CRYPTOLOGIE ET RELATIONS INTERNATIONALES

PAR

IVAN MAXIMOFF (*)

La cryptologie a longtemps été un domaine réservé des Etats et de leurs plus hautes autorités. Jusqu'au début du siècle dernier, des individus remarquables tels que Polybe, César, Bacon, Vigenère ou Painvin ont pu innover dans ce domaine et ainsi procurer des avantages stratégiques à leurs patries. A partir de la Seconde Guerre mondiale, ce sont des organisations nationales soutenues par des innovations technologiques qui ont hérité de ce rôle. Dans le monde libre, les Anglo-Saxons, forts de leurs nouvelles compétences, prennent une avance en la matière, puis atteignent peu à peu à une véritable hégémonie. La cryptologie est par nature un domaine ambigu pour les relations internationales : elle permet aux diplomates de communiquer discrètement, mais les services de renseignements en usent également pour écouter les communications étrangères. Malgré tout, les échanges internationaux existent dans ce domaine.

Les Etats ont d'abord sévèrement réglementé cette technologie, puis ont finalement essayé de la maîtriser par d'autres moyens, en s'appuyant parfois sur des coopérations ou des accords internationaux. Certains Etats ont rapidement pris conscience de la nécessité de légiférer sur l'utilisation des moyens cryptologiques. Ces législations doivent tenir compte de nombreux paramètres apparemment antagoniques, comme les libertés individuelles, les missions de police ou les enjeux financiers. Elles ont évolué progressivement d'une interdiction pure et simple à un contrôle strict et finalement à une quasi-libéralisation.

Afin de comprendre les enjeux, nous préciserons d'abord quelques notions techniques et rappellerons quelques exemples historiques montrant l'importance stratégique de la maîtrise de la cryptologie, avant de comparer les évolutions des législations françaises et américaines et de présenter ensuite un panorama mondial des législations actuelles. Enfin, nous évoquerons les principaux échanges internationaux dans ce domaine.

(*) Ingénieur au ministère français de la Défense, titulaire du Brevet d'études supérieures de la sécurité des systèmes d'information.

APPROCHE TECHNIQUE ET HISTORIQUE

Pour aborder le domaine de la cryptologie dans les relations internationales contemporaines, il est nécessaire d'assimiler quelques notions permettant d'appréhender les possibilités et limites de cette science. Il convient aussi de s'intéresser à l'impact de la cryptologie sur certains événements historiques pour comprendre l'importance que certains Etats lui accordent.

Repères techniques

Le chiffre incassable existe bel et bien

Cet algorithme dont la robustesse est mathématiquement démontrée depuis le début du XX^{e} siècle est connu sous les noms de «masque jetable», «bande aléatoire une fois» ou chiffrement de Vernam. Toutefois, ce système nécessite des quantités très importantes d'aléa vrai et est complexe à mettre en œuvre.

La sécurité réside totalement dans la clef

Une bonne logique de chiffrement n'a pas à être secrète : seule la connaissance de la clef utilisée permet de retrouver le clair. L'unique solution pour décrypter un message est alors d'essayer toutes les clefs sur le chiffré et de vérifier que le résultat obtenu correspond à un clair cohérent.

Entropie et taille de clef

Cette valeur s'exprime en bits et représente le nombre de clefs qui peuvent être utilisées; elle correspond au logarithme en base 2 du nombre de clefs possibles. La clef se présente sous la forme d'une série de chiffres (cas du code de carte bleue), d'une série de caractères alphanumériques (mot de passe) ou d'un nombre exprimé en valeur hexadécimale plus adaptée aux mémoires informatiques. Un code de carte bleue ayant quatre chiffres, il a 10 000 valeurs possibles. Le logarithme en base 2 de 10 000 vaut 13,28; l'entropie est alors inférieure à 14 bits. Une clef de 40 bits a 2^{40} (environ mille milliards) valeurs possibles.

Evolution sécurité/entropie

Contrairement à une impression trompeuse, une clef de 128 bits n'est pas seulement trois fois plus résistante qu'une clef de 40 bits. Le véritable ratio est le résultat de l'opération suivante : $2^{128}/2^{40} = 2^{128-40} = 2^{88}$ soit environ 10^{26} ou cent millions de milliards de milliards. Autrement dit, passer d'une clef de 40 à 128 bits renforce, en théorie, la sécurité non pas d'un facteur

trois, mais d'un facteur de très loin supérieur à l'âge de l'univers exprimé en secondes.

Le tableau suivant est une mise à jour d'un tableau publié par Bruce Schneier dans *Cryptographie appliquée*.

Estimation du temps moyen d'une attaque exhaustive pour une machine construite en 2004

Entropie exprimée en bits						
Coût	*40*	*56*	*64*	*80*	*112*	*128*
100 K$	30 ms	30 mn	5 jours	9 siècles	10^{12} ans	10^{17} ans
1 M$	3 ms	3 mn	12 h	90 ans	10^{11} ans	10^{16} ans
10 M$	0.3 ms	2 s	72 mn	9 ans	10^{10} ans	10^{15} ans
100 M$	0.03 ms	0.2 s	7 mn	300 jours	10^{9} ans	10^{14} ans
1 G$	3 µs	20 ms	42 s	1 mois	10^{8} ans	10^{13} ans
10 G$	0.3 µs	2 ms	4 s	3 jours	10^{7} ans	10^{12} ans
100 G$	30 ns	0.2 ms	0.4 s	7 h	10^{6} ans	10^{11} ans

Une machine d'un million de dollars construite pour un algorithme particulier mettrait 10^{17} années pour effectuer une attaque exhaustive sur 128 bits. Notre soleil sera déjà éteint alors que cette machine n'aura testé que 0,0000001 % de l'espace des clefs.

