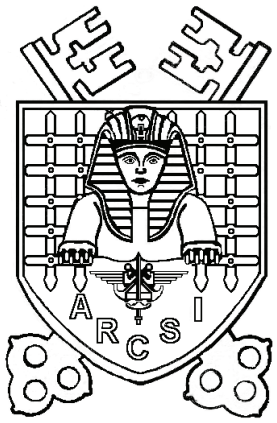

ASSOCIATION des RESERVISTES du CHIFFRE et de la SECURITE de L'INFORMATION

Nouvelle série
n° 28 - 2000

Document interne à l'Association
Réservé aux adhérents

5 . La cryptologie et le renseignement

En hommage au colonel Pierre BENAITEAU, président de l'ARCSI[1] (Association des Réservistes du Chiffre et de la Sécurité de l'Information), spécialiste du Chiffre, décédé le 3 septembre 1999.

La cryptologie et les questions relatives au chiffrement sont au cœur de l'actualité en France. La cryptologie est un domaine en pleine révolution ; historiquement principalement militaire et diplomatique, elle est devenue civile et a pénétré dans notre vie quotidienne. La carte à puce, le commerce électronique, la télévision, la radiotéléphonie en dépendent. Elle touche à la sécurité de nos sociétés : sécurité des réseaux, des ordinateurs, des dossiers médicaux, signature électronique...

Elle prend une importance particulière avec l'essor d'Internet : on doit assurer la sécurité des transactions commerciales, garantir la confidentialité des informations et protéger la vie privée. Les logiciels de courrier électronique comportent désormais une option de cryptologie. Cette technique est longtemps restée en France sous contrôle gouvernemental mais depuis 1996 la législation s'est progressivement assouplie. Un décret du Premier Ministre de mars 99 autorise même les particuliers à utiliser librement une clé de chiffrement d'une longueur de128 bits (ce qui permet 2^{128} combinaisons). Deux principales méthodes de chiffrements existent aujourd'hui : la cryptologie à clé secrète et celle à clé publique[2].

Définissons les deux techniques de chiffrement.

Clé secrète : Méthode qui permet de chiffrer le texte à l'aide d'une opération utilisant une clé unique et secrète que le destinataire emploie dans l'autre sens pour déchiffrer et ainsi retrouver le message originel. Aujourd'hui, les méthodes modernes utilisent des transformations basées sur les mathématiques. Plus la clé employée est longue plus le message est difficile à décrypter. Une clé de 40 bits permet 2^{40} possibilités (soit plus de mille milliards). Certains logiciels de décryptement emploient la "force brute" c'est à dire qu'ils explorent systématiquement les 2^{40} possibilités[3] l'une après l'autre. (C'est comme si un cambrioleur essayait systématiquement toutes les combinaisons d'un coffre-fort pour l'ouvrir.) Ces logiciels nécessitent des ordinateurs très puissants comme "deep crack" qui réussit cette opération en 12 secondes, mais qui coûte la modique somme de 1.5 million de Francs. Si la longueur de la clé s'allonge, le temps nécessaire pour le décryptement augmente de façon exponentielle :
60 bits : plus de 3 heures ; 70 bits : 5mois ; 80 bits plus de 400 ans...

Un ordinateur plus puissant mettra moins de temps, néanmoins un système de chiffrement doté d'une clé à 128 bits est aujourd'hui incassable même par les plus gros ordinateurs de la planète, sauf si par exemple une partie des 128 bits n'est pas totalement inconnue de l'attaquant. Les systèmes de chiffrement à clé secrète les plus employés sont : le

[1] l'ARCSI s'est d'abord appelée AORSC en 1928, puis ARC en 1948.
[2] Nous l'expliquons plus loin.
[3] On trouve en moyenne la clé avant d'avoir exploré la moitié des possibilités, c'est à dire $2^{39.}$

DES (Data Encryption Standard) qui est basé sur une clé de 56 bits, l'IDEA (International Data Encryption Algorithm) utilisant une clé de 128 bits comme le "Blowfish"

