

LES ÉCOUTES TÉLÉPHONIQUES

Les écoutes téléphoniques désignent l'interception volontaire de communications téléphoniques sans le consentement des personnes concernées. Cette pratique, strictement encadrée par la loi, n'est autorisée que dans le cadre d'enquêtes judiciaires menées par les autorités compétentes. Toute écoute clandestine réalisée par un particulier, un employeur ou une tierce personne constitue un délit pénal.

Les compagnies téléphoniques sont liées à la loi par des contrats ou licences qui donnent accès à l'écoute téléphonique aux autorités.

Quand la commutation téléphonique était mécanique, un détecteur devait être installé sur la ligne par un technicien, qui liait ensuite les circuits pour router le signal audio de l'appel.

Maintenant que la plupart des appels ont été convertis à la technologie numérique, l'écoute téléphonique est devenue beaucoup plus facile, parce qu'accessible par ordinateur. Si le détecteur est implanté sur un commutateur numérique, l'ordinateur de commutation copie et transfère simplement les données qui représentent la conversation téléphonique une deuxième ligne ; il est donc impossible de déterminer si une ligne est sous écoute. Un détecteur bien conçu installé sur une ligne peut être difficile à détecter. Les parasites ou bruits que certaines personnes interprètent comme une écoute téléphonique sont simplement des diaphonies créées par le couplage de signaux provenant d'autres lignes téléphoniques.

Parallèlement à ces formes de surveillance légale, peuvent se produire des écoutes illégales, résultant des agissements clandestins et non autorisés de personnes « privées » voire « publiques ».

Voici un extrait d'une étude sur l'écoute téléphonique réalisée allant du bon vieux téléphone filaire de 1876 aux plus modernes systèmes de téléphonie.

Chacun sait que la solidité d'une chaîne ne vaut que par son maillon le plus faible.

Dans le cas des télécommunications, le maillon faible est justement le système de transmission à distance. Qu'il y ait intervention humaine, comme jadis dans le télégraphe ou avec les opératrices du téléphone, ou que la transmission se fasse par câble, radio ou satellites, le simple fait d'envoyer un signal sur un support physique, le fragilise en terme de sécurité.

Nous allons étudier des méthodes d'interception téléphoniques agrémentées de quelques faits historiques piochés ça et là.

Nous étudierons les techniques de détournement et de capture de l'information, depuis le télégraphe jusqu'aux systèmes informatiques.

Nous évoquerons les différents moyens de protection et de sécurité, les procédés de cryptage faisant l'objet d'un autre chapitre.

Les écoutes téléphoniques sont les plus répandues aujourd'hui, réalisées aussi bien sur l'ordre des politiciens ou des PDG véreux, d'offices clandestines pour le compte d'entreprise, de la police, voire même de la presse. N'importe qui en réalité, peut écouter n'importe qui. Même les ministres s'écoutent entre eux aujourd'hui, c'est à la mode. Les points de raccordement sont multiples, de même que les méthodes.

Les failles viennent aussi des opérateurs. Il faut bien des complicités, ne serait-ce que pour savoir où il faut connecter une bretelle.

Commençons avec le Télégraphe

Les problèmes du télégraphe optique de Chappe

Le système de Chappe, présentait en terme de sécurité une lacune de taille : il suffisait de s'équiper d'une lunette assez puissante et de se placer au bon endroit pour capter les messages qui circulaient sur le réseau. Le monopole institué dès l'origine de ce procédé de transmission ne pouvait qu'aiguiser la curiosité des ennemis politique ou militaire de l'État Français. Dès 1801, seul le projet de transmission des résultats de la Loterie nationale est retenu comme application purement civile.

Pendant la Révolution et l'Empire, les usages du télégraphe sont essentiellement militaires, et sous la Restauration, plutôt de police.

Chappe avait mis au point un « vocabulaire » codé, et que seuls les personnels aux extrémités des lignes possédaient ces codes, de sorte que les postes intermédiaires ne savaient pas ce qu'ils transmettaient.

En 1836 une affaire de fraude télégraphique relance le débat sur l'usage de ce moyen de communication.

Deux banquiers bordelais avaient soudoyé un employé du télégraphe pour qu'il ajoute des signaux supplémentaires à la suite de l'envoi des dépêches officielles. Ce système leur permettait d'être informés de l'évolution du cours de la rente d'État avant l'arrivée de la presse qui était expédiée par malle-poste.

Le dispositif était assez rudimentaire et donnait à cette affaire un côté rocambolesque. Pour éviter les erreurs de transmission, inévitables dans le système Chappe, chaque dépêche était décodée au milieu du parcours par le directeur du bureau local de Tours. Le message était alors réémis vers Bordeaux. Les pirates injectaient des signaux supplémentaires indiquant l'évolution des cours de la Bourse, en aval de Tours. Pour informer leurs comparses qui effectuaient cette opération, les fraudeurs leur expédiaient par la malle-poste de Paris des gants blancs ou gris selon que le cours de la rente était en hausse ou non. La fraude dura deux ans. Quand elle fut découverte, les protagonistes furent traduits devant les assises... mais relâchés. Le monopole télégraphique de l'État n'étant pas défini par la loi, on ne pouvait pas les condamner.

Le développement du réseau de télégraphe électrique filaire posa d'emblée les mêmes problèmes de sécurité.

Monopole d'usage de l'État au début, les dépêches étaient « chiffrées » par sécurité. Cependant, sous la pression des saint-simoniens, Louis Napoléon Bonaparte voit dans le télégraphe un instrument susceptible de favoriser l'industrie et de commerce.

L'assemblée reste cependant hésitante. En perdant son monopole d'utilisation du télégraphe « le gouvernement n'aura plus aucun privilège... ». Pour « éviter » qu'on ne livre l'usage du télégraphe aux factions qui s'en serviraient pour ourdir avec plus de facilité et de rapidité leurs détestables complots (*Ferdinand Barrot, discours à la Chambre des députés, 1er mars 1850, in Le Moniteur universel*) la loi exige que les dépêches privées soient en langage clair et signées. L'utilisateur doit déclarer son identité. Ce dispositif de censure n'est pas propre à la loi française ; on trouve des régimes juridiques voisins en Prusse, en Autriche et aux Pays-Bas.

Écoutes télégraphiques à l'aide d'un téléphone :

Lors des expériences menées à [Dax par Jules Thore](#) en 1878 Dufourcet raconte :

Ce n'est pas seulement par des effets d'induction d'une ligne sur une autre qu'on arrive à lire au son les dépêches ; il suffit pour cela de prendre deux fils, de les planter en terre dans une zone de plusieurs centaines de mètres de rayon tout autour d'un bureau, et de les attacher à un téléphone des plus médiocres ; toutes les dépêches transmises ou reçues par ce bureau viendront se répercuter sur la plaque vibrante et lui faire rendre un son assez fort pour qu'une personne un peu exercée puisse les lire .

Avec le téléphone

Très tôt on a pratiqué l'écoute en commercialisant de petits téléphones à installer dans une enceinte privée. Le microphone était caché dans la pièce et les écouteurs dans un autre local pour écouter les conversations.



vers 1900.

Le piratage physique des installations téléphoniques avait commencé avec les militaires en temps de guerre.

En mars 1915, c'est dans le secteur du Saillant de Saint-Mihiel (Meuse), que sont nées des techniques qui vont changer les façons de faire la guerre. Grâce à un sous-lieutenant français **André Delavie** sont apparues, presque par hasard, il y a plus de cent ans sont apparues les premières écoutes téléphoniques.



[Récit de cette histoire \(pdf\)](#)

Le colonel de Malleray le nomme officier téléphoniste, à la tête de 30 téléphonistes. Au cours d'une série d'attaques qui durent cinq jours, les fils ne sont pas coupés, et ce fait est si nouveau et si important que le 20 mars, il est signalé au commandant.

Dans la quinzaine du 5 au 20 mars 1915, un autre fait a attiré l'attention du sous-lieutenant Delavie. Il s'aperçoit, en écoutant sur une de ses lignes, qu'on entend les communications échangées sur d'autres. Ce sont des mélanges, lui disent ses hommes, et on ne peut les éviter. Bien loin d'être satisfait d'une telle explication, le sous-lieutenant examine les lignes dans leur construction ainsi que les tableaux auxquelles elles aboutissent et s'assure qu'aucun contact pouvant provoquer un mélange n'est possible. Il en construit une parfaitement isolée des autres, entre son central de Saint-Agnant, la cote 360 et le camp des réserves de Ronval (forêt d'Apremont), et constate qu'on entend les conversations des lignes voisines ! Dans les postes téléphoniques les plus avancés, les téléphonistes qu'il questionne lui disent et il s'en rend compte qu'on perçoit sur nos lignes, un peu faibles, des mots étrangers.

L'idée géniale jaillit : profiter de ce phénomène pour surprendre les communications téléphoniques allemandes ! Le problème vient des prises de terre à l'extrémité : en les éloignant de plusieurs dizaines de mètres de celles des prises de terre des postes téléphoniques, on peut capter des courants de retour ; et comme les lignes allemandes sont proches, parfois à 50 mètres, on entend distinctement les conversations ennemies !

Le 3 avril, Delavie écrit dans son journal :

« Le capitaine du génie Salmon, ancien élève de Polytechnique, est venu ce matin ; il ne voulait pas se rendre à l'évidence ; je lui ai prouvé par la théorie que les choses pouvaient se passer telles que je les avais expliquées et ensuite je l'ai amené voir l'expérience elle-même ; je lui ai fait contrôler jusque dans les moindres détails de façon qu'il n'y ait pas de doute. Il a très bien entendu et sa réponse définitive a été celle-ci que je transcris malgré son allure militaire : « Eh bien, vous m'avez foutu sur le cul ! »

Le 2 mai, il écrit que son « invention est en route : le corps d'armée en a tiré un certain nombre ». Deux jours plus tard, il affirme : « Mes expériences ont réussi au-delà de toute espérance. Je puis capter à mon gré toutes les communications téléphoniques. Je vais aménager des appareils pour l'écoute des Allemands. Dès hier, on les a entendus chanter dans leurs trous, rire, se moquer du 75, régler le tir, etc. Dans quelques jours, je crois que nous les entendrons comme si nous y étions ». Les généraux d'abord sceptiques furent conquis par les résultats et créèrent une organisation pour les exploiter à grande échelle...

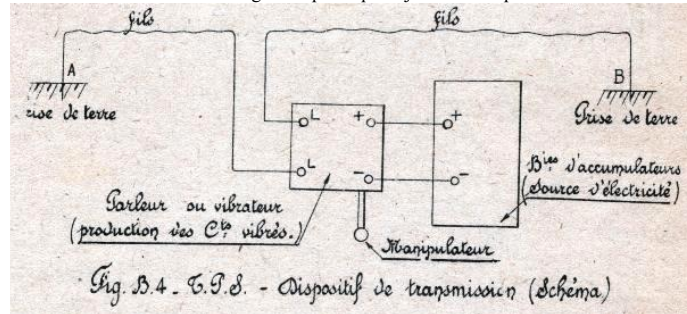
En 1917 le système a bien évolué :

Je vous recommande de consulter le site "[Des téléphonistes et télégraphistes passerands en 14-18](#)" qui raconte ces moments.

Les transmissions se faisaient par téléphonie, mais aussi par télégraphie soit Télégraphie électrique, soit Télégraphie Par le Sol (T.P.S.) soit Télégraphie Sans Fil (T.S.F.). On y apprend comment faire de la télégraphie par le sol (T.P.S.)

« La télégraphie par le sol a été utilisée dès 1917 pour établir des liaisons à courte distance (portée 3 km environ).

Elle évitait l'utilisation d'une ligne téléphonique sujette aux coupures lors des bombardements. »



On a rapidement compris aussi qu'elle pouvait aussi servir de communication entre 2 galeries de mine sans qu'il soit nécessaire de tirer du câble entre les 2 boyaux ... La réception ne peut toutefois pas dépasser un rayon de 3 km. Le fil en lui-même est un fil de terre, donc assez solide, beaucoup plus solide que le fil normal de téléphone et il est aussi assez court (moins de 100 m). Il ne peut être coupé que par de l'artillerie, et pas par le piétinement ou autre. S'il est coupé et qu'il existe une extrémité qui reste fichée en terre, le système fonctionne encore. S'il est tout à fait coupé, il est facile de le faire réparer, même en plein bombardement par un télégraphiste qui n'a pas besoin d'aller fort loin pour retrouver la coupure... L'invention a fait l'objet d'un brevet dès 1910 ; ce n'est donc pas un secret militaire.