Le chiffrement asymétrique

En 1976, deux universitaires américains, Whietfield Diffie et Martin Hellman, ont suggéré une approche fondamentalement nouvelle de la cryptologie en proposant un chiffrement pour lequel la clef de chiffrement est différente de la clef de déchiffrement. On considère alors le couple clef publique/clef privée : une relation mathématique relie la clef publique et la clef privée telle que la connaissance de l'une des deux ne permet pas de retrouver l'autre. Le principe est le suivant : Alice diffuse sa clef publique sur un annuaire public; Bob chiffre son message à l'aide de la clef publique d'Alice; seule celle-ci, qui dispose de la clef privée associée, est en mesure de le déchiffrer. Les algorithmes existants reposent sur des problèmes mathématiques réputés complexes comme la factorisation de grands nombres. Ainsi, pour «casser» un système RSA, il ne faut plus réaliser une attaque exhaustive mais factoriser un grand nombre.

Ce problème de factorisation est réputé difficile, mais sa complexité n'est pas démontrée mathématiquement. Si une entité découvre un algorithme ou une nouvelle technologie permettant une factorisation rapide, elle sera en mesure de «casser» le RSA. Le concept de taille de clef est alors très différent de celui utilisé pour les algorithmes symétriques, puisqu'elle ne représente plus l'entropie du système mais simplement la taille occupée physi-

quement par la clef. Ces méthodes de chiffrement nécessitent des capacités de calculs importants et sont donc utilisées principalement pour l'échange de clefs de sessions utilisées ensuite par des algorithmes symétriques beaucoup plus rapides.

Repères historiques

Des Egyptiens à l'Antiquité

Les prémisses de l'utilisation d'éléments cryptologiques apparaissent très tôt dans l'histoire : le plus ancien cryptogramme, découvert sur une tablette mésopotamienne du XV^e^ siècle avant notre ère, contient une formule chiffrée pour la fabrication de vernis.

Le procédé Atbash est employé dans l'Ancien Testament. Dans ce système, la première lettre de l'alphabet est remplacée par la dernière et *vice versa*, l'avant-dernière par la deuxième, *etc.* Ainsi, en hébreu, le mot BABEL devient SHESHAK. Le mot ATBASH est le résultat de la transformation par ce système des premières lettres de l'alphabet hébreu.

Thucydide rapporte l'utilisation du premier instrument cryptographique : la scytale lacédémonienne consiste en un bâton de bois autour duquel une bande de cuir est entourée. L'expéditeur écrit son message sur toute la longueur de la scytale et déroule ensuite la bande qui apparaît alors couverte d'une suite de lettres sans signification. Le destinataire doit enrouler cette bande sur un bâton de même diamètre pour retrouver le message.

Polybe est à l'origine du premier procédé de chiffrement par substitution, dit carré de Polybe, qui inspira de nombreux systèmes pendant plusieurs siècles. Jules César fut aussi l'inventeur d'un système de chiffrement consistant à décaler chaque lettre claire de trois rangs : CESAR devient alors FHVDU.

Les dix-neuf premiers siècles de notre ère

Les premiers écrits de cryptanalyse sont l'œuvre d'Abu Yusuf Ya'qub au IX^e^ siècle. Celui-ci décrit une technique de décryptement fondée sur l'analyse des fréquences des caractères, qui était encore d'actualité à la fin du XX^e^ siècle pour décrypter certains produits commerciaux. Ce système a donné son nom au «saint» patron fictif des chiffreurs français, URLO, formé à partir des lettres les plus fréquentes dans un texte français, à savoir respectivement ESAINT URLO.

Au XIII^e^ siècle, Roger Bacon décrit plusieurs cryptosystèmes. En 1585, Blaise de Vigenère propose un procédé améliorant le chiffre de Jules César, appelé carré de Vigenère : ce chiffre, longtemps considéré comme indécryptable, a été cassé en 1854 par Charles Babbage, le père de l'informatique.

Des applications professionnelles utilisent encore ce chiffre avec un siècle et demi de retard.

Les deux Guerres mondiales

Fin 1916, les Allemands obtiennent du Président Woodrow Wilson la possibilité d'utiliser la liaison télégraphique reliant Washington à l'ambassade américaine à Berlin pour faciliter les négociations d'un plan de paix. Les Allemands disposaient ainsi d'une liaison chiffrée dans leur propre code entre Berlin et Washington, sous le couvert d'une liaison diplomatique américaine. Les Anglais qui écoutaient cette liaison ont détecté le passage de données chiffrées par des systèmes allemands et parvinrent à reconstituer en partie le télégramme original. Le Télégramme Zimmerman, du nom du ministre allemand des Affaires étrangères Arthur Zimmerman, proposait une alliance au Mexique contre les Etats-Unis.