Clé publique : méthode qui permet de chiffrer le texte à l'aide d'une clé publique et non secrète, le déchiffrement s'opérant grâce à une clé secrète liée à la clé publique par une relation mathématique telle que, connaissant une des deux clés, il est matériellement impossible d'en déduire l'autre. Le procédé le plus connu est le système RSA qui repose sur la difficulté de décomposer en facteurs un grand nombre (de plus de 130 chiffres) qui est le produit de deux nombres premiers. Chaque utilisateur dispose d'un couple clé publique - clé secrète, sa clé publique est connue de ses correspondants, elle peut par exemple figurer dans un annuaire spécialisé. Tous ceux qui connaissent la clé publique d'un utilisateur peuvent chiffrer un message avec cette clé et lui envoyer. Le destinataire est seul capable de déchiffrer à l'aide de sa clé secrète le message crypté reçu, inversement un texte chiffré à l'aide de sa clé secrète identifie son auteur. Quiconque connaît la clé publique peut déchiffrer le cryptogramme qui n'a pu être chiffré que par le détenteur de la clé secrète. C'est la base de la signature électronique, actuellement en cours de légalisation par la Justice. C'est un élément capital pour la sécurisation des transactions bancaires et du commerce électronique.

La cryptologie et la cryptanalyse ont longtemps été l'apanage des militaires et des diplomates, même si les entreprises commerciales chiffraient parfois leurs transactions[4].

1) Le Chiffre et l'Histoire

Il n'y a guère de grands moments de l'Histoire qui n'aient été le théâtre d'un combat entre gens du chiffre. Le Chiffre est une arme complémentaire des autres et parfois même la meilleure de toutes. Présent lors des guerres de religions, de la guerre d'Indépendance américaine, de la Révolution française, de l'Empire napoléonien, de la guerre de Sécession, des deux guerres mondiales, de la guerre froide...
Il est également la clé de voûte du monde du renseignement, de l'institution militaire, de la diplomatie, de la sûreté de l'Etat.

Le renseignement est une construction qui inlassablement exige des nouvelles "pierres" pour le compléter et le renouveler. On pourrait d'ailleurs faire une histoire des conflits par la seule étude des radios ou dépêches décryptées.

En 80 ans, le chiffre a connu une véritable mutation tant dans les moyens de chiffrement que dans le profil des chiffreurs. Le premier conflit mondial va exploiter cette discipline d'autant plus intensément que le progrès met de nouveaux outils à la disposition des belligérants : le téléphone, la télégraphie sans fil, la radio, les écoutes et la radiogoniométrie. La multiplication des messages favorisée par la technique, l'étendue et la mobilité du front obligent à communiquer en langage secret. Par la suite on est ainsi passé du chiffre manuel "crayon-papier" de la première guerre aux machines de la seconde guerre comme Enigma, Red, Purple, à la KL7 à rotors de l'OTAN puis plus tard à Myosotis pour arriver au chiffre électronique intégré dans les moyens de communication et les terminaux. Les services de décryptement anglo-américains ont accumulé les succès sous le nom bien connu d' ULTRA et MAGIC[5], mais la Section du Chiffre de l'Etat-major français a aussi décrypté entre septembre

[4] Les exemples abondent dès l'Antiquité et particulièrement au Moyen-âge. La célèbre américaine Edith Wharton (1868-1937)mentionne un message chiffré adressé à un riche spéculateur américain dans son roman the Custom of the Country

[5] Il faut citer dans les principales machines à décrypter, les Bombes et les Colossus, premiers ordinateurs crées en 1943.

1939 et mai 1940 des milliers de messages tactiques allemands chiffrés en procédés manuels mais hélas, cela n'a pas servi à grand chose, car c'était des messages non stratégiques. On n'a pas eu le temps de les exploiter. Une division blindée française de 1939 a une compagnie de transmission, une division allemande a un bataillon de transmission. Les allemands transmettent en plus en phonie et souvent en clair. Un long poème de 75 vers, illustré par une clé a été composé le 30 septembre 1914 par un (ou des) chiffreurs anonymes. Il rend un hommage appuyé au commandant GIVIERGE qui fut un virtuose du chiffre :

"Je veux, prenant pour lyre un cor ou bien un fifre,
Chantant la jeune gloire et la beauté du Chiffre,
Guider tes premiers pas, Cryptologue, ingénu
Dans les sentiers secrets d'un domaine inconnu...
...Chiffrer pour la Patrie
est le sort le plus beau, le plus digne d'envie"

Ce combat permanent mené dans l'ombre des cabinets noirs a ses héros méconnus.