Dès 1916, l'expérience du sous-lieutenant Delavie se généralise avant la création officielle, début 1917, des Sections spéciales d'écoute mises au service du Service de Renseignements.

Celles-ci se composent de techniciens qui doivent repérer les endroits où des « fuites » permettent d'intercepter les conversations ennemies et d'interprètes capables d'écouter, en temps réel, les conversations ennemies.

Le rôle de ces interprètes est d'autant plus difficile qu'il leur faut comprendre non seulement l'allemand mais aussi ses différents patois, et être familiarisés, dans la langue de Goethe comme dans celle de Voltaire, avec la terminologie militaire.

La plupart des interprètes travaillant déjà pour l'état-major, les Sections spéciales se rabattrent sur quelques professeurs et sur des volontaires de la Légion étrangère d'origine allemande ou suisse.

Durant les deux dernières années de la guerre, les écoutes téléphoniques rendront d'inappréciables services, permettant de juger du moral des troupes ennemies, de tenir à jour ses mouvements et, au niveau des champs de bataille, d'être informé de ses offensives et de capter les informations destinées au réglage de l'artillerie. Ajoutons que ces humbles auxiliaires du Service de Renseignements travaillent dans les tranchées de première ligne, directement sous le feu des Allemands. Leur travail de repérage permettra aussi de colmater quelques brèches béantes ouvertes dans les communications françaises. Leur rôle et même leur simple existence sont restés, jusqu'à ce jour, quasi ignorés des historiens.

Anecdote : Le Cri de Paris août 1917

C'est dans une caserne très parisienne que la scène se passe.

Mme de M., dont le mari est mobilisé à l'état-major d'une armée alliée, entre invincible et émue dans un bureau - un bureau, non, le dernier salon où l'on flirte. Après le baise-main et l'échange des usuelles politesses, elle expose l'objet de sa visite à l'officier de service : - Mon cher capitaine, ayez l'obligeance de téléphoner tout de suite à mon mari que bébé est maintenant tout à fait bien et que sa petite colique n'a rien été.

L'officier s'empresse de téléphoner à l'état major la bonne nouvelle. La dame remercie et part dans un frou-frou soyeux et parfumé.

C'est la guerre.

Apparue en 1917, la TPS nécessite le cryptage des messages, ce qui est peu compatible avec les situations d'urgence, aussi est-elle le plus souvent utilisée comme un moyen de secours, des ingénieurs français s'aperçoivent que, grâce à un phénomène technique lié au mode de communication de l'époque (le « retour » des téléphones se faisant par la terre, au moyen de piquets enfoncés dans le sol), il est possible, dans certaines conditions, d'écouter les conversations adverses. Et ce, d'autant plus que les premières années de la guerre se feront dans les tranchées et que les lignes ennemies sont parfois proches de quelques mètres.

Dès 1916, pendant la bataille de Verdun, un premier poste d'écoute artisanal donnera de bons résultats, et l'expérience se généralise avant la création officielle, début 1917, des Sections spéciales d'écoute mises au service du Service de Renseignements. Celles-ci se composent de techniciens qui doivent repérer les endroits où des « fuites » permettent d'intercepter les conversations ennemies et d'interprètes capables d'écouter, en temps réel, les conversations ennemies. Le rôle de ces interprètes est d'autant plus difficile qu'il leur faut comprendre non seulement l'allemand mais aussi ses différents patois, et être familiarisés, dans la langue de Goethe comme dans celle de Voltaire, avec la terminologie militaire. La plupart des interprètes travaillant déjà pour l'état-major, les Sections spéciales se rabattront sur quelques professeurs et sur des volontaires de la Légion étrangère d'origine allemande ou suisse.

Durant les deux dernières années de la guerre, les écoutes téléphoniques rendront d'inappréciables services, permettant de juger du moral des troupes ennemies, de tenir à jour ses mouvements et, au niveau des champs de bataille, d'être informé de ses offensives et de capter les informations destinées au réglage de l'artillerie. Ajoutons que ces humbles auxiliaires du Service de Renseignements travaillent dans les tranchées de première ligne, directement sous le feu des Allemands. Leur travail de repérage permettra aussi de colmater quelques brèches béantes ouvertes dans les communications françaises. Leur rôle et même leur simple existence sont restés, jusqu'à ce jour, quasi ignorés des historiens.

1940 L'histoire de la Source K. (Extrait de « Résistance PTT »)

Le 20 juillet 1940, les services d'entretien des lignes souterraines à grande distance regagnent Paris.

L'accord passé entre l'administration des P.T.T. et les autorités d'occupation prévoit la reprise en main par les techniciens français, sous contrôle allemand, de l'ensemble du réseau, à l'exception des territoires intégrés au Reich, ou rattachés au protectorat du gauléiter nommé en Belgique Robert Keller retrouve donc son poste et ses responsabilités. Ses équipes conservent leur ancienne structure, mais doivent supporter l'incorporation d'un ou deux pionniers allemands par groupe. Durant plusieurs mois, la tâche essentielle consiste en une réfection rapide des grands circuits. Keller, qui nourrit déjà certains projets, veille à la bonne exécution des travaux. Il stimule si bien ses hommes que peu à peu la surveillance se relâche et qu'il parvient à visiter ses chantiers sans être flanqué de ses indésirables accompagnateurs. Bientôt même, les équipes d'urgence ne vont plus avoir d'observateurs à leurs côtés lors des interventions.

C'est au cours de ces quelques mois que Robert Keller établit un plan d'action avec schéma visant à neutraliser le réseau des lignes souterraines à grande distance. On ignore tout des liaisons qu'il eut à cette époque, car il a emporté ce secret dans sa mort, mais ce qui est certain, c'est que ce plan parvint en Angleterre puisqu'il figurait parmi les archives du B.C.R.A. (Bureau central de renseignements et d'action était un service d'espionnage français, créé en 1940). Minutieusement rédigé, il montrait comment, en quelques heures, on pouvait bloquer tous les circuits, et isoler téléphoniquement les centres vitaux du commandement allemand. Ce projet, conçu dans le cadre d'un débarquement allié, aurait été d'une importance capitale en juin 1944 si son auteur avait encore été là pour le faire appliquer. Mais la discrétion, bien compréhensive, dont Robert Keller fit preuve, ne permit à aucun de ses camarades de pouvoir l'utiliser.

Devenu représentant du S.R. au sein de la Direction des Recherches et du Contrôle technique des P.T.T., le capitaine Combaux s'est assuré le concours de M. Sueur, ingénieur de ce service. Les deux hommes ont longuement réfléchi sur les moyens à mettre en œuvre pour capter les conversations allemandes qui passent par les câbles à grande distance. Sécurisés par l'important dispositif qui contrôle les circuits, les occupants les utilisent en exclusivité pour leurs liaisons avec le Reich.

Les lignes : Paris - Reims - Verdun - Metz, reliée à Sarrebruck, et Paris - Châlons - Nancy - Sarrebourg - Strasbourg reliée à Appenweier, sont particulièrement surveillées puisqu'elles mettent en relations toutes les sphères des autorités d'occupation avec leurs hiérarchies de Berlin. Combaux et Sueur savent bien que surprendre les communications qui s'échangent sur ces câbles prioritaires permettrait de percer le secret des plans allemands, et par là même de leur porter un terrible coup en faisant bénéficier les Alliés de ces informations. Seulement atteindre les circuits par les voies normales relève de l'utopie. Tous les postes d'amplification, toutes les stations de répéteurs, sont, ainsi qu'on l'a montré précédemment, placés sous une surveillance sévère. Les vérificateurs français qui en assurent le fonctionnement ne peuvent faire le moindre geste sans éveiller l'attention des techniciens allemands qui les doublent. La seule et unique possibilité qui existe, mais combien illusoire et insensée dans sa réalisation, c'est celle avancée par M. Sueur : le « piquage sauvage sur câbles ».

Pourtant, aussi téméraire et extravagant qu'il soit, c'est à ce projet que s'attaquent les deux hommes. Sur le papier, son exécution ne paraît pas insurmontable. Il faut préparer des amplificateurs spéciaux à grande impédance d'entrée qui puissent être insérés dans les circuits sans modifier les impulsions des stations de mesure. Les câbles étant en effet équilibrés en constantes électriques fixes, la moindre variation est facilement décelable. Or, dans le plan établi par Sueur, il conviendrait d'introduire sur la ligne des appareils et un mètre de câble les reliant au circuit. Un tel branchement présente de gros risques, car il entraînerait sûrement une modification des indices sur les mesures habituelles ; à moins que les appareils espions ne soient appropriés avec une précision rigoureuse. C'est un premier obstacle, mais il peut être franchi grâce à la haute compétence des spécialistes. Le second palier du projet consiste à louer au plus près du lieu de dérivation prévu une habitation discrète dans laquelle on pourrait placer les têtes et les amorces de câble ainsi que les amplificateurs d'écoutes. C'est le point qui présente le moins de difficultés, encore que rechercher une maison libre, présentant des garanties de tranquillité et de sécurité, sur le parcours des lignes, n'apparaisse pas aussi simple que cela.

Mais ces deux premiers volets de l'opération imaginée par Sueur et Combaux ne sont qu'un aimable enfantillage en regard de ce que représente le dernier, car il s'agit maintenant d'intervenir sur le câble lui-même. À partir de là, on entre dans une phase du projet qui semble irréalisable. Il faudrait, en effet, en dépit de la surveillance allemande, ouvrir des fouilles sur la ligne, ce qui peut déjà demander plusieurs jours ; creuser une tranchée préparatoire au niveau de la dérivation ; sortir du pavillon loué les amorces préalablement apprêtées ; accéder au câble en service, l'ouvrir, dénuder les fils un par un et sélectionner sans erreur ceux des circuits à mettre en écoute, les couper, les dériver, puis rétablir vivement le contact

afin que l'opération ne cause pas un trop long dérangement susceptible d'intriguer les techniciens allemands ; ensuite, remettre tout en place et refermer les fouilles. Un travail aussi périlleux, comportant tant de risques, qui pourrait le faire ?

Ceux qui tenteraient de l'entreprendre devraient être des hommes aux nerfs d'acier, aux capacités professionnelles affirmées, connaissant parfaitement le schéma des grands circuits et leurs particularités, doués d'une audace hors du commun, et animés d'un esprit patriotique poussé jusqu'à l'abnégation. De plus, il ne pourrait s'agir que d'une équipe soudée, habituée à travailler en harmonie et confiance, dirigée par un responsable lucide aux compétences certaines, capable de maîtriser les impondérables.

Enthousiaste et sceptique à la fois, le capitaine Combaux posa la question :

— Un tel chef d'équipe existe-t-il seulement ?

— Oui, répondit M. Sueur, je le connais, c'est l'Ingénieur Robert Keller.

C'est dans les premiers jours de septembre 1941, la date est imprécise, que les deux instigateurs de ce projet extraordinaire le soumettent à Keller. L'entrevue a lieu dans le bureau de M. Sueur, rue Bertrand. Cet entretien mémorable mérite d'être relaté par l'un de ses participants. Écoutons donc le capitaine Combaux nous en faire le récit :

« Je posai le problème ; M. Sueur développa la solution technique. Robert Keller écoutait et approuvait. J'étais plus ému que je n'aurais voulu le paraître lorsque je m'adressai à lui pour insister une dernière fois, avant la décision finale, sur les dangers de l'aventure. J'étais officier ; le risque de guerre faisait partie de mon métier. Je pouvais sentir au-dessus de moi des chefs militaires qui surveilleraient de loin le combat que nous allions livrer. Il n'en était pas de même pour mes compagnons. Ils devaient agir à l'insu de leurs supérieurs hiérarchiques ; quelque envie que nous en ayons eue, nous avions le devoir de ne point compromettre dans une affaire aussi grave le Directeur des Télécommunications, dont nous connaissions les bons sentiments, mais qui avait la lourde charge de défendre devant l'occupant l'ensemble de nos services. Robert Keller avait, plus que tout autre, des raisons d'hésiter. Il songeait à sa femme et à ses quatre enfants. Il pouvait, sans déshonneur, rejeter une entreprise aussi téméraire, et dans laquelle il allait courir, en raison même de ses fonctions, les risques les plus graves. Il accepta cependant. Il fit avec résolution le premier pas sur la route fatale qui allait le mener au supplice...