Les Anglais étaient alors placés devant un dilemme : la révélation du contenu aux Etats-Unis pouvait précipiter l'entrée en guerre de ces derniers, mais il fallait alors justifier la possession d'un tel document et donc révéler les capacités de décryptement. Les Anglais ont donc inventé une histoire contenant un ensemble de demi-vérités qui permettait de ne pas trop renseigner les Américains sur leurs capacités d'interception. Le Télégramme Zimmerman se retrouva dans la presse américaine en mars 1917. Les Anglais poussèrent le cynisme à inspirer à la presse britannique des articles critiquant l'inefficacité des services secrets anglais. Le 2 avril 1917, le Président Woodrow Wilson montait à la tribune du Capitole pour demander au Congrès de «*faire du monde un lieu où la démocratie soit en sécurité*» en faisant référence à «*la note interceptée, adressée au ministre allemand à Mexico*».

Durant la Seconde Guerre mondiale, l'équipement de chiffrement principal de l'Allemagne était l'Enigma, une machine dérivée d'un système commercial datant des années vingt. Dès 1934, les Polonais mettaient au point la Bomba, un appareil spécialement conçu pour cryptanalyser Enigma et, en 1938, ils décryptaient 75 % des messages allemands. Une fois la Pologne écrasée, les cryptanalystes polonais ont rejoint la France et ont adapté, avec l'aide des Français, leur Bomba aux dernières versions d'Enigma. Ils se réfugièrent ensuite en Grande-Bretagne et, en mai 1940, la première «bombe» anglaise plus rapide et efficace que son ancêtre polonais décryptait des messages Enigma de la *Luftwaffe*.

Ces décryptements portaient le nom de code ULTRA. On a écrit que Winston Churchill a délibérément sacrifié la ville de Coventry, victime d'un bombardement allemand, pour préserver le secret d'ULTRA, alors qu'il disposait de l'information grâce à un décryptement : les historiens sont partagés sur la réalité de cette décision, mais cette anecdote souligne la difficulté d'uti-

liser des renseignements issus de décryptements sans révéler ses capacités. L'existence des «bombes» ne fut révélée qu'en 1973.

Toutes proportions gardées, la révolution technologique que fut l'apparition de l'informatique utilisée pour les décryptements alliés a participé activement à la victoire sur le front européen comme la révolution technologique issue du projet Manhattan a précipité la victoire dans le Pacifique.

1991 : l'assassinat de Shahpour Bakhtiar

L'ancien Premier ministre iranien Shahpour Bakhtiar est abattu à Paris en août 1991. Très rapidement, des officiels américains accusent les Iraniens d'avoir commandité cet attentat. Plusieurs articles de presse laissent entendre que les Anglo-Saxons ont intercepté des communications entre Téhéran et ses missions diplomatiques en Europe, qui prouvent l'implication des Iraniens. Or, ces communications étaient chiffrées à l'aide d'équipements commercialisés par une société suisse. Les Iraniens sont donc rapidement arrivés à la conclusion que leurs matériels de chiffrement étaient piégés. L'affaire, qui aurait pu rester confidentielle, est apparue au grand jour lorsqu'un représentant de la société suisse a été arrêté puis retenu prisonnier en Iran.

Il semble que la France a décliné une offre de prise d'intérêts dans cette société suisse et que ce sont finalement les Américains qui, avec le soutien des Allemands, en ont pris le contrôle indirect.

Législations de l'utilisation de la cryptologie

Evolution des législations françaises et américaines

Avant les années quatre-vingt-dix : forte limitation

En France, les équipements intégrant de la cryptologie sont considérés comme des matériels de guerre. La cryptologie reste alors un domaine réservé de l'Etat. Aux Etats-Unis, l'utilisation par des Américains de produits américains n'est pas limitée; cependant, l'exportation de matériels robustes utilisant des clefs supérieures à 40 bits est interdite, à l'exception de ceux utilisant l'algorithme standard américain : le DES (*Data Encryption Standard*). Ainsi, seuls les produits que la NSA (*National Security Agency*) est en mesure de décrypter sont autorisés à l'exportation.

L'avantage est alors aux Etats-Unis, puisque leurs entreprises ont les moyens de se protéger efficacement des interceptions étrangères et qu'ils gardent la possibilité de décrypter les communications étrangères chiffrées par de produits américains. Ainsi, les entreprises américaines peuvent déve-

lopper leurs compétences en cryptologie et obtenir des marchés à l'export. La France, quant à elle, empêche ses entreprises de se protéger : seuls certains industriels travaillant pour la Défense sont en mesure de développer des compétences mais les marchés exports sont fermés; en contrepartie, les écoutes intérieures restent possibles.

Première moitié des années quatre-vingt-dix : évolution juridique en France et technologique aux Etats-Unis

En France, les systèmes cryptographiques ne sont plus considérés comme des matériels de guerre, mais leur utilisation est soumise à autorisation préalable s'ils assurent des fonctions de confidentialité. Les entreprises peuvent enfin se doter de moyens de chiffrement pour protéger leurs secrets industriels.

Aux Etats-Unis, la législation n'évolue pas, mais la diffusion libre sur l'Internet d'un logiciel de chiffrement fort perturbe le système. En 1991, Philip Zimmerman met à disposition, sur plusieurs serveurs publics, un logiciel désigné sous le nom de *Pretty Good Privacy* (PGP) : c'est un outil qui intègre un système hybride de cryptographie à base d'algorithmes symétriques et asymétriques; il ne respecte pas la législation américaine puisqu'il est diffusé sur l'Internet et est donc accessible de tous pays. Les poursuites initiées contre Philip Zimmerman par la justice américaine sont abandonnées : une faille de la législation permet d'exporter les sources sous forme papier puis, une fois en Europe, de les scanner, de les compiler et donc de proposer légalement PGP en téléchargement sur des serveurs situés aux Pays-Bas.