2) Chiffre et RENSEIGNEMENT

Une sculpture, symbolisant la cryptologie se dresse à l'entrée du siège de la CIA à Langley. Des centaines de lettres y sont gravées reproduisant un message chiffré. Seuls l'artiste, créateur de l'œuvre et le directeur de l'institution connaissent le texte en clair de ce message.[6]

La cryptologie et surtout la cryptanalyse est un des piliers du monde du renseignement, elle a joué un rôle primordial et longtemps tenu top-secret au cours des deux guerres mondiales et a été une arme efficace des services de renseignement pendant la guerre froide, elle est également au centre de ce que les Anglo-saxons appelle " l'intelligence économique".

Le colonel Paillole dans sa préface de l'Histoire Mondiale du renseignement, insiste sur l'importance des écoutes et du décryptement.[7] C'est Gottfried Schapper et George Schoeder spécialiste du décryptement, qui sont en 1933 les initiateurs du projet de la "Forschungsamt" (Agence centrale de renseignement du Reich, équivalent des Renseignements Généraux en France). Très vite, elle emploie plus de 250 techniciens du "Chiffrierstelle" (Section du Chiffre). L'agence n'apparaît pas dans les organigrammes officiels car le cloisonnement avec les autres services de renseignement allemands est étanche. Toute information donnée sur son existence est passible de la peine de mort. On tient à la protéger hermétiquement des services spéciaux étrangers mais aussi du Sicherheitdienst et de l'Abwehr.

Le chiffre semble avoir été dans de nombreux pays, un domaine où les meilleurs spécialistes ne s'appréciaient guère entre eux quand ils ne se méfiaient pas les uns des autres, allant jusqu'à faire de la rétention d'informations. Jalousies, rancœurs sont hélas fréquentes. Ne parlons pas des services du chiffre entre Alliés, là aussi les mêmes causes produisent les mêmes effets avec le chauvinisme en prime.

Dans ses Mémoires, le général Givierge se désole de cette triste réalité : "La jalousie des Affaires étrangères réduisit dès 1913 toute la partie diplomatique, pour laquelle le cabinet et ses chiffreurs arrêtèrent de nous fournir des documents." Des renseignements sont occultés, lesquels recoupés avec d'autres auraient pu se révéler capitaux. Les cryptologues sont très

[6] Selon un spécialiste, ce texte aurait été décrypté, il y a seulement quelques mois.
[7] R. Faligot, R. Kauffer; Histoire mondiale du renseignement; tome 1 : 1870-1939; p 8.

convoités par les services de renseignements adverses. Hans Thilo Schmidt[8] n'hésitera pas dans les années 30 à offrir ses services à l'attaché militaire auprès de l'ambassade de France à Berlin. Dans ses Mémoires, Faire face, Marthe Richard écrit qu'un chiffreur français a été arrêté dans les bureaux de l'Etat-major de la guerre en 1939 : "Notre service secret venait de découvrir le code qui avait servi aux Allemands pendant la campagne de Pologne... Sans aucun doute, ce code secret avait été changé depuis lors, mais nos services étaient passionnés de connaître, dans tous les détails, toute la stratégie de l'invasion de la Pologne... Malgré tout, le service secret ennemi était au courant des travaux de nos techniciens du Chiffre, grâce à un de ses agents employé à ce bureau."[9]

