-il très tôt introduit la consultation des comptes et le paiement en ligne. Même s'il ne s'est pas développé aussi vite qu'on nous l'avait annoncé, le commerce électronique commence à entrer dans les mœurs. Dans l'ensemble, le public est favorable à cette évolution qui contribue grandement à simplifier et accélérer ses démarches. Cependant la condition pour que cette modernisation soit acceptée, est que soit instaurée la confiance : la divulgation d'un numéro de carte bancaire sur l'Internet est encore une opération risquée. Si la carte Vitale contient le dossier médical du patient comment sera-t-il protégé ?

Par conséquent, pour l'individu, les enjeux portent essentiellement sur la sécurité de son portefeuille et la protection de sa vie privée. Naturellement si on peut lui offrir la garantie qu'en se mettant au volant de son ordinateur il ne sera ni dérangé par des messages publicitaires indésirables (le SPAM) ni obligé de se battre contre les virus et que s'il souhaite envoyer un billet doux à sa dulcinée il pourra le faire sans craindre d'être lu, l'internaute sera ravi. Cette offre existe mais elle est, comme on l'a vu, accompagnée du risque de subir un contrôle permanent du contenu de son ordinateur.

Conclusion

L'histoire de la cryptographie a commencé il y a plus de 2 500 ans, suivant apparemment d'assez loin l'invention de l'écriture, sans doute parce que celle-ci constituait déjà une barrière infranchissable pour nombre de gens : les hiéroglyphes n'attendirent-ils pas Champollion quelques millénaires ? L'histoire de la sécurité informatique, elle, a commencé il y a environ 25 ans, c'est-à-dire peu de temps après l'avènement de l'informatique, elle-même née, rappelons-nous, de la lutte contre le chiffre. L'étape suivante, nous dit-on, ce seront les ordinateurs quantiques dont la puissance dépassera tout ce que nous pouvons imaginer et qui devraient venir à bout de la cryptographie mathématique. Mais cette fois les chiffreurs ont pris les devants : il se pourrait que des procédés de cryptologie quantique soient disponibles avant les ordinateurs. Des essais ont même commencé.

Dans la lutte ancestrale entre l'épée et la cuirasse, le combat était à peu près resté équilibré. Récemment, on a pu croire que la cuirasse l'avait définitivement emporté quand sont apparus des algorithmes soumis à la sagacité de toute la communauté internationale et utilisant des clefs surdimensionnées. Malheureusement ces procédés, impossibles à mettre en œuvre autrement qu'en recourant aux techniques électroniques et informatiques souffrent des vulnérabilités que celles-ci comportent quand elles ne sont pas développées et exploitées dans un environnement de confiance.

Gageons qu'il en sera toujours ainsi. Au demeurant, dans le système le plus sécurisé qui soit, l'homme restera toujours le maillon faible. Mais qui voudrait le voir sortir ?