Seconde moitié des années quatre-vingt-dix : recours au «tiers de confiance»

Le séquestre de clefs est une solution permettant à chacun d'utiliser la cryptographie, mais laissant aux forces de l'ordre la possibilité de déchiffrer les messages illégaux. Le chiffreur fournit une copie de sa clef à un tiers qui sera en mesure de la transmettre à la justice.

L'*American Escrowed Encryptrion Standard* a été conçu par le gouvernement américain en 1994. Dans ce standard, le tiers de confiance était composé de deux autorités fédérales destinataires chacune de la moitié de la clef. Le gouvernement américain a utilisé ce système pour son propre compte et l'a rendu obligatoire pour les sociétés travaillant avec lui mais il n'a pas pu devenir un standard de fait.

En 1998, la France a proposé un concept équivalent. L'idée était d'autoriser un chiffrement fort à condition que les clefs soient déposées auprès d'un tiers de confiance. Ce dernier est une société privée agréée par l'Etat, qui a pour mission de recueillir les clefs, de les protéger et, sous réserve d'une décision de justice, de les remettre à l'Etat. Si le système de séquestre

est utilisé, la taille des clefs n'est plus réglementée. Bien que quelques sociétés aient reçu un agrément du gouvernement, le système est resté marginal. Simultanément, la France assouplissait sa réglementation et les produits de 40 bits n'étaient plus soumis qu'à déclaration. Avec cette nouvelle réglementation, la France pouvait développer une industrie cryptologique compétente. Les industriels français avaient désormais les moyens de se protéger des interceptions étrangères. La menace de l'espionnage industriel est en effet en augmentation à cette époque puisque les systèmes d'interceptions de la Guerre froide n'ont plus, en apparence, de réels ennemis à écouter et la tentation devient grande d'orienter les antennes vers des cibles civiles.

Depuis 1999 : vers la libéralisation

Dès le début des années quatre-vingt, les pressions ont été fortes sur les gouvernements pour libéraliser la cryptographie. Les groupes de protection de la vie privée sont rejoints par les entreprises, pour lesquelles le développement des échanges numériques et du commerce électronique nécessite l'utilisation de produits cryptographiques forts. En 1999, la France prend l'initiative en modifiant fondamentalement sa politique vis-à-vis de la cryptologie : les produits de 128 bits sont désormais autorisés sur simple déclaration, en France et à l'exportation; les entreprises ont désormais la possibilité de concevoir et d'exporter des produits de chiffrement robustes, alors que leurs concurrentes américaines sont toujours limitées à l'exportation. Les Etats-Unis modifient alors rapidement leur législation et calquent leurs règles d'exportation sur celles de la France. La réaction américaine fut si prompte que l'industrie française n'a pas eu le temps de profiter de son avantage temporaire pour gagner de nouveaux marchés.

Différents paramètres, principalement des motivations concurrentielles, ont poussé les Etats à abandonner progressivement le contrôle législatif exclusif et total des produits cryptographiques. Cet abandon pourtant officialisé par les nouvelles lois apparues à la fin du siècle dernier n'est probablement pas complet. Le contrôle d'infrastructures comme les réseaux de communications, la maîtrise des systèmes d'exploitation, l'influence auprès des organismes normalisateurs et la connivence de certains industriels sont des paramètres sur lesquels des Etats peuvent encore s'appuyer.

Panorama des législations mondiales

Le tableau suivant présente l'état actuel des réglementations de soixante Etats.

Etat	*Exportation*	*Importation*
Argentine	Wassenaar	Non contrôlée
Afrique du Sud	Contrôlée	Contrôle limité
Allemagne	UE + Wassenaar	Non contrôlée

Etat	*Exportation*	*Importation*
Israël	Contrôlée	Contrôlée
Italie	UE + Wassenaar	Non contrôlée
Japon	Wassenaar	

Etat	*Exportation*	*Importation*
Arabie Saoudite	Non contrôlée	Non contrôlée
Australie	Wassenaar	Non contrôlée
Autriche	UE + Wassenaar	Non contrôlée
Bangladesh	Non contrôlée	Non contrôlée
Belarus	Contrôlée	Contrôlée
Belgique	UE + Wassenaar	Non contrôlée
Birmanie	Contrôlée	Contrôle limité
Brésil	Non contrôlée	Non contrôlée
Bulgarie	Wassenaar	Non contrôlée
Canada	Wassenaar	Non contrôlée
Chili	Non contrôlée	Non contrôlée
Chine	Contrôlée	Contrôlée
Colombie	Non contrôlée	Non contrôlée
Corée du Sud	Wassenaar	Contrôle limité
Danemark	UE + Wassenaar	Non contrôlée
Egypte		Contrôle limité
Espagne	UE + Wassenaar	Non contrôlée
Estonie	Wassenaar	Non contrôlée
Etats-Unis	Wassenaar	Non contrôlée
Finlande	UE + Wassenaar	Non contrôlée
France	UE + Wassenaar	Contrôle limité
Grande-Bretagne	UE + Wassenaar	Non contrôlée
Grèce	UE + Wassenaar	Non contrôlée
Hongrie	UE + Wassenaar	Contrôle limité
Inde		Contrôle limité
Indonésie	Non contrôlée	Non contrôlée
Irlande	UE + Wassenaar	Non contrôlée