Il nous dit tout de suite qu'il avait derrière lui une équipe sur laquelle il pouvait compter, prête à braver tous les dangers pourvu que cela soit contre l'ennemi et pour la France. Le vérificateur Lobreau, les chefs d'équipe Laurent Matheron et Pierre Guillou étaient de ceux-là. Ils l'avaient suivi et assisté au cours de la première campagne de France. Ils

allaient être auprès de lui, devant un danger considérablement accru, et avec la même fidélité.

Sur Robert Keller, en vérité, reposait le succès ou l'échec de l'entreprise. Si Sueur pouvait se charger de l'étude et de la réalisation des amplificateurs, si je pouvais régler l'acquisition du local et les questions d'exploitation, lui seul était capable de réaliser l'essentiel, d'accomplir ce tour de force incroyable que représentait le travail sur câble... » Que Robert Keller eût refusé à cet instant les propositions de ses interlocuteurs, et la Source K serait demeurée à l'état de projet, car aucun technicien des P.T.T. ne réunissait alors ni les compétences ni les qualités requises. Pas un ne possédait suffisamment d'ascendant et n'inspirait assez la confiance pour entraîner une équipe de spécialistes cette voie périlleuse.

Et ceux qui au S.R. choisirent l'initiale K de Keller pour désigner la source de renseignements vitaux qui leur parvinrent par ce canal ne pouvaient mieux montrer que c'est à cet homme héroïque qu'ils durent la somme d'informations sensationnelles dont ils firent bénéficier les Alliés.

L'acceptation de Robert Keller déclenche le démarrage de l'opération. Sueur effectue une étude très poussée pour déterminer le nombre d'amplificateurs nécessaires. Il parvient à la conclusion qu'il faut en prévoir un minimum de 6. Leur fabrication délicate, et le coût élevé de celle-ci, posent un premier problème. Un habile travail d'approche permet toutefois à l'ingénieur d'acquiescer la complicité active du chef des laboratoires de la Société anonyme de télécommunications, société privée, qui travaille exclusivement pour les P.T.T. M. Lebedinski, russe d'origine, mais naturalisé français, accepte en effet spontanément de faire construire dans les ateliers de son entreprise repliée à Montluçon les pièces détachées des appareils conçus par M. Sueur. Grâce aux camions qui font la navette entre l'usine et les entrepôts demeurés en zone occupée, les éléments d'amplificateurs passeront sans problèmes la ligne de démarcation. De son côté, le capitaine Combaux règle la question des fonds nécessaires à une telle opération.

Doté par les soins du S.R. d'un laissez-passer permanent, il se déplace à volonté entre les deux zones ; ce qui lui permet de recevoir du capitaine Simoneau au cours de ses voyages tout l'argent indispensable à la mise sur pied du projet. Dans le même temps, le poste P 2 du S.R. fait diligence pour recruter et former des opérateurs valables. Tâche ardue assurément, car ceux-ci doivent parler, et surtout parfaitement comprendre la langue allemande, y compris dans les variations de la conversation courante. Il leur faut également posséder le sens de l'initiative et l'instinct de débrouillardise, vitaux pour leur travail et leur sécurité. Enfin, il va de soi que pour noter tout ce qu'ils entendront, il leur est indispensable d'avoir une parfaite maîtrise de la sténo, et de connaître les structures de fonctionnement des services du Reich.

Le premier opérateur envoyé à Combaux par Simoneau arrive à Paris le 5 mars 1942 ; c'est le sergent-chef Édouard Jung. Ayant suivi les cours accélérés du centre d'instruction clandestin du S.R., connaissant parfaitement l'organigramme de la Wehrmacht et les noms des principaux officiers des différents services fonctionnant à Paris, c'est un habile spécialiste des transmissions, Alsacien de naissance, que Simoneau a eu la chance de pouvoir récupérer. Nanti de pièces d'identité irréprochables, il est aussitôt dirigé sur la Compagnie d'Assurances « La Nationale » où le sous-directeur M. Grimpel et l'agent général pour la région parisienne, M. Lionel Levavasseur, lui fournissent la carte accréditive d'inspecteur qui lui assurera une couverture de premier ordre.

Quelques jours plus tard, Jung parvient à repérer un pavillon libre sur le parcours du câble dans la Grande Rue de Noisy-le-Grand.

(Ce pavillon était situé au 89 Grande Rue (aujourd'hui avenue Emile Cossonneau) à l'intersection de la N 370 et du CD N° 75 E. Réaménagé ces dernières années, ce carrefour porte maintenant le nom de « Place du 8 Mai 1945 ». La municipalité de Noisy-le-Grand a donné le nom de « rue du Réseau Robert Keller » à l'ancienne rue des Grammonts qui prend naissance à cet endroit pour rejoindre les bords de Marne.)

Après quelques démarches, il en obtient la location que Combaux s'empresse de régler. Située à moins de 6 mètres de la ligne, cette petite maison offre toutes garanties par son isolement, et son sous-sol surplombe de peu la route nationale sous laquelle court le câble Paris-Metz. Sans perdre de temps, Édouard Jung s'y installe, complétant l'aménagement sommaire laissé par le propriétaire de quelques meubles ramenés du marché aux puces de Montreuil. À peine sur place, sous prétexte de fuites dans les canalisations d'écoulement, il creuse une tranchée jusqu'à la haie de clôture bordant la route nationale, puis le mur du sous-sol est percé afin de laisser le passage à une gaine de protection. Le 6 avril 1942, tout est prêt pour recevoir le matériel d'écoute. Trois jours après, M. Lebedinski fait livrer les amplificateurs que M. Sueur transporte aussitôt au pavillon ; les têtes de câble et les amorces suivent. Il ne reste plus sur place qu'à procéder au montage de tout cet équipement en attente de branchement.

Le 10 avril, c'est chose faite ; la première phase de l'opération est terminée. Pendant la durée de ces préparatifs, Robert Keller n'est pas resté inactif. Après un minutieux examen des schémas et un relevé de la zone choisie pour la dérivation, il a mis au point le procédé d'attaque du câble et réuni l'outillage le plus adapté à cette intervention.

Puis, après mûre réflexion, il a choisi les hommes lui paraissant les plus qualifiés et les plus audacieux pour entreprendre un travail aussi difficile.

À chacun d'eux, il a soumis le plan de l'affaire en insistant sur les risques qu'elle comporte. Sur de leur fidèle discrétion, quelle que soit la décision prise, il leur a demandé de réfléchir avant de donner leur réponse. Mais celle-ci ne s'est pas fait attendre et, l'un après l'autre, les six compagnons qu'il a sollicités sont venus lui dire qu'ils étaient prêts à le suivre dans cette action dont ils savent mieux que personne qu'elle risque de les entraîner sur un mortel chemin.

Les affiches collées sur les panneaux de service dans chaque atelier, dans chaque centre, sont à cet égard éloquentes. L'administration militaire allemande prévient en effet que : « Tout endommagement des moyens de transmission sera puni de la peine de mort. » Malgré cette menace, dont ils savent bien qu'elle n'est pas formulée à la légère, les hommes choisis par Keller n'hésitent pas. Et aujourd'hui, l'on ne sait pas ce qu'il convient d'admirer le plus : de cette confiance totale montrée vis-à-vis d'un chef estimé, mais téméraire, ou de ce tranquille courage patriotique bien dans la tradition de l'engagement résistant.

Le 2 avril, l'équipe formée par Robert Keller est constituée. Elle comprend :

Les vérificateurs : Lobreau du centre Paris-Saint-Amand, et Fugier du centre de La Ferté-sous-Jouarre.

Les techniciens sur ligne : Pierre Guilou, Laurent Matheron, Abscheidt et Levasseur.

Dans le plan prévu par Keller, chacun de ces spécialistes aura un rôle important à jouer pour lequel, en dehors des compétences professionnelles, l'audace et le sang-froid ne devront pas faire défaut. Ce plan, il faut maintenant l'exécuter.

Le 15 avril 1942, Robert Keller crée un défaut artificiel sur le câble Paris-Metz. La « Feldschalt-Abteilung » saisit le service de dérangement des lignes souterraines à grande distance d'une énergique réclamation, car deux circuits sont interrompus. C'est bien ce qu'espérait Robert Keller qui, nanti d'une autorisation de travaux en bonne et due forme signée par l'Administration, regroupe son équipe et part à la recherche du point de rupture. Naturellement, celui-ci est découvert à Noisy-le-Grand, en face du pavillon loué par Édouard Jung.

Le 16 au matin, les fouilles sont entreprises sur le trajet du câble. Afin de donner le change à d'éventuels curieux, deux tranchées sont ouvertes à côté de celle dans laquelle la dérivation doit être effectuée.

Le 17, en fin de matinée, un technicien allemand vient sur place s'informer de l'état des travaux. Satisfait de la célérité déployée par les spécialistes français et des réponses rassurantes qui lui sont faites, il repart aussitôt. Keller a décidé, pour des raisons de sécurité, que l'intervention sur le câble se fera de nuit, et il en a informé Combaux. Dans la soirée du 18, ce dernier vient rejoindre l'équipe sur le chantier. Une tente d'intempérie a été disposée au-dessus de la fouille centrale afin de masquer un peu les travaux, et de filtrer l'éclairage dispensé par les lanternes ; des lueurs trop vives pouvant provoquer une réaction des patrouilles allemandes obnubilées par les consignes sévères du camouflage lumineux. Un peu avant 21 heures, Keller, Guillou et Matheron descendent dans la tranchée et s'attaquent au câble. Sitôt la gaine de plomb mise à jour, Keller se porte sur la ligne de service et donne l'ordre aux deux vérificateurs des stations de répéteurs encadrantes : Lobreau à Paris-Saint-Amand, et Fugier à La Ferté-sous-Jouarre, de retirer un à un chaque circuit de l'exploitation durant le temps nécessaire à sa coupure et à sa dérivation.

C'est ce que font sans hésiter les deux hommes, sous les yeux mêmes des techniciens allemands, en prétextant un contrôle des mesures. Pour eux, la nuit va être longue, car ils vont devoir agir avec une apparence routine désinvolte devant leurs surveillants, tout en portant une extrême attention aux directives précises que leur transmettra Keller.

Aucune erreur ne leur est permise, car elle se répercuterait aussitôt dans les autres centres d'amplificateurs dont le personnel a été laissé en dehors de l'action.

Dans la fosse, penchés sur leur ouvrage, les trois hommes travaillent dans un silence tendu. Keller sélectionne les fils, ne quittant pratiquement pas le téléphone qui assure la liaison avec les vérificateurs, annonçant tranquillement les références du circuit à suspendre le temps de l'intervention. Guillou et Matheron, les mâchoires serrées, s'activent, mesurant leurs gestes rapides. Ils coupent, décapent, épissurent, soudent, les mains plongées dans l'inextricable amas de conducteurs, s'arrêtant un bref instant pour essuyer la sueur, due à l'effort et à la l'émotion, qui perle à leur front. Sur la chaussée, Combaux feint de s'affairer à quelque tâche urgente, veillant à ce que les lueurs qui filtrent de la tente mal jointe n'alertent

pas les servants d'une batterie de D.C.A. de la Wehrmacht située à moins de 300 mètres en amont. De temps en temps, une estafette motocycliste allemande passe, contournant la barrière mobile du chantier, jetant un regard distrait sur les fouilles. Dans la tranchée, autour du câble, on s'affaire toujours sur le même rythme. Soudain, désastre ! une manœuvre un peu trop rapide entraîne une forte variation de la constante électrique de l'isolement. Au centre de Paris-Saint-Amand, Lobreau, la gorge sèche, voit l'aiguille de l'appareil de mesure battre la chamade. Un bref coup d'œil sur le côté lui montre les deux Allemands de service avachis sur leurs chaises, les paupières lourdes, aux prises avec le traditionnel coup de barre de l'après-minuit. Ils n'ont rien remarqué ; les minutes passent angoissantes pour le vérificateur qui devrait réagir, mais que sa complicité avec l'équipe maintient cloué sur son siège, le regard fixé sur le cadran témoin. Pourant petit à petit, l'aiguille revient vers la zone de sécurité. Là-bas, sous la tente, Keller et Guillou se démenent pour rétablir l'isolement. Un quart d'heure encore, et Lobreau, avec le soulagement qu'on imagine, voit la tension revenir à son niveau habituel.