C'est par la défection d'un chiffreur soviétique en poste au Canada qu'on a pu dès 1945 mesurer l'ampleur de la pénétration des centres atomiques américains. En 1960,deux chiffreurs de la National Security Agency[10] passent à l'Est. Dans une conférence de presse organisée par les Soviétiques, ils annoncent que les Etats-Unis peuvent "casser" les systèmes de chiffrement de nombreux pays. Deux autres professionnels français du Chiffre dont les noms de code étaient Larionov et Sidorov furent recrutés en 1959, le premier était officier. Le colonel Vassili Mitrokhine et Christopher Andrew révèlent dans leur livre, The Mitrokhine Archive, the KGB in Europe and the West, qu'un fonctionnaire du service du Chiffre du Quai d'Orsay, dont le nom de code est "Jour"[11] a livré à Moscou, l'ensemble du courrier diplomatique échangé entre le ministère des Affaires étrangères et ses ambassades. L'auteur ajoute que les agents étrangers travaillant pour le KGB se révèlent être le plus souvent des diplomates ou des personnels du Chiffre. Les chiffreurs seraient-ils si loyaux en France, que contrairement aux autres pays, on n'a jamais démasqué de "taupes" parmi eux ? Ou plutôt ne serait ce pas plus cyniquement dû au fait qu'on ne les ait jamais découverts ? N'oublions pas que le véritable triomphe des services britanniques pendant la seconde Guerre Mondiale est d'avoir décrypté les messages de la machine à crypter de l'armée allemande, la fameuse "Enigma" et d'une machine de niveau supérieur la « Schlüsselzusatz » et d'avoir ainsi pu lire à livre ouvert dans les plans de l'ennemi.

Il y a quinze ans, deux commissaires de la DST rendirent visite au colonel, chef du Service Central du Chiffre, car à leur grande surprise, le Chiffre se trouvait en deuxième position (juste après l'arme atomique) sur la liste d'objectifs prioritaires trouvée sur un agent des Soviétiques. "Mais pouvait-on accorder autant d'importance à une activité souvent jugée marginale par nos élites civiles et militaires?" nous a confié ce colonel.

---

[8] Frère d'un des meilleurs connaisseurs de l'arme blindée de la Reichswher, il est chômeur et très aigri par le peu de reconnaissance que son pays fait de ses états de services lors de la Grande Guerre, où il a d'ailleurs été gazé. C'est à cette époque qu'il rencontre le chef de la "Chriffrierstelle" auquel son frère l'a présenté pour qu'il l'emploie.

[9] M. Richard ; Faire face ; SLIM ; 1947 ; p 51.

[10] Organisme de renseignement créé en 1952, considéré comme le plus performant en matière technique et informatique, responsable des chiffres et des décryptements. En 1995 la NSA a publié sur Internet des documents d'ordre technique et historique dont le fameux et volumineux dossier Venona, Soviet Espionage and the American Response (1937-1957) ; R.L.Benson ; M.Warner Editors, August 1996. On sait que certaines des activités de la NSA ont été réorganisées en 97-98 : « Le groupe Z (cryptanalyse), chargé de casser les codes et les cryptages adverses. Le groupe Z a joui à n'en pas douter, un rôle clé dans le travail de déchiffrement des communications irakiennes interceptées par l'UNSCOM. ». Le Monde du Renseignement ; n°=351 ; 28.01.99. Il faut lire à ce sujet le très intéressant numéro précédent, n°=350 ; 14.01.99.

[11] Il est recruté à l'âge de 23 ans en 1947 et est encore en activité un quart de siècle plus tard. Il reçoit en 1983, l'Ordre de "l'Amitié entre les Peuples" pour sa longue et fructueuse coopération.