Etat	*Exportation*	*Importation*
Kazakhstan	Contrôlée	Contrôlée
Kirghizstan	Non contrôlée	Non contrôlée
Lettonie	EU	Non contrôlée
Lituanie	Wassenaar	Contrôlée
Luxembourg	Wassenaar	Non contrôlée
Malaisie	Non contrôlée	Non contrôlée
Mexique	Non contrôlée	Non contrôlée
Moldavie	Contrôlée	Contrôlée
Norvège	Wassenaar	Non contrôlée
Nouvelle-Zélande	Wassenaar	Non contrôlée
Pakistan	Contrôlée	Contrôlée
Pays-Bas	UE + Wassenaar	Non contrôlée
Pérou	Non contrôlée	Non contrôlée
Pologne	Wassenaar	Contrôle limité
Porto Rico		Non contrôlée
Portugal	UE + Wassenaar	Non contrôlée
République Tchèque	Wassenaar	Contrôle limité
Roumanie	Wassenaar	Non contrôlée
Russie	Wassenaar	Contrôlée
Singapour	Wassenaar	Non contrôlée
Slovaquie	Wassenaar	
Suède	UE + Wassenaar	Non contrôlée
Suisse	Wassenaar	Non contrôlée
Turquie	Wassenaar	
Ukraine	Wassenaar	
Uruguay		Non contrôlée
Vietnam	Contrôlée	

La mention «contrôle limité» précise que les importations de produits intégrant de la cryptographie forte peuvent être autorisées à condition qu'une démarche administrative déclarative soit effectuée. La mention «contrôlée» concerne différentes politiques de restrictions. Les règles d'exportation résultant de l'accord de Wassenaar et de l'Union européenne sont décrites ci-après.

Régulations des echanges bilatéraux et multilatéraux

Panorama des services cryptologiques nationaux

La plupart des grands Etats disposent de services cryptologiques. Deux grandes familles sont identifiables : les services cryptographiques traitant de la protection des communications ou COMSEC (Communication Security) et les services de cryptanalyses intervenant sur les interceptions ou COMINT (Communication Intelligence).

Le tableau suivant liste les services de plusieurs grandes nations ayant à traiter de cryptologie ainsi que leur rattachement administratif.

Pays		*Organisation*	*Rattachement*
Allemagne	COMSEC	Bundesamt für Sicherheit in der Informationstechnik (BSI)	Ministère de l'Intérieur
	SIGINT	Bundesnachrichtendiest (BND)	Chancellerie fédérale, mais le domaine 62 (cryptanalyse) serait intégré au BSI.
Australie	COMSEC	Defense Signal Directorate	Premier ministre
	SIGINT	*Idem*	*Idem*
Etats-Unis	COMSEC	National Security Agency (NSA)	Président
	SIGINT	*Idem*	*Idem*
France	COMSEC	Secrétariat général de la Défense nationale/ Direction centrale de la sécurité de systèmes d'information (SGDN/DCSSI)	Premier ministre
	SIGINT	Direction générale de la sécurité extérieure/ Direction technique (DGSE/ DT)	Ministère de la Défense
Grande-Bretagne	COMSEC	Government Communications Head-Quarters/Communications Electronics Security Group (GCHQ//CESG)	Ministère des Affaires étrangères
	SIGINT	Government Communications Head-Quarters (GCHQ//Operations and Requirement /Division H)	*Idem*
Nouvelle-Zélande	COMSEC	Government Communications Security Bureau	Premier ministre
	SIGINT	*Idem*	*Idem*
Russie	COMSEC	Federal'noe Agentstvo Pravitel'stvennoï Svyazi i Informatsii / Headquarters of communication's security (FAPSI/GUBS)	Président
	SIGINT	Federal'noe Agentstvo Pravitel'stvennoï Svyazi i Informatsii / Headquarters of radio electronic intelligence of communication's means (FAPSI/GURRSS)	*Idem*

Seule la France a nettement partagé le domaine de la cryptologie en deux services distincts et dépendant d'entités administratives de rangs différents. La cryptologie ne représente qu'une partie des activités des services cités. Nous pouvons évaluer grossièrement le personnel du service COMSEC français à une centaine de personnes – dont peut-être la moitié traite de cryptologie – et le service SIGINT à un millier de personnes – dont seul un faible pourcentage doit traiter de cryptologie. La NSA emploierait plus de quarante mille personnes, dont de nombreux mathématiciens. Bien que dif-

ficilement comparables, ces chiffres indiquent l'importance que les Etats-Unis attachent à ce domaine.