Trois heures du matin. Cela fait maintenant six heures que les trois postiers s'acharnent sur les fils ; cinquante-cinq grands circuits sont déjà dérivés, mais Keller et ses deux camarades poursuivent leur travail. À La Ferté-sous-Jouarre, au poste de répéteur, Fugier, les mains rendues moites par l'énervement, affecte le plus grand calme en déconnectant puis replaçant ses lignes sous le regard endormi de ses surveillants. Imperturbable dans la fosse, Keller continue de donner ses directives tout en refixant les isolants, cependant que Guillou et Matheron, tantôt accroupis, tantôt à genoux, les reins brûlants, endoloris par l'effort constant de recherche d'une meilleure position, maîtrisent leurs gestes, un peu plus gourds maintenant que la fatigue se fait sentir. Au-dessus d'eux, sur la route, Combaux, rongé par l'anxiété, sent les minutes devenir de plus en plus longues au fur et à mesure que le temps passe. En cette nuit froide d'avril, silencieuse, et lugubre sous la pâle clarté des candélabres qui diffusent une faible lumière bleutée, lui seul a tout loisir de laisser ses pensées s'égarer dans l'évocation du risque-tout en écoutant les clochers de Noisy et de Neuilly de chaque côté de la Marne se renvoyer les heures si lentes à s'écouler. Ses trois compagnons, eux, tendus vers le but à atteindre, absorbés par leur difficile travail, ne connaissent pas en ce moment, et c'est heureux pour la réussite de l'opération, ce dangereux vagabondage de l'esprit.

Quatre heures vingt. Robert Keller replie le schéma qui lui a permis de sélectionner les circuits.

Guillou et Matheron fignolent la dernière épissure. Le câble est regarni, puis calé soigneusement au niveau du piquage.

Quatre heures quarante. La dérivation est terminée. Les trois hommes remontent. Rapidement la fouille est comblée. L'aube se lève lorsque les dernières pelletées de terre égalisent le terrain.

Abrutis de fatigue dans la camionnette qui les ramène à Paris, les auteurs de cette extraordinaire opération demeurent silencieux. Réalisent-ils qu'ils viennent d'effectuer véritable exploit ? Soixante-dix grands circuits ont été dérivés, parmi lesquels ceux qui assurent les liaisons de la Kriegsmarine, de la Luftwaffe, de la Wehrmacht, et de Gestapo, entre Paris et Berlin ! Jamais aucun service d'espionnage n'avait rêvé pouvoir bénéficier d'une telle source !

La dérivation étant effectuée, c'est maintenant à M. Sueur qu'il appartient de mettre la table d'écoute en service. Prévenu par le capitaine Combaux de la réussite de l'opération, il arrive aux premières heures de la matinée du 19 avril au pavillon de Noisy, accompagné d'un fidèle ami, spécialiste des Transmissions de l'État, M. Deguingamp auquel il accorde toute confiance. Immédiatement, ils se mettent en devoir de procéder aux raccordements. Laissés en attente, les fils qui s'épanouissent sur des appareils appelés « têtes de câble » vont être reliés aux amplificateurs, puis les postes d'écoute sont à leur tour branchés. Lorsque Édouard Jung, informé par Combaux, se présente, tout est pratiquement prêt à fonctionner. Avec une infinie prudence, les deux techniciens effectuent les premiers essais. On a choisi le moment où Lobreau et Fugier auront repris leur service afin qu'ils puissent veiller, chacun dans leur centre, sur les mesureurs de tension. Mais tout va bien, le travail accompli par Keller, Guillou, et Matheron ne recèle aucune imperfection. Jung peut commencer ses longues factions ; la Source K est opérationnelle !

C'est le 19 avril 1942 dans la soirée, que l'opérateur du S.R. enregistre les premières conversations ; mais c'est vraiment à partir du 20 que l'écoute porte ses fruits. En cette seule journée, Édouard Jung intercepte plus de 60 communications. L'importance du trafic l'oblige alors à sélectionner parmi ce flot continu les circuits présentant le plus grand intérêt, et il se contente de relever les liaisons des armes — marine- aviation-armée de terre — avec le Haut Commandement de Berlin. Devant un pareil afflux, le capitaine Combaux réclame un second opérateur, et le S.R. choisit parmi les agents en stage M. Rocard, jeune licencié d'allemand, ancien lecteur dans une université d'outre-Rhin. L'arrivée de ce deuxième spécialiste double bien sûr le nombre d'informations. Les deux hommes abattent une besogne écrasante.

Aux heures d'écoute s'ajoute le temps passé à transcrire à l'encre sympathique, sur des lettres, rapports, ou contrats, les renseignements les plus importants ; ceux présentant un moindre intérêt sont acheminés irrégulièrement par porteur. À Combaux revient le soin d'organiser la transmission au poste P 2 du S.R. de toutes ces informations. Il parvient à assurer cette liaison et le passage de la ligne de démarcation grâce à un ambulancier de la S.N.C.F. ; par la suite, il emploiera également un garçon des wagons-lits, puis un mécanicien de locomotive. Arrivés dans le service du capitaine Simoneau, les renseignements fournis par la Source K sont triés soigneusement. Ceux qui peuvent intéresser le gouvernement de Vichy et influencer sa politique vis-à-vis du Reich sont remis au colonel Rivet qui, après les avoir analysés minutieusement, décide ou non de leur envoi au général Revers, chef d'État-major de Darlan. Mais les plus vitaux, ceux qui fournissent des indications précieuses sur les projets allemands, ainsi que ceux qui font état de la situation militaire et de l'évolution de la stratégie du Haut Commandement, passent directement du S.R. à l'I.S. par les liaisons « Olga », ou par les liaisons radio de l'équipe du commandant Bertrand, ou encore par les postes de Berne et de Lisbonne.

(Notons qu'il existait, entre autres, une liaison du S.R. Lyon-Londres qui était assurée par le relais d'Annemasse de M. Francillon, qui, arrêté un peu plus tard, sera fusillé par les Allemands).

Afin que leur origine ne puisse être décelée, les rapports émanant de la Source K subissent par le poste P 2 un démarquage avant leur transmission à l'échelon supérieur. Cette précaution interdit une remontée à contresens de la filière, et elle est d'autant plus facile à assurer qu'il ne peut y avoir de retours par cette voie-là. Pour compléter la sécurité, un cloisonnement rigoureux verrouille les maillons de la chaîne par groupes de deux à quatre unités. Ainsi, les opérateurs n'ont qu'un seul interlocuteur Combaux, mais les techniciens des P.T.T., mis à part Sueur et Keller, ne le connaissent pas. Parallèlement, les agents de liaison ignorent tout des postiers. En fait, le pivot de l'affaire est le capitaine Combaux ; en cas d'intervention ennemie, c'est donc lui qu'il convient de protéger.

Robert Keller l'a parfaitement compris, et il s'y emploiera le moment venu.

Devant les résultats inespérés des écoutes sur le câble Paris-Metz, Sueur, Combaux, et Keller envisagent de réaliser la même opération sur le Paris-Strasbourg. Une étude fouillée des grands circuits a montré que les liaisons téléphoniques allemandes empruntent également ce canal. En juillet 1942, Robert Keller présente à ses deux amis le schéma de la dérivation à entreprendre. Entre-temps, un troisième opérateur formé par le S.R. a été mis à la disposition de la Source K par le poste P 2. Il s'agit d'un jeune Alsacien :

Prosper Riss, qui reçoit également une couverture d'inspecteur d'assurances de « La Nationale ». Combaux le charge de rechercher un pavillon libre sur le parcours de la ligne souterraine. Il en trouve bientôt un à Livry-Gargan dans lequel il s'installe aussitôt. Sur la demande de Sueur, M. Lebedinski commande les pièces détachées nécessaires au montage de nouveaux amplificateurs, tandis que Pierre Guillou, promu depuis peu au grade de chef d'équipe, délimite sur place le tracé de la tranchée de jonction.

Fin août, l'aménagement du local est terminé ; il ne reste plus qu'à mettre en place les amplificateurs et à effectuer la dérivation.

Cependant à Noisy-le-Grand, le climat se détériore. Les Allemands ont décidé d'implanter une forte unité à l'Est de Paris et, dans cette perspective, un détachement précurseur sillonne la bourgade afin de rechercher de nouveaux cantonnements. Une vaste opération de réquisition de locaux, de maisons, de chambres commence, au grand dam des Noisèens furieux. Dans le quartier où se trouve situé le pavillon des écoutes, la grogne s'affirme particulièrement, et plusieurs réclamations parviennent à la Mairie pour signaler à la commission de recensement qu'au lieu de « vouloir imposer à de braves Français l'hébergement d'officiers allemands, elle ferait mieux de s'intéresser aux individus suspects, vivant d'on ne sait quoi, qui hantent un pavillon même pas trop meublé »

À ces protestations s'ajoutent des commérages de quartier qui évoquent l'activité d'espions... allemands ! Nous sommes à la mi- septembre, et les ragots prolifèrent de plus en plus.

Prévenu par Édouard Jung, le capitaine Combaux, s'inspirant de la règle des services secrets : « la sécurité prime tout », décide alors le repli immédiat de la station clandestine.

Dans la nuit du 16 au 17 septembre, Robert Keller, Pierre Guillou, et Laurent Matheron, démontent toute l'installation, colmatent les têtes de câble, et font disparaître toute trace de la dérivation. Lelendemain, M. Sueur et Deguingamp viennent récupérer les amplificateurs qu'ils transportent à Livry-Gargan. Le 18 au soir, plus rien ne subsiste de cinq mois d'écoutes permanentes. Le petit pavillon de Noisy-le-Grand retourne à l'anonymat, prêt à accueillir les indésirables locataires dont ses murs ont pourtant enregistré

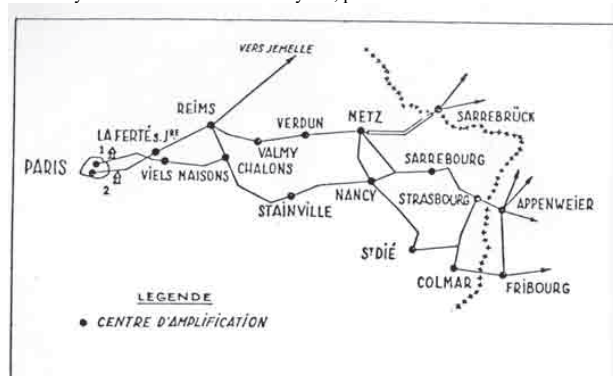


Schéma des câbles à grande distance reliant, en 1942, la France à l'Allemagne. (Les chiffres 1 et 2 indiquent les points de dérivation choisis pour la mise en place des écoutes, à Noisy-le-Grand et à Livry-Gargan.) (Fonds P.T.T.)

les conversations plus secrètes de leurs dirigeants.

L'écoute en temps réel d'une ligne par un micro sucre :

Cette solution consiste à écouter et enregistrer les appels à distance en temps réel en intervenant qu'une seule fois pour toute sur la ligne. À un endroit de la liaison de l'abonné on branche un sucre émetteur, en faisant une épissure sur le câble, dans le boîtier de répartition, la prise de bureau ou le téléphone lui-même si on y a accès. Un professionnel évitera les deux dernières possibilités. Tout simplement parce que si la personne écoutée utilise un tuner FM, un scanner, des interférences pourraient trahir la présence du sucre. Si l'émetteur est raccordé à l'extérieur du bureau, de l'immeuble, il ne pourra pas être détecté. L'inconvénient majeur de ce type de système, c'est qu'en plus de l'espion, n'importe qui peut écouter la conversation jusqu'à 200 voire 500 m à condition que son récepteur radio soit réglé sur la bonne fréquence. L'espion disposant d'un récepteur radio intégrant un magnétophone peut enregistrer la conversation directement à distance sans craindre de se faire repérer. Si le subterfuge est découvert, il n'y a que le sucre qui sera localisé et détruit. Il existe un autre problème, ce petit gadget consomme du courant ne serait-ce que pour son fonctionnement, il pourra donc être éventuellement repéré par un spécialiste doté d'un analyseur de ligne ou d'un détecteur de microémetteur. La haute fréquence peut suivre le câble sur une certaine distance, assez courte, mais qui peut-être suffisante.