UNE MONDIALISATION DES SUJETS SOUMIS AU DECHIFFREMENT ET DECRYPTEMENT

La cryptologie est un morceau du puzzle du renseignement : "Le renseignement convoque un idéal d'exhaustivité des connaissances, qui s'affirme au XIX ème siècle : il cesse d'être exclusivement militaire pour englober la totalité de l'espace politique. N'étant limité en pratique que par les moyens qui peuvent y être mis en œuvre, il s'étend des techniques de guerre (ordre de bataille, capacités et mode d'emploi des systèmes d'armes, codes, chiffres et communications[12], théorie et pratique de la tactique et de la stratégie des forces adverses), à l'ensemble des informations concernant les états actuellement ou potentiellement ennemis, leurs dirigeants et leurs objectifs, mais aussi les opposants intérieurs, réels ou supposés, les leurs comme les nôtres."
L'épisode Venona vient confirmer combien la recherche du renseignement par les moyens techniques est vitale. Ce nom poétique est le nom de code attribué par les décrypteurs des service secrets anglo-américains aux messages radios chiffrés de 1940 à 1948 échangés par l'URSS avec ses agents en place en Grande-Bretagne, Australie et Etats-Unis. Il fallut plusieurs années aux cryptanalystes américains et britanniques pour exploiter les carences d'un système qu'ils avaient découverts grâce entre autres à la réutilisation de codes soviétiques datant de 1927 : "Des listes impressionnantes par leur volume donnaient des centaines de noms de codes d'agents au service des Soviétiques sur le territoire américain dont ceux d'Antenna et Liberal qui devaient plus tard être reconnus comme ceux attribués aux époux Rosenberg"[13]

Lors de la guerre d'Indochine, on commençait à chiffrer puis on finissait en clair pour des raisons de temps ou de manque de pratique. Un message hybride était ainsi transmis, trahissant souvent le code. On devine l'importance que le Chiffre peut présenter pour les régimes totalitaires. Tous les chiffreurs devaient être membre du parti communiste en URSS et au Vietnam et les écoles du chiffre avaient l'honneur de recevoir les dirigeants. Les polices politiques inhérentes à ce type de gouvernement souvent désignées par le terme plus anodin de "forces de sécurité" se tenaient très au courant de tous les progrès techniques dans le domaine de la cryptologie.

Les enjeux de la cryptologie

Comme sur tous les théâtres d'opérations militaires, celui du récent Kosovo n'a pas manqué d'alimenter la guerre des systèmes d'information dont la cryptologie fait partie, même si le Pentagone s'est refusé à recourir à des actions de piratage informatiques sur les systèmes serbes[14]. Les entreprises vivent dans un environnement mondial qui évolue et se transforme radicalement. Les enjeux commerciaux pour la France et les perspectives pour l'Europe sont multiples. La concurrence et la coopération doivent savamment être dosées face aux Etats-Unis et au Japon.

Le renseignement qui est maintenant devenu principalement économique couvre à la fois la recherche d'informations et la manière dont on va protéger ses propres secrets. La guerre économique doit recourir à une stratégie du renseignement où les techniques, les marchés, les partenaires, les concurrents, les cultures sont à observer continuellement car il faut pouvoir les interpréter en permanence pour s'adapter au marché.

Certes le cyberespace est prometteur: Profits escomptés par millions, emplois espérés par milliers, mais y "surfer" sans précaution peut s'avérer risqué pour ceux qui n'y auront pas

[12] A. Dewerpe; Espion, une anthropologie historique du secret d'état contemporain, Gallimard, p225.
[13] Général Ribadeau Dumas, bulletin de l'ARCSI; n°25 97/98
[14] Le Monde; 10/11/99; p5.

été bien préparés et qui n'auront pas pris conscience des menaces, ni évalué les risques contenus dans les réseaux informatiques sans utiliser la parade que sont les technologies de la sécurité, dont la première est la cryptologie. Ce fruit longtemps défendu car longtemps sous contrôle militaire est un objet à double tranchant capable de servir les meilleures causes comme la défense de la vie privée ou du patrimoine d'un pays, comme les pires : la dissimulation d'actes condamnables, les mafias, le blanchiment d'argent, le terrorisme... Le contrôle de la cryptologie ne doit pas être négligé. L'existence du décryptement comme source d'information et l'explication qui a pu en être donnée par les services de renseignements a longtemps été tenue secrète et souvent lorsqu'elle a été révélée, elle est restée 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 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 MITROKHINE 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 lui-même avait été également tenu à l'écart de ces informations, de crainte qu'il en fasse mention au directeur de la CIA.

Concluons que le décryptement s'est révélé être au cours de l'Histoire une source précieuse du renseignement, source fiable mais combien fragile si l'on sait que la moindre indiscrétion peut ruiner les efforts engagés.