Les échanges intergouvernementaux

Le pacte UKUSA

Un des éléments majeurs de la stratégie des Etats-Unis à l'égard du Pacte de Varsovie a consisté à créer un pacte de sécurité destiné à intercepter les communications du bloc soviétique. Issu du système américano-britannique qui a fait ses preuves pendant la Seconde Guerre mondiale, ce pacte secret, conclu en 1947 entre le Royaume-Uni et les Etats-Unis, a été étendu au Canada puis à la Nouvelle-Zélande et à l'Australie. Le choix de ces anciennes colonies britanniques ne doit rien au hasard, puisque les stations d'écoutes ainsi installées permettent d'obtenir une couverture mondiale. Les interceptions peuvent concerner des données chiffrées et il devient nécessaire de les décrypter. Les moyens de décryptement étant particulièrement onéreux, ils ne sont pas dupliqués et c'est la NSA qui intervient le plus souvent pour ces opérations. L'ensemble du système interception, décryptement et tri est connu sous le nom de réseau Echelon.

Coopération en matière de renseignement

L'OTAN a institué des échanges entre services de renseignements désignés sous le nom de Totem. Dans le domaine du décryptement, les Etats-Unis sont de très loin les plus performants. La majorité des équipements ou logiciels de chiffrement sont plus ou moins directement conçus par des sociétés anglo-saxonnes et on peut raisonnablement penser que leurs décryptements ne posent pas de réels problèmes à la NSA. Les compétences cryptologiques s'étant malgré tout diffusées, de nombreuses nations produisent désormais des produits cryptographiques. La coopération entre services nationaux devient alors indispensable. La NSA propose donc des partenariats avec les services étrangers. Les échanges Totem sont bilatéraux et les informations échangées ne peuvent pas être rediffusées. Ainsi, la NSA maintient son hégémonie en acquérant une capacité globale qui ne peut être obtenue par aucune autre nation.

Liaisons interétatiques

La première liaison téléphonique chiffrée installée spécifiquement pour un échange entre chefs d'Etat date de 1939. Son objet était d'assurer la confidentialité des échanges entre W. Churchill et Franklin Roosevelt. Les Américains ont fait développer, dès 1942, SIGSALY, premier système numérique de chiffrement téléphonique. L'existence de cette liaison est restée secrète jusqu'en 1976, alors que son retrait date de 1946. En 1959, les

Etats-Unis proposent à l'Union soviétique d'établir une ligne sécurisée entre Washington et Moscou. La crise des missiles de Cuba précipite le projet. L'accord pour l'établissement d'une liaison directe, à base de télex chiffrés selon l'algorithme de Vernam, est signé à Genève en juin 1963. Ce message diplomatique fort est considéré comme le signe du début de la «coexistence pacifique». Aujourd'hui, la liaison est composée de deux lignes satellitaires.

Ce type de liaison est un symbole diplomatique important. Pendant les années soixante, l'Union soviétique a insisté pour l'établissement de semblables liaisons avec la France et la Grande-Bretagne : elle voulait ainsi montrer que les Etats-Unis n'étaient pas leurs seuls interlocuteurs. Fin 1999, les Présidents chinois et français ont décidé d'installer un «téléphone rouge» entre Paris et Pékin afin d'émettre le signe d'une intensification de leur coopération politique. Les Etats-Unis disposeraient actuellement d'une cinquantaine de liaisons présidentielles chiffrées. La France en dispose de cinq, soit une avec chaque membre du Conseil de sécurité et une avec l'Allemagne. Ce type de liaison peut présenter quelques inconvénients : ainsi, lorsque le Président Jimmy Carter a utilisé le télex chiffrant pour négocier les accords SALT 2 directement avec le Président Leonid Brejnev, les traducteurs du côté soviétique n'étaient pas habitués au vocabulaire stratégique et les mauvaises interprétations ont notablement compliqué les négociations.

Organisations ou régulations multilatérales

La cryptologie au sein de l'OTAN

La nature multinationale de l'Organisation du Traité de l'Atlantique-Nord impose d'organiser la compatibilité des équipements et donc des systèmes de chiffrements. L'agence SECAN (Security and Evaluation Agency) a donc été créée pour traiter de la compatibilité et de l'évaluation des équipements de cryptologie. Cette agence présente des caractéristiques qui montrent l'importance que les Etats-Unis attachent à ce domaine.

SECAN est financée totalement sur fonds américains, n'emploie que des Américains et est localisée physiquement dans les locaux d'un service de renseignements : la NSA. Pour pouvoir être déployé, un équipement de chiffrement doit avoir reçu un agrément de SECAN. Cet agrément est discrétionnaire et SECAN n'a pas à justifier ses refus d'agrément. Ainsi, elle n'a pas à révéler ses techniques de cryptanalyse. En évaluant les logiques de chiffrements proposées par les différents membres, SECAN obtient une idée parfaite des connaissances cryptographiques de ses partenaires. SECAN s'est avéré un outil efficace d'antiprolifération en limitant le nombre de pays producteurs compétents à un club très fermé. En effet, les normes

imposées par ce service sont particulièrement sévères et limitent de fait les candidats.

Un autre service de l'OTAN possède les mêmes caractéristiques particulières : DACAN (Distributing Accounting Agency) a pour mission de générer les clefs ou de fournir les moyens d'en créer aux autres nations de l'organisation.

A ce jour, la France ne dispose d'aucun algorithme national agréé par SECAN.