On trouve en vente libre sur Internet ce type de matériel. Une Société propose, par exemple, « Pack émetteur de conversations téléphoniques + récepteur. Ce pack complet prêt à l'emploi va vous permettre de mettre en surveillance une ligne téléphonique de la façon la plus simple possible. Branchez le MP114 dans la ligne analogique que vous voulez superviser puis à l'aide du récepteur, écoutez dans un rayon de plusieurs dizaines de mètres les conversations émises et reçues sur cette ligne. Idéal pour contrôler une ligne

téléphonique lors d'audit ou de formation de personnel (standardiste, etc. ...). « Transportez » par exemple vos conversations téléphoniques afin de pouvoir permettre à des collaborateurs de partager vos conversations lorsque vous le désirez. Par ailleurs, si vous ajoutez notre VR2 à ce pack, vous pouvez aussi enregistrer les conversations en toute simplicité même en votre absence et ainsi les analyser ultérieurement ! »

Raccordement sur une ligne analogique :

C'est la méthode la plus facile, mais aussi la moins discrète qui finira par l'arrestation du fraudeur s'il l'utilise en plus pour téléphoner gratuitement. Par contre dans le cas d'une écoute légale ou illégale cela peut durer plus longtemps. Elle est simple et peut être réalisée à peu de frais sur les lignes analogiques. Elle consiste à installer une bretelle en Y sur une ligne déjà existante. Il est en effet possible de se connecter sur tous les points d'un cheminement, de la sortie du central téléphonique au point final d'implantation du poste. Généralement, cette connexion est réalisée au niveau d'un sous-répartiteur ou d'un boîtier de répartition de quartier. Cette solution provoque généralement un défaut d'impédance et un affaiblissement sur la ligne. Un spécialiste équipé d'un matériel comme un analyseur de ligne analogique, peut détecter une anomalie.

La police, la gendarmerie, la DST découvrent dans les égouts, des épissures dans les câbles sur lesquels des bretelles sont réalisées. Les manchons raccordant deux câbles so ouverts, des bretelles, des straps mettant deux lignes en parallèle, des magnétophones ou émetteurs miniatures sont retrouvés à l'intérieur.

Dans les gaines techniques ou les cabines de brassage, on retrouve le même type de piratage. Il ne coûte que très peu. Le piratage s'effectue le plus souvent en faisant des épissures sur les câbles, cette solution est en effet plus discrète, qu'un raccordement au niveau du répartiteur général, ou sur la tête PTT, puisque les techniciens de France Télécom y interviennent à chaque fois qu'ils ont une ligne à rajouter. Sur cette partie de l'installation, le PDG d'une société ne peut pas faire grand-chose. Il n'y a que la police qui peut intervenir sur dépôt d'une plainte.

Il existe un autre moyen d'espionnage peu connu, qui peut être utilisé sur les postes analogiques.

Il peut permettre d'écouter en plus ce qui se passe dans un local, même si le téléphone est raccroché. La micro-pastille du combiné continue à capter des sons en permanence.

Cette pastille va donc générer des impulsions. Les électroniciens qui connaissent l'effet piézo-électrique du quartz, comprendront où je veux en venir. Avec un équipement sensible, il est parfaitement possible de faire de l'écoute avec certains postes. Ce type de technique est plutôt utilisé par les laboratoires des services secrets étrangers très en pointe dans le développement des nouvelles technologies d'espionnage. Ce moyen concerne plutôt les sites ou personnes ultra-sensibles.

Un fait historique d'écoute microphonique

Pour diriger le C.E. en Afrique du Nord, le S.R. a désigné le lieutenant-colonel Chrétien, qui, après un ultime stage à la villa « Eole », arrive à Alger en mars 1941. En Algérie, au Maroc, et en Tunisie, les Allemands et les Italiens ont envoyé des commissions dites « d'armistice » dont la mission officielle est de vérifier que les clauses du cessez-le-feu sont bien appliquées par les autorités civiles et militaires dépendant du gouvernement de Vichy. En réalité, ces commissions sont formées d'une majorité d'agents de l'Abwehr chargés d'organiser un réseau de renseignements et de recueillir des informations sur les agissements anglais et américains dans le Maghreb.

À Alger, le pouvoir officiel est détenu par le général Weygand qui, après un bref passage au Ministère de la Défense à Vichy, a été désigné comme Délégué général du gouvernement pour l'Afrique Française, fonction et titre créés spécialement pour lui. Investi de pouvoirs jamais atteints par un officier supérieur, son autorité s'exerce, tant sur le plan militaire que civil, sur toute l'Afrique du Nord et sur l'Afrique-Occidentale française. Les gouverneurs Noguès au Maroc, Esteva en Tunisie, Abrial en Algérie et Boisson en A.O.F. se trouvent placés sous ses ordres et il va veiller à ce que soient strictement appliquées toutes les décisions prises à Vichy. Dans certains cas, notamment dans la mise en place des mesures édictées contre les juifs, il ira même au-delà des décrets promulgués par le gouvernement Pétain. Adeptes farouches de la « Révolution nationale », il mène la lutte contre tous ceux qu'il nomme « les mauvais Français », anciens partisans du Front Populaire, francs-maçons, communistes, gaullistes, républicains convaincus, et il accorde tout son soutien à la « Légion française des Combattants », aux sections de « l'Ordre légionnaire », aux militants de Bucart, de Déat, et de Doriot, bref à tous ceux qui dansent sur le cadavre de la République. Son comportement en Afrique du Nord reflète donc parfaitement ses convictions. Weygand pense sincèrement qu'il faut à la France un ordre nouveau, duquel seraient bannies les institutions et les idées républicaines. Hostile à l'Angleterre, surtout depuis Mers el-Kébir, haineux vis-à-vis de De Gaulle qu'il qualifie de déserteur, méfiant à l'égard des Américains auxquels il reproche de n'être pas venus au secours de l'armée française, violemment anticomuniste, il ne s'en considère pas moins comme un ennemi irréductible de l'Allemagne. C'est en jouant sur cette dernière carte que le lieutenant-colonel Chrétien, et Paul Paillolle lui-même, obtiendront le feu vert pour leur service.

Déjà à Vichy, alors qu'il détenait le ministère de la Défense, Weygand avait donné son accord au colonel Rivet pour la création d'un S.R. et d'un C.E. clandestins, sous le couvert d'un service des Menées antinationales, chargé de « suivre » les agissements allemands et italiens, et ce, malgré l'opposition de la clique Laval-Marquet-Darlan. À cet égard, il avait fait connaître son opinion en déclarant à son interlocuteur : « la guerre continue, l'armistice n'est qu'une suspension d'armes ».

C'est en s'appuyant sur cette position nuancée que les T.R. parviendront à leurs fins, car il faut bien admettre que sans cet appui, Paillolle et ses camarades ne seraient jamais parvenus, malgré toute leur bonne volonté, à organiser et à structurer aussi rapidement leurs antennes clandestines.

Dès son implantation à Alger, le T.R. 119 s'est vite rendu compte du danger représenté par les commissions d'armistice italo-allemandes. Véritable vivier du renseignement, elles informent régulièrement l'O.V.R.A. et l'Abwehr sur le climat politique, ainsi que sur l'activité des milieux musulmans indépendantistes qu'elles entretiennent sournoisement. Mais elles s'acharnent surtout à tisser, avec leurs homologues du Maroc et de la Tunisie, un filet d'espionnage sur toute l'Afrique du Nord ; filet destiné à recueillir toutes indications utiles à leurs pays, et à enserrer dans ses mailles les agents des autres nations directement, ou indirectement, mêlées au conflit.

Le lieutenant-colonel Chrétien, dès son arrivée à Alger, s'est attaché à rechercher les moyens les plus efficaces pour contrer l'action de ces commissions. Installées dans plusieurs hôtels de la ville, l'hôtel d'Angleterre, l'hôtel Aletti, l'hôtel Albert, où elles ont regroupé leurs bureaux et appartements privés, elles travaillent officiellement avec leurs ambassades ou consulats respectifs. Évidemment, le T.R. est parvenu à s'assurer les services de quelques employés qui lui apportent de temps en temps des renseignements non négligeables, mais c'est loin d'être suffisant pour assurer une surveillance efficace. Chrétien et son adjoint, le commandant Le Capelain, voudraient percer à jour le jeu ennemi afin d'en prévenir les retombées. Naturellement, des tables d'écoutes ont été mises en place, mais elles ne s'affirment guère rentables, car les adversaires ne sont pas des novices. Ils savent très bien que leurs conversations téléphoniques doivent être interceptées. La preuve : un officier allemand téléphonant de l'hôtel Aletti à l'un de ses collègues de Casablanca sera entendu lui disant : « Je vous en prie, mon cher, parlez plus lentement afin que ces messieurs aient le temps de prendre en note notre conversation ! » Ce n'est donc pas par ce canal-là qu'il faut s'attendre à des révélations. L'idéal serait de pouvoir écouter les propos qui s'échangent dans l'intimité des pièces de travail ou d'habitation, lorsqu'Allemands et Italiens se croient entre eux, lorsqu'ils reçoivent leurs informateurs ou qu'ils évoquent leur activité. Il faudrait avoir une oreille dans chaque chambre, dans chaque bureau, mais comment ?

C'est alors que le commandant Le Capelain parla d'un réseau d'écoutes microphoniques permanentes !

C'est en juin 1941 que le Commandant Le Capelain songe pour la première fois à réaliser un dispositif qui permettrait d'enregistrer les conversations ennemies sur les lieux mêmes où elles doivent être, par définition, les plus confidentielles. Sans avoir des idées très précises sur les moyens, il pense que le réseau téléphonique peut offrir un champ d'investigations intéressant, et il sollicite le concours de son collègue, le commandant Guérin du bureau des Transmissions. Du point de vue technique, Guérin est évidemment bien placé pour juger des possibilités du projet, mais il ne dispose pas des éléments nécessaires à sa réalisation, pas plus qu'il ne possède de locaux ou de matériel pour effectuer l'étude. Mais, et cela va s'affirmer d'un grand intérêt pour le T.R. 119, il a noué d'excellentes relations avec le chef du service central des P.T.T. en Algérie : M.

Escande, haut fonctionnaire intègre et courageux dont le patriotisme ne fait aucun doute.

Guérin lui expose sans détour l'idée de Le Capelain, et les deux hommes réfléchissent ensemble à l'aspect pratique de ce plan. Ayant la haute main sur la totalité des systèmes de communication existant alors en Algérie, Escande se trouve remarquablement placé pour entreprendre, ou couvrir, toute action requérant les moyens techniques de son administration, mais il ne peut rien faire sans le concours de spécialistes éprouvés et discrets. Le projet qui lui est soumis demande en effet une étude très approfondie, et nécessite des recherches originales que seuls des ingénieurs des P.T.T. peuvent mener. Or il se trouve que trois de ces spécialistes ont été détachés par l'administration auprès du bureau des transmissions, et qu'ils travaillent donc dans cet ensemble technique qu'on appelle : le Central protégé.

Afin de rendre plus compréhensible le récit qui va suivre, il est bon d'en « planter le décor ».

Accrochée au flanc des collines du Sahel, au débouché de la plaine de la Mitidja, la ville d'Alger est construite en amphithéâtre. Ses immeubles et ses villas s'étagent sur les hauteurs qui dominent la baie jusqu'aux plateaux environnants. Dans le centre, la dénivellation contraint les ruelles et les voies à suivre une pente assez sensible ; c'est ainsi que la place du Forum, où se dresse l'imposant bâtiment du Gouvernement Général, s'étale à près de quarante mètres au-dessus du niveau de la rue d'Isly. La place Bugeaud, lieu de l'implantation des bureaux de l'État Major du 19 Corps, se situe à l'intersection des rues d'Isly et Généraux Morns, soit en contrebas d'une vingtaine de mètres par rapport à la rue Berthezène qui ceinture les immeubles de la Résidence. Accolé à l'un de ceux-ci un local de service communique, en fonction de cette dénivellation, par un escalier en puits, avec un tunnel qui débouche à l'intérieur même de la cour desservant les garages de l'État-Major. Dans ce souterrain, à l'abri de toute incursion et de tout bombardement, les transmissions ont établi leur central téléphonique, d'où son nom de « Central protégé ». On ne peut donc y accéder que, soit par l'enceinte militaire, soit par le puits partant des communs de la Résidence; deux lieux étroitement surveillés.