"La pénétration de l'ensemble d'un système de communications livre des informations dont la véracité est indiscutable, puisqu'elles proviennent de ce que l'adversaire se dit à lui-même. Mais le Renseignement ne gagne pas les guerres : la victoire appartient au belligérant le plus fort et le plus intelligent. Le renseignement permet d'être plus fort et plus intelligent, en rendant possible l'utilisation plus judicieuse des moyens dont on dispose ; il est sans utilité si l'on est sans moyens et sans capacités."[15]

Les média et l'opinion publique de la plupart des pays n'ont retenu des nouveaux décrets sur la cryptologie que les bienfaits supposés de sa libéralisation sans mentionner ou sans se préoccuper du fait que l'exportation du matériel américain est subordonnée à un " technical review" (examen technique) et que ce puissant pays continue d'interdire la vente hors de son territoire des moyens de sécurité les plus sophistiqués[16]. Procédure qui apparaît simplificatrice mais signifiant que la N.S.A. examine et contrôle la qualité de tous les produits cryptologiques qu'elle est susceptible de nous vendre ainsi qu'au monde entier. La France risque de voir s'amplifier "l'invasion" des produits d'outre-Atlantique, on peut même imaginer des scénarios catastrophes où les Américains vérifieraient tout, au point qu'un juge français devrait demander à la justice américaine de bien vouloir décrypter pour lui des messages chiffrés, afin d'élucider un crime commis sur notre territoire. Comment rendre la justice dans ces conditions ? Sachant qu'une bonne partie des affaires judiciaires sont aujourd'hui résolues par des interceptions autorisées par la justice, et que bientôt tout sera crypté, on comprend quelles possibilités cette libéralisation peut octroyer à des trafiquants. Pour compenser les effets de cette libéralisation, on envisage alors d'obliger les éventuelles personnes mises en examen à remettre spontanément les informations destinées à pouvoir les confondre (par ex. Les clés de chiffrement). Idée séduisante mais qui s'oppose à la loi européenne dite du

[15] G. Bloch; L'autre Ultra, Magic: les décryptements américains pendant la seconde guerre mondiale; juin 90; p 31.

[16] La nouvelle politique américaine annoncée en septembre 99 entretient le mythe de la libéralisation en étendant les possibilités d'exportation des logiciels de cryptage quelle que soit la longueur de leurs clés (à de rares exceptions près) , mais reste discrète sur le maintien voir le renforcement de ce "technical review". On a naturellement confiance dans les performances de ces produits américains, toutefois les pressions de l'administration américaine sur ses industriels pour qu'ils intègrent dans ces matériels cryptologiques un dispositif "key recovery" permettent à la NSA et au FBI de lire en clair les messages chiffrés à l'insu de l'utilisateur.

"principe d'auto-incrimination" qui veut qu'on ne puisse fournir les preuves contre soi-même[17]. On peut bien sûr s'en tenir aux pratiques anglo-saxonnes de connivence entre les industriels et les forces de sécurité. En France les preuves apportées dans ces conditions ne sont pas recevables. Aux Etats-Unis un projet de loi prévoit que ces preuves n'auraient même pas à être présentées mais que seul le contenu livré par l'industriel suffirait.

On peut regretter le système antérieur des Tiers de Confiance[18] qui présentait des solutions acceptables mais qui a été temporairement suspendu. Ce n'est pas un hasard si ce qui touche à la politique cryptologique est nommé aux Etats-Unis "information dominance" et si les contacts directs de la N.S.A. avec Microsoft viennent d'être dénoncés par un de leurs sénateurs.

Les services de renseignement aussi performants soient-ils en matière d'exploitation de données cryptologiques ne sont jamais que les instruments d'une politique mais ils peuvent aider un Etat à gagner une guerre militaire, commerciale ou simplement à gagner du temps pour résoudre des problèmes divers.