L'Arrangement de Wassenaar

L'Arrangement de Wassenaar est un des quatre accords internationaux traitant du contrôle des exportations. Il a été conclu par un groupe de trente-trois Etats pour limiter l'exportation d'armements conventionnels et de biens ou technologies à double usage vers des Etats «paria». Il permet d'échanger des informations sur le commerce des armes conventionnelles et des biens à double usage. Les participants sont simplement invités à intégrer certaines règles dans leur politique d'exportation. Les produits cryptographiques présentant les spécifications suivantes sont considérés comme biens à doubles usages : clefs supérieures à 56 bits pour les algorithmes symétriques; clefs supérieures à 512 bits pour les algorithmes asymétriques de type RSA; clefs supérieures à 112 bits pour les algorithmes basés sur le logarithme discret.

Ces règles permettent d'avoir une idée des capacités de décryptement des pays occidentaux qui, pour les plus performants, doivent être de l'ordre de grandeur des valeurs ci-dessus. Dans le grand élan de libéralisation cryptographique de la fin du millénaire, l'Arrangement de Wassenaar a temporairement «autorisé» 64 bits pour les logiciels de grande diffusion, mais cette règle a ensuite été abrogée. La concrétisation de la menace intervenue le 11 septembre 2001 et l'augmentation du nombre des décryptements à réaliser ont visiblement convaincu les cosignataires de ramener la limite à une entropie plus raisonnable.

Les travaux universitaires

La cryptologie est devenue une discipline universitaire à part entière à partir de 1976 et de la publication par W. Diffie et M. Hellman de leur article introduisant l'idée de cryptographie à clef publique. En 1977, Rivest, Shamir et Adleman publient et brevettent l'un des premiers algorithmes asymétriques RSA basé sur le problème de la factorisation des grands nombres. Depuis, de nombreux colloques internationaux, tels que la conférence RSA, Eurocrypt, Asiacrypt, Indocrypt sont organisés tous les ans : cinquante-deux colloques internationaux sont organisés en 2004. Une fois la cryptologie tombée dans le domaine universitaire, il devient délicat pour les

Etats de contrôler le domaine. La reconnaissance d'un chercheur étant fonction de ses publications, il est quasiment impossible de lui demander de taire ses découvertes. Ainsi, bien qu'Israël ait une politique de contrôle fort de la cryptologie, les meilleurs chercheurs reconnus sont israéliens.

Certaines publications proposent des cryptanalyses opérationnelles d'équipements réels comme celle du GSM. En revanche, on peut s'étonner du peu de publications de chercheurs américains. Une explication vient probablement du fait que la NSA est réputée être le plus grand employeur de mathématiciens au monde. Au contraire des services de renseignements, des agences COMSEC peuvent autoriser la publication des travaux de leurs chercheurs. Ces publications permettent à ces services d'obtenir une légitimité sur le plan international, ce dont n'a plus besoin la NSA.

L'Advanced Encryption Standard

En 1976, les Etats-Unis ont défini un algorithme de chiffrement standard pour protéger les fichiers sensibles : le *Data Encryption Standard* (DES). Cette logique, initialement conçue par IBM sous le nom de LUCIFER, avait une entropie de 64 bits. La NSA a modifié quelques paramètres et a surtout ramené la taille de la clef à 56 bits, ce qui donne une idée des capacités informatiques de la NSA à cette époque. Le DES, devenu un standard international de fait, est apparu au fil du temps de moins en moins adapté aux applications modernes. La NSA a décidé de faire développer un nouveau standard plus sûr, l'AES (*Advanced Encryption Standard*) et a organisé un concours ouvert à l'ensemble de la communauté internationale : une vingtaine d'algorithmes furent retenus et purent être évalués par la communauté scientifique.

C'est finalement un algorithme belge, initialement baptisé Rinjdael, qui a été retenu par la NSA. Les Etats-Unis ont donc décidé d'utiliser pour leur utilisation propre (hors défense) un algorithme étranger et en ont ainsi fait un nouveau standard international. Il est très probable que la NSA n'est pas en mesure de décrypter un message chiffré convenablement avec l'AES. Les décryptements ne sont alors envisageables que par des voies détournées, comme de mauvaises applications, de mauvaises générations de clefs, de mauvais échanges de clefs, des systèmes d'exploitation bogués, des équipements piégés, *etc.* Le choix d'un algorithme étranger dénote une confiance absolue dans les capacités américaines d'évaluations cryptographiques et une réelle volonté de faire reconnaître le nouveau standard sur le plan international.

L'Europe

Législation

L'exportation des biens à doubles usages, incluant les systèmes cryptographiques, est réglementée par un règlement communautaire de 2000

amendé en 2001. Le règlement européen reprend les propositions de l'Arrangement de Wassenaar : les exportations intracommunautaires sont libéralisées, à l'exception de produits très particuliers comme ceux permettant la cryptanalyse. Pour les exportations vers l'Australie, le Canada, la République tchèque, la Hongrie, le Japon, la Nouvelle-Zélande, la Norvège, la Pologne, la Suisse et les Etats-Unis, une autorisation générale d'exportation communautaire peut être délivrée. Pour les exportations vers les autres Etats, une autorisation nationale peut être délivrée valide uniquement pour un Etat particulier. Sinon, chaque fabriquant doit obtenir une autorisation individuelle.

Utilisation

L'Union européenne n'est pas réputée pour sa capacité à manipuler les informations sensibles. Une commission parlementaire chargée d'enquêter sur le réseau Echelon a permis de mettre en avant les lacunes de l'Union en matière de communications sécurisées : le chef des services du chiffre à Bruxelles a affirmé devant cette commission que le système de chiffrements utilisé par l'Union européenne était «*fiable puisqu'il était testé par les Américains eux-mêmes*». Ce fonctionnaire européen anglais s'est aussi targué d'avoir de très bons contacts à la NSA et que quelqu'un de sa famille y travaillait. Il confirmait que la NSA «*vérifie régulièrement nos systèmes pour voir s'ils sont bien verrouillés et correctement utilisés*».