Les trois agents des P.T.T. qui assurent le bon fonctionnement de ce central et représentent leur administration dans la liaison avec l'équipement militaire sont, à cette époque M. La Maïda ingénieur, M. Pettenati ingénieur des travaux, et M. Rebaudingo contrôleur I.E.M. En raison de leur fonction et de leur mission, ce sont évidemment des hommes qui présentent toutes garanties de discrétion et de patriotisme ; la sélection de la sécurité des armées ne souffrant aucun doute à ce sujet. C'est donc tout naturellement vers eux que M. Escande se tourne pour envisager la réalisation du projet du commandant Le Capelain et, comme il le souhaitait, il recueille aussitôt leur adhésion. Quelques notes de service anodines leur laissent d'ailleurs bientôt les mains libres pour s'assurer du contrôle total des lignes qu'il s'agit de « métamorphoser ».

En 1941, l'espionnage microphonique fait un peu figure de science-fiction. Certes, les Américains sont déjà parvenus à capter des conversations en utilisant un système de micros clandestins reliés à un appareillage d'écoutes, mais au prix d'une installation réalisée par fils dissimulés. En Europe, et à fortiori, en Afrique du Nord, cette technique n'apparaît que futuriste. On ignore encore tout des moyens d'écoute qui se développeront d'une façon fulgurante après la guerre avec la transistorisation et la miniaturisation, puis grâce aux progrès importants de l'électronique. Seuls, quelques techniciens des communications et transmissions savent que l'on peut, en utilisant la liaison téléphonique, à l'aide de quelques astuces professionnelles, espionner les bruits d'une pièce, mais l'audibilité en est toujours médiocre à cause du phénomène de résonance. C'est malgré tout en partant de ce procédé que l'ingénieur La Maïda va établir un schéma parfait, avec le concours de ses collègues Henri Pettenati et Louis Rebauding plan général étant défini, chacun de ces hommes se met au travail pour monter une maquette d'essai, suivant sa spécialisation.

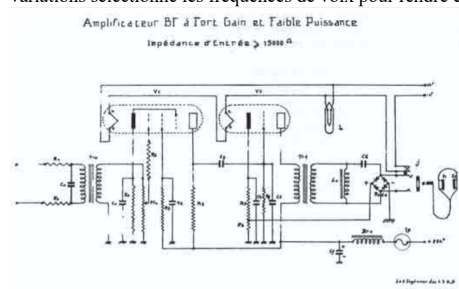
Le principe retenu paraît simple : tout poste téléphonique comporte un microphone normalement alimenté par une batterie située dans le central auquel il est rattaché. Le courant ne parvient dans ce microphone que lorsque l'appareil est décroché, c'est-à-dire en position de conversation. Le fait de raccrocher le combiné provoque le fonctionnement d'un interrupteur dont le rôle est de couper le courant ; le microphone n'étant plus alimenté, il devient sans effet. Or, si l'on établit une jonction métallique entre les deux lames de l'interrupteur, celui-ci se trouve neutralisé, et le courant continue d'arriver jusqu'au micro, même si le poste est en position « raccroché ». Dans ces conditions, le microphone reste opérationnel en permanence, et il transmet tous les bruits qui s'échangent dans la pièce où se trouve l'appareil. On voudra bien nous pardonner d'aborder ces problèmes techniques, mais ils sont nécessaires pour la compréhension des faits.

Cependant, une telle modification du circuit normal entraîne une répercussion sur le fonctionnement du central. En effet, un poste ainsi « trafiqué » provoque irrémédiablement un incident de ligne que les téléphonistes désignent sous le nom de « faux appel », et il risque fort d'éveiller l'attention d'un usager un peu méfiant, surpris par les interférences qui peuvent survenir en cours d'utilisation. Ce premier problème va pourtant être solutionné par l'ingénieur La Maida qui met au point un relais doté d'une bobine à 3 enroulements à flux différentiels, et conçoit une platine de retransmission qui rétablit le circuit initial malgré les modifications apportées au poste d'abonné.

Un premier essai effectué au petit laboratoire de la direction des L.S.G.D. (Lignes souterraines à grande distance) montre que ce système s'avère satisfaisant dès lors qu'un bâti métallique est adapté pour recevoir la platine. Puis, Louis Rebaudingo, au câblage, équipe un montage adéquat à cette nouvelle fonction, tandis qu'Henri Pettenati étudie un modèle d'amplificateur perfectionné. De la régularité et de la précision de cet appareil, dépend en effet la possibilité d'une écoute normale.

Une maquette originale essayée au répartiteur du central d'Isly montre que le bruit de fond des lignes en câbles urbains devient rapidement gênant, et qu'il faut, par conséquent, utiliser un courant microphonique aussi fort que possible. L'ennui d'un tel courant, c'est qu'il manque de « discrétion » et risque d'être facilement décelable par un appareil de mesure de sensibilité courante, mais tous les essais effectués avec un courant plus faible aboutissent à un résultat négatif pour l'intelligibilité de l'écoute. Il faut donc en prendre le risque. Pendant ce temps, le commandant Le Capelain est parvenu, grâce à M. Escande, à se procurer une « couverture » civile qui lui permet de se trouver au cœur de l'action ; sa nomination au poste d'Inspecteur des P.T.T. sous le nom de Paul Edmond l'autorise à se déplacer comme il l'entend dans les locaux administratifs. Son premier souci, dans cette nouvelle fonction, est de recenser soigneusement le nombre d'appareils devant faire l'objet d'une modification. C'est ainsi qu'il détermine qu'il y aura lieu de truquer 29 postes d'abonnés répartis entre l'hôtel d'Angleterre, l'hôtel Albert-Ier, l'hôtel Aletti, et la résidence de l'amiral Saiza à El-Biar.

À la mi-septembre 1941, la maquette définitive de l'ensemble est réalisée. Louis Rebaudingo a parfaitement maîtrisé le problème d'incorporation des platines de retransmissions montées sur des bâtis métalliques, et il a installé des machines d'appel spéciales. De son côté, Henri Pettenati, après bien des tâtonnements, est parvenu à mettre au point un amplificateur spécifique à deux étages, d'une impédance d'entrée supérieure à 15 000 ohms, comportant un dispositif antichocs placé aux bornes du casque de l'opérateur, qui permet d'éviter l'écho résonnant des chocs mécaniques auxquels pourrait être soumis le poste, et risquant de gêner la finesse de l'ouïe. De plus, un filtre à variations sélectionne les fréquences de voix pour rendre encore plus compréhensibles les conversations en écoute.



L'ensemble paraît au point et donne toute satisfaction aux essais. On passe alors immédiatement au stade de la réalisation. Deux collaborateurs de Louis Rebaudingo, MM. Mergny et Trotignon, mis dans le secret de l'opération, acceptent de prêter leur concours, et il va s'affirmer essentiel. C'est en effet Mergny qui se charge de procéder à la pose chez les intéressés des appareils truqués ou d'en effectuer le changement sous un prétexte quelconque. Trotignon lui, agent des installations intérieures, assure le montage en série des platines de relais des retransmetteurs sur lignes automatiques et vérifie leur réglage.

Un autre technicien du service, M. Legée, recruté par l'ingénieur La Maïda, construit, suivant les plans de ce dernier, le meuble d'écoute comportant dix positions plus une position de dirigeur. Dans le même temps, Henri Pettenati surveille attentivement la fabrication des sept amplificateurs imaginés par lui ; le personnel qui les réalise ignore leur destination. Quelques jours plus tard, par fragments, les tables et le meuble d'écoute sont transportés dans le tunnel du central protégé. L'ensemble est monté de telle façon que les tables peuvent être, à la moindre alerte, transformées en un système d'écoutes téléphoniques normal. Pièce par pièce, tous les éléments arrivent ; les connexions sont faites et les branchements préparés.

M. La Maïda pousse même le soin jusqu'à doter cette implantation clandestine d'un confort qui sera fort apprécié des opérateurs. Agents du T.R., ceux-ci sont sélectionnés par le commandant Le Capelain, alias Paul Edmond, qui les instruit de leur fonction. Se relayant par équipes de trois, ils doivent assurer leur travail vingt-quatre heures sur vingt-quatre. Au début du mois d'octobre 1941, Mergny et Rebaudingo commencent leur prospection. Des interférences ont été créées astucieusement sur les lignes à surveiller, et les abonnés allemands et italiens ne tardent pas à formuler des réclamations. C'est le moment qu'attendent les deux hommes pour agir. Se rendant sur place, ils s'empressent de changer là un appareil soi-disant défectueux pour le remplacer par un autre préalablement « équipé ». Ailleurs, ils démontent les postes et remplacent subrepticement la capsule microphonique par une autre. Sur la recommandation de Pettenati, soucieux d'obtenir les meilleures conditions d'audition pour ses amplis, ils agrandissent discrètement les trous percés dans les coiffes d'ébonite qui protègent le microphone. Pendant ce temps, au central protégé, on met la dernière main à l'équipement de l'appareillage. MM.

Escande et La Maida assistent aux ultimes essais, aux côtés du commandant Le Capelain et de ses opérateurs. Le 25 octobre, tout est prêt ; le plan « Écoutes microphoniques d'Alger » devient une réalité. Pour la première fois, dans l'histoire des services du Contre-Espionnage français, un réseau entier d'écoutes microphoniques fonctionne !

Dès les premières auditions, le commandant Le Capelain se rend compte qu'il dispose d'une source d'informations secrètes de première grandeur. Après l'émotion du début, liée aux craintes de voir le système rapidement découvert par les « abonnés », le ton des conversations interceptées montre à l'évidence que ni les Allemands ni les Italiens ne soupçonnent une indiscretion. Leurs propos reflètent une confiance totale dans l'inviolabilité des locaux qu'ils occupent. Sur le plan technique, les opérateurs souffrent de la volubilité des officiers de Mussolini dont les bavardages ininterrompus et l'élocution particulièrement rapide perturbent l'intelligibilité de l'écoute. Averti, Henri Pettenati va d'ailleurs concevoir un filtre spécial gommant un peu l'acuité des sons (*) et « sélectionnant », grâce à des caractéristiques différentes, les amplificateurs recueillant les voix italiennes aux sonorités plus aiguës que celles des Allemands à fond guttural.

(* Les travaux des spécialistes ont mis en évidence, après la guerre, que l'être humain possédait une « oreille géographique ». On sait maintenant qu'une oreille française a une courbe de sélectivité qui s'étend de 500 à 2 000 périodes, alors que celle d'un Anglais va de 2000 à 6000 périodes. Ni l'un ni l'autre ne perçoivent les sons de la même manière qu'un Japonais ou un Africain. On a créé d'ailleurs depuis une oreille électronique en s'inspirant de cette découverte. C'est ainsi que les travaux du Docteur Tomatis ont abouti à la réalisation d'appareils auditifs permettant à certaines formes de surdité de connaître une quasi-guérison.)

Chaque jour, et souvent deux fois dans la même journée, les informations captées sont triées, puis résumées en rapports condensés remis aux services du colonel Chrétien. Classés suivant leur origine et leur nature, ceux-ci sont ensuite répertoriés avant d'être acheminés vers leurs destinataires. Par ce canal clandestin, des renseignements d'importance vitale sur les agissements et les intentions des représentants de l'Axe parviennent aux Alliés, et, pour ce qui le concerne, à l'État-Major de l'Armée d'armistice. C'est ainsi que les visites de contrôles périodiques effectuées à l'improviste par les membres des commissions allemande et italienne dans les camps militaires seront toutes annoncées quelques heures, voire quelques jours, avant aux responsables d'unités ; ce qui leur permettra de dissimuler le matériel et l'armement dont les stocks sont supérieurs aux normes prévues.

À la mi-janvier 1942, les ingénieurs des P.T.T. ont terminé la première tranche du programme.

29 lignes sont sous contrôle-écoute :

21 lignes Mogador aboutissant à l'hôtel d'Angleterre

5 lignes Mogador aboutissant à l'hôtel Albert

3 lignes Mogador aboutissant à la résidence privée de l'Amiral Saiza.