Il faut reconnaître que le recours aux technologies cryptographiques est une pierre angulaire de la société de l'information. Des millions d'ordinateurs sont connectés dans le monde entier par l'intermédiaire de réseaux privés et d'Internet. Sans cryptage, les entreprises et les personnes privées sont exposées au risque de voir leurs données ou transactions dévoilées, volées ou modifiées. Une clé dérobée s'appelle dans le milieu des initiés une clé compromise. La faiblesse humaine est un des facteurs à considérer car l'appât du gain et les affaires de mœurs sont les deux mamelles de la trahison. Pour minimiser ce risque, les mesures gouvernementales doivent tenir compte des libertés individuelles et publiques. Si les logiciels sont mauvais en terme de qualité, ils ne peuvent pas être bons en terme de sécurité. "Les risques liés à la malveillance informatique doivent être couverts comme d'autres risques apparus avec certains progrès techniques... Les assureurs français se doivent d'être vigilants. Leurs concurrents étrangers, américains en particulier, pourraient fort bien profiter de ce marché lié aux risques engendrés par les nouvelles technologies dont leur industrie possède déjà le quasi-monopole."[19]

La presse française s'est fait l'écho en janvier 99 de l'affaire Crypto-AG. Cette firme suisse avait vendu du matériel de cryptologie à plusieurs pays. Sa technologie avait été "piégée" en vertu d'un accord secret passée avec la NSA, laquelle interceptait en clair toutes les transmissions de données (radio, télex, fax...) Le service du contre-espionnage militaire iranien a arrêté Hans Bühler, représentant de Crypto-AG à Téhéran. La compagnie a "racheté" la liberté de Bühler pour un million de dollars et l'a licencié pour avoir révélé que: " Crypto-AG était un centre d'espions travaillant avec les services secrets allemands et américains." Les liens du régime iranien avec les groupes terroristes installés au Moyen-Orient furent ainsi révélés grâce à ce matériel suisse[20].

Les décryptements historiques sont au cœur de controverses, dont le temps, s'il a apporté de la sérénité n'a pas atténué les convictions opposées des uns et des autres. Le professeur Renouvin refusa d'accorder au radiotélégramme de la Victoire, le rôle que certains et non des

---

[17] Le principe d'auto-incrimination ne semble pas compatible avec la jurisprudence de la Cour des Droits de l'Homme.

[18] Organismes agréés par l'administration auprès desquels, les utilisateurs déposent leurs clés "longues" et que seule la justice peut obtenir dans le cadre d'une instruction. Ce système prévu par la loi de 1996, « ne répondait en rien aux exigences de sécurité du pays » a dit en janvier 1999 le Premier ministre. Un de ses conseillers ayant expliqué : « Pendant que nos services bâtissaient une nouvelle ligne Maginot, ils n'ont pas mis en place les divisions blindées mobiles dont nous avions besoin. En outre, au cours de l'année écoulée le système n'a pas fait la preuve de sa fiabilité économique… ». Le Monde du Renseignement ; n°=351 ; 28.01.99.
On parle déjà de rétablir les Tiers de Confiance.

[19] Général J.L. Desvignes; Risques n° 39, juillet-septembre 99.

[20] Valeurs actuelles; 16/1/99; p16.

moindres, tel Clemenceau lui avaient reconnu. Renouvin était un grand mutilé de la guerre 14-18, on comprend qu'il ait pu répugner à placer le Chiffre et ses exécutants protégés au sein de leur Cabinet noir loin de la boue des tranchées, au rang de principaux vainqueurs.

On peut aussi envoyer de faux messages chiffrés afin de désinformer l'adversaire. Entre les deux guerres, le SR (Service de Renseignement) français s'était procuré les codes de plusieurs puissances. L'Allemagne et l'Italie avaient téléguidé l'opération en faisant vendre certains codes uniquement conçus pour intoxiquer l'adversaire.

Gilbert Bloch soulève un autre grave problème qui ne touche pas uniquement la cryptologie : "L'intoxication n'est nullement cantonnée au domaine militaire. Son exploitation politique, sociologique, commerciale et même culturelle nous submerge. Les spécialistes militaires, pourtant entraînés à la prudence et ou scepticisme ont pu être trompés... Dès lors, comment les simples citoyens ne le seraient-ils pas ?" [21]

Sophie de LASTOURS

[21] G. Bloch; Renseignement et intoxication durant la Seconde guerre mondiale; l'Harmattan; p 95.