Cette anecdote montre à quel point l'Union européenne est en retard sur les questions de renseignement. Il est probable qu'une fois les failles identifiées par la NSA, celle-ci ne s'empresse pas de prévenir l'Union européenne des vulnérabilités de son système, mais utilise l'information. Finalement, l'Europe a décidé, au début de l'année 2003, de créer une Agence européenne de sécurité des réseaux. Le périmètre de responsabilité de cette agence n'est pas encore totalement défini, mais il est possible qu'elle ait un rôle centralisateur en matière de cryptologie. Certains Etats sont très réticents à cette idée. La France ne s'est pas portée candidate pour accueillir cette agence, qui s'est finalement installée en Grèce.

France : des prises de contrôle étrangères

Nous avons vu dans l'affaire iranienne que la prise de contrôle d'une société par des fonds étrangers pouvait s'avérer significative. Deux exemples récents concernant directement la France sont révélateurs du fait que ces méthodes sont peut-être toujours d'actualité.

La France est la nation dans laquelle la carte à puce a connu le plus vif succès dès son apparition. La société GEMPLUS est une société française spécialisée dans les cartes à puces. Ces dernières intègrent des moyens cryptologiques forts et contiennent des clefs protégées matériellement. Pour

extraire malhonnêtement ces clefs, différents moyens sont envisageables à partir d'attaques très complexes. Il y a donc un savoir-faire très particulier dans ce domaine : GEMPLUS était très en avance. Pour combler leur retard, les Etats-Unis ont simplement racheté GEMPLUS *via* un fond de placement. Malgré une réaction tardive, la France n'a pas été en mesure de garder GEMPLUS dans son giron. Les Etats-Unis ont donc désormais rattrapé la France dans ce domaine d'excellence qu'est la carte à puce.

En 2003, le ministère français de la Défense a lancé un appel d'offres pour acquérir une infrastructure de gestion de clefs (IGC). Cet outil permet de gérer, certifier et distribuer les clefs de chiffrements utilisées par les applications cryptographiques. La société Thalès a été retenue pour ce marché; pour obtenir des coûts de développement raisonnables, sa proposition s'appuyait sur des modules déjà existants. Elle a choisi comme partenaire la société irlandaise Baltimore, spécialiste des IGC grand public. Depuis, Baltimore a été rachetée par une société concurrente qui appartient à un fond d'investissement américain. Même sans imaginer une opération d'intelligence économique et en ne considérant que de simples investissements dans des entreprises européennes, il est regrettable qu'un système aussi sensible soit réalisé en partie par une entreprise étrangère. Les compétences existent en France. Il est vraiment dommage que des considérations économiques priment sur la sécurité.

* *
*

Jusqu'aux années quatre-vingt-dix, la cryptologie reste une science réservée aux militaires et aux diplomates. Son contrôle demeure ainsi relativement aisé. Quelques nations parviennent à maintenir les compétences au sein d'un cercle restreint. Cette politique de non-prolifération sera maintenue efficacement jusqu'à la fin des années quatre-vingt et la prise en compte du domaine par la communauté scientifique. L'avènement de l'Internet et du commerce électronique au début des années quatre-vingt pousse les Etats à modifier leurs approches.

Les intérêts antagoniques de différentes organisations internationales vont alors s'affronter. L'OCDE promeut explicitement la libéralisation de la cryptologie afin de favoriser le commerce électronique pour lequel la confidentialité est un paramètre essentiel. A l'opposé, l'Arrangement de Wassenaar, dont l'objectif est de limiter la prolifération de certains armements, tente de limiter la diffusion de produits cryptologiquement forts. La vague d'optimisme pacifique résultant de l'écroulement de l'URSS et les espoirs placés dans la mondialisation ont incité les Etats à favoriser l'approche économique au détriment des aspects sécuritaires.

Face aux menaces asymétriques, le renseignement a un rôle majeur à jouer et les interceptions ne devraient pas être neutralisées par la diffusion

inconsidérée de produits cryptographiques forts. Pour autant, cette menace sur les sociétés modernes ne doit pas faire oublier le danger de l'intelligence économique. Les différents rapports traitant d'Echelon et de son utilisation contre des intérêts européens sont suffisamment explicites pour qu'il en soit tenu compte. Il est donc souhaitable de participer aux organisations internationales traitant de cryptologie pour y défendre ses intérêts.

L'approche française consistant à séparer ses services cryptographiques et de cryptanalyses peut alors s'avérer être un atout intéressant. En effet, ses représentants sont moins sujets à caution que les intervenants anglo-saxons systématiquement affiliés aux services de renseignements. L'augmentation des effectifs français traitant de cryptologie et l'activité croissante de la France à l'international dans ce domaine sont de bon augure. La création de l'Agence européenne de sécurité des réseaux indique que l'Europe a pris conscience de son retard dans le domaine de la sécurité des systèmes d'informations. Sa capacité à fixer une politique cryptologique cohérente et indépendante nous renseignera rapidement sur son efficacité.