Le système donnant entière satisfaction, le commandant Le Capelain demande alors qu'il soit étendu à l'hôtel Aletti et au Consulat d'Allemagne. Justement, les Allemands réclament de nouvelles lignes pour leurs bureaux consulaires en cours de réaménagements. Louis Rebaudingo, qui s'est rendu sur place pour reconnaître l'implantation des postes, gagne un peu de temps, malgré les récriminations de ses interlocuteurs, afin de laisser la possibilité à ses monteurs et câbleurs d'équiper les bâtis. Le 8 février 1942, accompagné de son fidèle Mergny, il procède à une première installation chez le Secrétaire Général du Consulat. Cette ligne, portant le n° 324.16, est mise en service dès le

lendemain. Le 18 février, soit neuf jours plus tard, une seconde ligne truquée : n° 331.51, posée dans le bureau même du consul, s'ajoute au faisceau des tables d'écoute. Deux jours après, M. Escande reçoit une demande pressante du Secrétariat consulaire qui exige l'installation d'un standard à plusieurs directions. Pris de court, le chef du service central des P.T.T. manœuvre habilement pour gagner quelques jours, le temps nécessaire à Louis Rebaudingo et Henri Pettenati pour fabriquer un nouveau matériel spécialement élaboré pour un standard. Une semaine ne s'est pas écoulée que les Allemands reviennent à la charge, déclarant avoir un besoin urgent de cet appareillage. Louis Rebaudingo répond qu'il attend l'arrivée d'un matériel convenable pour leur donner satisfaction. Pendant ce temps, une troisième ligne truquée, ayant le no 333.65, est dans le bureau de l'Ambassadeur Pfeiffer, avec un renvoi dans sa chambre à coucher, à la tête de son lit. Là, on peut dire que les opérateurs vont capter bien des... conversations qui n'auront aucun caractère politique, même si elles sacrifient au confidentiel.

Ne pouvant différer plus longtemps, Mergny et Rebaudingo, pourvus d'un combiné multiple modifié par leurs soins, installent chez les secrétaires du Consulat un tableau administratif 1 + 4 dont les lignes viennent se joindre à celles du meuble-écoutes. Ainsi, presque toutes les pièces de l'immeuble passent sous le contrôle auditif des opérateurs du Commandant Le Capelain.

Ce délicat et discret travail, qui fut mené à bien par les agents des P.T.T., ne s'effectua pourtant pas sans problèmes, car le Consulat allemand se trouvait dans une zone différente du secteur Alger-Isly, et il fallut passer les lignes en coupure sur le répartiteur du Central protégé et les raccorder sur l'autocommutateur de ce secteur.

Sans doute jaloux des aménagements obtenus par leurs collègues, les Italiens manifestèrent à leur tour le désir de voir leur Consulat doté des mêmes installations, et, sans se faire autrement prier, nos techniciens procédèrent à l'installation d'un circuit semblable au Consulat italien rue Charras. Le résultat devait s'affirmer particulièrement payant, puisque c'est par ce canal d'écoutes que les opérateurs apprirent le code secret des transmissions de la Marine italienne, lequel fut aussitôt fourni aux Britanniques. On conçoit aisément quels bénéfices ceux-ci purent en tirer !

La masse d'informations fournies par les écoutes microphoniques d'Alger fut considérable. Parmi tous les rapports qui parvenaient régulièrement au TR 119, certains influèrent d'une façon décisive sur le sort de la guerre. Mais c'est certainement en muselant l'activité des services d'espionnage italo-allemands en A.F.N., qui agissaient, rappelons-le, sous la couverture des commissions d'armistice, que le dispositif imaginé par Le Capelain et réalisé par les postiers d'Alger joua un rôle déterminant dans la lutte souterraine que se livraient l'Abwehr et le C.E. français.

Si les hommes de Paillote réussirent à neutraliser près de 400 agents de l'ennemi au cours de la période de fonctionnement des écoutes, ils le doivent avant tout à la remarquable équipe du Central protégé. La plupart de ces agents allemands ou italiens, dont l'arrivée était signalée aux responsables de l'organisation nazie par un code oral, rapidement découvert par les spécialistes du C.E., n'avaient pas plus tôt posé le pied sur la terre algérienne qu'ils étaient aussitôt interceptés. De la même façon, plusieurs traites furent démasqués. Ainsi un secrétaire des services français de la commission d'armistice dont les écoutes révélèrent les relations qu'il entretenait avec le commandant allemand Schmidt, officier chargé de la liaison entre les trois commissions, fut arrêté. Trouvé porteur de documents secrets signés par Weygand, il fut interrogé longuement et ne tarda pas à donner l'un de ses complices. Tous les deux furent passés par les armes. Une affaire extrêmement importante, qui aurait pu avoir de graves conséquences, fut également décelée par les écoutes. Un officier français, très lié avec un membre de ce groupe qu'on appela « le Comité des Cinq », avait pour maîtresse une fort jolie jeune femme brune à qui il ne cachait pas grand-chose de ses activités secrètes. Or, cette élégante personne au charme indéniable n'avait, de son côté, pas su résister à la virile prestance d'un lieutenant allemand qui lui soutirait habilement les renseignements qu'elle recueillait, sans trop y attacher d'importance il est vrai, auprès de son ami en titre. *Le Comité des Cinq : formé de MM. Lemaigre-Dubreuil, Jean Rigault, Jacques Tarbé de Saint-Hardouin, Henri d'Astier de la Vigerie, lieutenant-colonel Van Hecke, et Robert Murphy, consul général des États-Unis à Alger, complotaient pour mettre en place en Algérie, sous l'égide des Américains, un pouvoir placé sous les ordres du général Giraud.* C'est au cours d'une conversation captée dans l'un des salons de l'hôtel Albert-Ier que l'attention de l'opérateur fut attirée, car les propos échangés n'avaient plus rien d'un tendre duo. Le lendemain, le téléphone de la belle était mis sur écoute normale. Quinze jours plus tard, le C.E. possédait suffisamment d'éléments pour intervenir discrètement. On peut s'interroger sur les prolongements que cette affaire aurait pu avoir, notamment dans le cadre de l'opération « Torch » (*Débarquement allié en A.F.N.*), si le dispositif du Central protégé n'avait pas joué son rôle.

D'autres cas de trahison ou de compromission furent dévoilés par les écoutes, notamment celui d'un double jeu, subtil et compliqué, mené par un collaborateur de l'amiral Bonetti, membre apparemment zélé de l'O.V.R.A., qui devait finir par perdre brutalement la vie au cours de cette partie truquée qu'il avait engagée.

Certains rapports d'écoutes eurent des conséquences inattendues, tel celui qui révéla l'existence d'un cercle de jeux clandestin qui réunissait plusieurs fois par semaine des hommes d'affaires, mais aussi des officiers allemands, italiens, français et américains du service consulaire de Murphy ; tout ce beau monde fraternisant dans l'ambiance fiévreuse et enfumée d'un salon particulier ! Pour y mettre fin, le C.E. fit intervenir, sous le couvert d'une dénonciation anonyme, le commissaire de police Achiary. Grâce à cette source exceptionnelle, il put également être mis fin à un scandaleux trafic de tissus et de vaisselle, devenus introuvables en Algérie, dans lequel étaient compromis des fonctionnaires importants acquinés avec certains membres des commissions d'armistice. Mais c'est évidemment sur le plan politique et militaire que les informations recueillies au Central protégé s'affirmèrent les plus précieuses. Plus de 500 renseignements vitaux furent fournis par les écoutes microphoniques entre octobre 1941 et septembre 1942, dont, on l'a vu, le code des transmissions de la Marine italienne, et les lieux d'implantation des antennes de l'Abwehr en A.F.N. et en zone sud dans la métropole. Et c'est finalement l'importance de ces fuites qui alerta les services de l'Ausland-Abwehr à Berlin.

C'est à partir de juin 1942 qu'il devint évident aux responsables allemands de la section III C du Contre-espionnage que leur commission d'armistice d'Alger n'était plus sûre. Ils montrèrent donc une opération-test dans le but de vérifier leurs craintes. Leur représentant sur place, le capitaine Von Gagnern, paraissant au-dessus de tous soupçons, il leur fallait éprouver les autres membres de leur mission en poste dans la Ville Blanche. Ce contrôle, doublé d'une enquête individuelle serrée sur chacun d'eux, ne donna rien. La disparition, ou l'élimination par identification, des agents envoyés sur place et annoncés par le code habituel signifiait pourtant que leurs desseins étaient chaque fois percés à jour. Un conseil de spécialistes émit, après un minutieux examen des faits, l'hypothèse d'un espionnage par micros. Alerté par un câble codé, Von Gagnern fut prié de passer au peigne fin les locaux de travail et les appartements privés. Sa réponse, huit jours plus tard, désola les chefs de la III C, il n'avait rien trouvé. Curieusement, c'est presque par hasard que les Allemands furent aiguillés dans la bonne direction : un employé du chiffre apporta un beau matin une revue étrangère qui relatait la visite d'un ambassadeur soviétique à une personnalité politique d'un autre État, et l'article signalait le geste de ce diplomate qui, préalablement à l'entretien, couvrit l'appareil téléphonique de son manteau en disant : « On peut nous écouter par là ! »

Ce reportage banal fut une révélation pour les responsables allemands qui s'empressèrent d'enjoindre à Von Gagnern de « surveiller » ses postes téléphoniques. Dans un premier temps, celui-ci se contenta, afin de toujours pouvoir utiliser son appareil, de « coiffer » le microphone du combiné d'une calotte de caoutchouc qu'il retirait pour téléphoner. Au central protégé, les écoutes devinrent plus sourdes sur la ligne desservante, mais l'audition resta acceptable.

Cependant, décidés à tout mettre en œuvre pour juguler les fuites, les chefs de la branche III C de l'Abwehr finirent par se décider à envoyer à Alger une équipe de techniciens de la Siemens Halsk. Ayant transité par le Maroc, ceux-ci ne parvinrent sur place qu'au début du mois de septembre. Les opérateurs de Le Capelain furent parmi les premiers informés de cette visite : un secrétaire du consulat ayant cru bon d'en faire état dans une conversation banale avec deux de ses collègues. Il ne fallut bien évidemment que quelques heures aux ingénieurs allemands pour déceler l'anomalie présentée par les micros des appareils. Mais, fait extraordinaire, ils ne vérifièrent que les postes des bureaux et appartements de l'hôtel d'Angleterre, sans se préoccuper de ceux du consulat ! Cette attitude laisse supposer qu'ils accordaient toute confiance au personnel qui se portait lui-même garant de l'inviolabilité du lieu, et qu'ils ne soupçonnaient pas les agents des P.T.T. (Mergny et Rebaudingo) qui avaient procédé à l'installation et en assuraient l'entretien. Quoi qu'il en soit, pressés semble-t-il d'aller poursuivre leur tâche en Tunisie, ils ne menèrent pas plus loin leurs investigations.

Pour Von Gagnern, soulagé par l'éclaircissement du mystère des fuites, restait à déterminer à qui cet espionnage subtil profitait et, partant de là, quels en étaient les auteurs. Cependant, pour mener à bien son enquête, son champ d'action était réduit. Ne disposant pas, ou de très peu, d'informateurs locaux — on a vu que presque tous les agents envoyés furent interceptés, grâce aux écoutes, par les hommes de Paillote —, contraint de cantonner ses agissements dans le cadre étroit de ses attributions officielles qui devaient respecter l'apparente souveraineté du gouvernement de Vichy, il dut en passer par la voie diplomatique et adresser à son interlocuteur patenté — la commission française d'armistice — une réclamation en bonne et due forme. Celle-ci parvint au général Merlin qui désigna aussitôt le capitaine Flambard, des Transmissions, pour le représenter. On ne pouvait faire meilleur choix, puisque ce dernier, en tant qu'adjoint du commandant Guérin, qui, comme on l'a vu plus haut, dirigeait ce service, était parfaitement au courant du dispositif d'écoutes !

Le 28 septembre 1942, sur l'initiative de la commission d'armistice italo-allemande, une réunion se tient à l'hôtel d'Angleterre. Sont présents : d'une part, l'Amiral Saiza, le capitaine Von Gagnern, et le lieutenant de vaisseau Forési ; de l'autre : le capitaine Flambard, le capitaine interprète Lucioni, et pour représenter l'administration des P.T.T. : MM. La Maïda et Pettenati.

D'entrée, Von Gagnern se plaint d'être victime d'un « espionnage auditif » affectant les locaux à usage de bureaux, ainsi que certains appartements privés. L'Amiral Saiza, pour les Italiens, formule la même réclamation. Tous les deux insistent sur le fait que ces « indiscretions » sont dues à des appareils téléphoniques truqués qui permettent d'enregistrer les conversations même lorsque les combinés sont raccrochés.

Bien entendu, Flambard montre son étonnement, et déclare hautement que si ces faits sont confirmés ils ne peuvent être imputés à la commission d'armistice française, ce qui est effectivement vrai. Interrogés par l'officier des Transmissions, La Maïda et Pettenati se montrent catégoriques : une telle modification intervenant sur les postes aurait provoqué de graves incidents de fonctionnement sur les lignes et se serait répétée au Central de la rue d'Isly. Ils proposent à leurs interlocuteurs de vérifier eux-mêmes les installations. À ce moment, le lieutenant de Vaisseau Forési sort de sa serviette un schéma de câblage relatif à l'un des appareils en service dans son bureau et il en démontre l'anomalie. Henri Pettenati l'examine attentivement et fait répondre par l'interprète

— « Il est évident que le schéma tel qu'il est présenté ici comporte une irrégularité. S'il a été relevé sans erreur, il ne fait aucun doute que le câblage du poste observé n'est pas correct. »

Monsieur La Maïda ajoute de son côté « qu'en fonction du manque de personnel qualifié, les femmes actuellement affectées au montage des postes en service ont pu commettre certaines erreurs ». Il propose donc que les appareils douteux soient remplacés, et renvoyés aux ateliers pour examen approfondi. Puis il indique, après avoir brièvement exposé

les principes de fonctionnement, quelles sont les tensions utilisées. Le lieutenant de Vaisseau Forési reconnaît que ces valeurs sont bien conformes à celles mesurées par les techniciens de la Siemens Halsk, mais, tout en prétendant ne pas y connaître grand-chose, il s'étonne que les micros modifiés n'aient pas provoqué d'incidents sur les appels en batterie centrale ou automatique ! Henri Pettenati répond qu'« il ne comprend vraiment pas non plus, ce cas ne s'étant jamais présenté à sa connaissance et qu'il serait plutôt porté à douter de l'exactitude du schéma relevé ».

Après une courte discussion, il est alors convenu que des essais devront être effectués au plus tôt avec un haut-parleur pour constater la possibilité d'écoute de chacun des appareils en service à l'hôtel d'Angleterre, à l'hôtel Albert-Ier, à la villa-résidence de l'Amiral Saiza et au Consulat italien de la rue Charras.

On note qu'il n'est pas question de l'hôtel Aletti, ni du Consulat allemand ; ce qui prouve bien que pour ce dernier Von Gagnon n'imagine même pas qu'il ait pu être espionné. On retrouve là une forme d'aveuglement souvent manifestée par les Allemands pour ce qui appartient exclusivement à leur domaine. Ils conçoivent bien que de tels faits se produisent dans un lieu échappant à leur contrôle, mais se refusent à les admettre comme possible dans les sphères placées en totalité sous leur autorité.

Le capitaine Flambard établit alors le procès-verbal de la réunion, et les participants se séparent après avoir pris date pour une nouvelle séance au cours de laquelle il sera procédé aux essais de tous les postes.

Pendant que ce premier colloque de l'enquête se déroulait à l'hôtel d'Angleterre, M. Escande prenait ses dispositions, sur instructions du commandant Le Capelain qui craignait une visite des Commissions d'Armistice au Central protégé, pour effacer toutes traces du dispositif. L'après-midi même, et toute la nuit, une équipe placée sous les ordres de l'ingénieur Lacroze s'empresse de démonter les installations.

Celles-ci furent remises en place dans un local désaffecté situé rue Généraux Morris, donc en un lieu pas très éloigné du Central protégé. Ce déménagement, réalisé en si peu de temps, fut un véritable tour de force.

Le 29 septembre au matin, rien ne subsistait de l'appareillage qui avait si bien fonctionné pendant de longs mois, mais il pouvait redevenir rapidement opérationnel si besoin était. Par prudence, Le Capelain ne le remit pas en service, alors qu'il était toujours possible d'intercepter les conversations du Consulat allemand.

Deux jours après, les mêmes protagonistes se retrouvent à l'hôtel d'Angleterre. Les premiers essais commencent, effectués par Mergny, requis comme exécutant, et en présence bien entendu des officiers de chaque commission. Suivant les instructions qui lui ont été données préalablement par Henri Pettenati, Mergny utilise les amplificateurs de telle façon qu'un effet de couplage Larsen provoque un hurlement intense démontrant évidemment l'anomalie du poste examiné, mais interdisant également d'entendre la moindre parole intelligible. Pettenati le fait constater à ses interlocuteurs assez surpris, et, sans insister davantage, enjoint à son compère de remplacer l'appareil défectueux. La même scène va se répéter dans plusieurs pièces ; tant et si bien qu'au onzième contrôle la surveillance hostile et méfiante du début se relâche. Ces messieurs préfèrent rester dans l'un des salons où, enfouis dans de profonds fauteuils, ils savourent leurs cigares tout en évoquant le déroulement des opérations sur le front de l'Est ; seul un sous-officier appelé en renfort suit le travail des postiers. Cette négligence va permettre à Mergny, tandis que Pettenati détourne l'attention de l'Allemand, de démonter plusieurs postes sans les avoir essayés, et ainsi il ne pourra plus être prouvé que tous les appareils étaient truqués ! L'ingénieur des P.T.T. feindra de déplorer la hâte de son subordonné, mais elle n'entraînera aucune réaction du sous-officier du Reich qui signera sans objections le procès-verbal établi à la fin de la journée.

Cependant, Von Gagnon va veiller par la suite, au cours des autres séances d'essais, à ce que tous les postes soient contrôlés. Quelques controverses surgiront d'ailleurs au moment de la signature du rapport contradictoire final ; Allemands et Italiens voulant qu'il soit précisé que tous les appareils ont été vérifiés, ce que refuse Henri Pettenati soutenu par Flambard. Finalement, après de longues discussions, les deux parties demeurent sur leurs positions, laissant aux Commissions italo-allemande et française le soin de rédiger un texte d'accord. Traité par correspondance officielle et retardée par les Français qui firent traîner l'affaire, la signature définitive n'eut jamais lieu car le 8 novembre 1942 l'opération « Torch » commençait. Les Alliés prenaient pied en A.F.N. Quelques jours plus tard, l'Algérie rentrait dans le camp de la liberté.

De l'avis même des plus hauts responsables des services secrets français et alliés, les écoutes microphoniques d'Alger jouèrent un rôle déterminant dans la guerre du renseignement. Les Allemands eux-mêmes, et Canaris le premier, admirent que l'organisation mise en place par Chrétien et Le Capelain, sous les ordres de Paillolle, leur porta un grave préjudice. Ils reconnurent s'être grossièrement trompés en mésestimant les capacités du S.R. français et principalement celles de ses antennes T.R. en A.F.N.

Lorsque les écoutes furent découvertes, ils en imputèrent la réalisation aux Alliés, et principalement à l'I.S. C'est pourquoi leurs représentants à Alger ne s'intéressèrent guère, en tout cas pas en profondeur, aux agissements des postiers, pourtant les plus aptes à monter une telle opération. Cette erreur d'appréciation coûta fort cher aux forces de l'Axe au moment du débarquement anglo-américain sur les côtes marocaines et oranaises, de même qu'elle leur fut fort préjudiciable dans la bataille souterraine des S.R., car leurs ennemis détenaient, grâce aux écoutes, bien des renseignements qui, se juxtaposant, allaient démanteler en partie une organisation patiemment mise en place depuis des années. Il serait faux de dire que cette erreur de l'Abwehr fut la cause de la disgrâce de Canaris, mais il serait pareillement inexact de prétendre qu'elle n'y contribua pas.

Ce qu'il faut retenir de cette affaire, très peu connue, des écoutes microphoniques d'Alger, c'est le rôle essentiel, déterminant, joué par une poignée d'hommes, par une équipe de postiers, qui n'hésitèrent pas à s'engager dans une partie difficile et dangereuse dont les conséquences étaient imprévisibles. Dans l'atmosphère pétainiste qui régnait en 1941-42 en Algérie, alors que la puissance de l'Axe se manifestait partout, il fallait placer bien haut le sens du patriotisme et de l'honneur pour affronter les risques d'une activité clandestine en faveur des Alliés et de la France libre. Le travail accompli par les techniciens des P.T.T. d'Alger, travail obscur, délicat et ingrat qui réclamait non seulement du courage, mais aussi un formidable effort de recherche et d'imagination, appartient indiscutablement à l'histoire de la lutte clandestine et s'inscrit en bonne place dans l'épopée de la Résistance. Pourtant, aucun de ceux qui l'assurèrent n'a obtenu la plus petite médaille de reconnaissance. Seules, quelques lettres de félicitations de chefs d'État-Major témoignent de la valeur d'un comportement discret certes, mais particulièrement efficace.

Les liaisons numériques et analogiques :

Dans le cas d'une société avec un raccordement numérique en RNIS sur son PABX, il ne sera pas possible de se raccorder sur la liaison venant du central public, avec des moyens aussi faibles que précédemment. Si un particulier a demandé une ligne RNIS, une interface S0, là aussi, il n'y a qu'un électronicien performant qui pourra intercepter la communication. Un piratage de ce type nécessite des équipements d'un coût très dissuasif. Pour les grosses sociétés, la partie sensible se situe donc entre la PABX et la prise murale à la condition que l'abonné utilise un poste analogique. Le piratage ne pourra être réalisé qu'à l'intérieur de la société ou de l'immeuble. On retrouvera donc la solution des sucres, des bretelles, ou des magnétophones dissimulés dans des gaines ou cabines techniques avec les mêmes inconvénients que précédemment. Cette possibilité, bien que délicate, reste à la portée des personnes pouvant rentrer régulièrement dans un immeuble, dans le cas d'un enregistreur. Pour ce qui est du sucre, il suffit d'y entrer une seule fois pour toutes et de l'installer. Ce genre d'opération est réalisée dans un faux plafond, une gaine technique, ou un endroit discret, ne subissant jamais la moindre visite technique. Les méthodes de détection, sont les mêmes que précédemment, détection d'une haute fréquence résiduelle, d'un défaut d'impédance, d'un affaiblissement anormal sur la ligne. Pour contrer ces procédés, le responsable des installations techniques doit veiller à ce que les gaines et les salles soient fermées à clef. Les chemins de câbles doivent être propres et ne comporter que les câbles de communication, d'un même type si possible, afin de permettre le repérage d'un nouveau câble, qui ne serait pas destiné à une utilisation normale des systèmes de la société. Il ne doit y avoir aucune épissure sur l'un d'eux. C'est toujours à l'endroit des boîtes de jonctions, que les risques existent.

L'affaire du Canard Enchaîné

Le 3 décembre 1973 au soir, un dessinateur et administrateur du journal passe devant le futur siège du Canard Enchaîné, au 173 rue St Honoré. Il aperçoit de la lumière et décide d'aller voir quel journaliste fait du zèle dans cet immeuble pas encore fini, à cette heure tardive.

Il surprend alors plusieurs hommes occupés à « sonoriser » les futurs locaux du journal. Ces derniers s'empressent de prendre la fuite, mais le mal est fait.

Le Canard va alors mettre à jour l'opération Palmes, commanditée par la DST. Le journal va publier comme à son habitude un certain nombre de détails croustillants (nom de la division de la DST, nom de la section technique qui s'est chargée des écoutes, noms et prénoms des commissaires et inspecteurs chargés de cette opération).

Le procès qui a suivi cette affaire mériterait à lui seul un livre :

Le Canard dépose une plainte pour « atteinte à la vie privée » et « violation de domicile ».

— Fin décembre 1976, le juge d'instruction déclare un « non-lieu » ... Ils n'ont tout d'abord pas retrouvé les auteurs de l'effraction. De plus, le bureau étant alors inoccupé il n'y avait pas à proprement parler de « domicile » et les conversations qui auraient pu s'y tenir ne pouvaient être que « professionnelles et non privées » (sic).

— Le Canard fait appel de cette décision, mais, en juillet 1977, la Cour d'Appel confirme le premier jugement.

— Le Canard se pourvoit alors en Cassation. La Cour de Cassation casse alors l'arrêt de la cour d'Appel pour un vice de forme dans le dossier.

— Le dossier est donc renvoyé devant la Cour d'Appel d'Amiens, qui estime qu'il y a prescription sur les faits.

Un ultime pourvoi en Cassation viendra clore ce dossier brûlant en février 1980.

On ne peut s'empêcher de se poser des questions sur l'indépendance des magistrats de l'époque ...

Les écoutes étaient vraisemblablement l'œuvre de la DST, qui en avait marre de ce palmipède qui semblait avoir des informateurs dans les plus hautes sphères de l'État. Mais une fois de plus, il semble que le pouvoir en place ait réussi à étouffer plus ou moins bien cette affaire.

Depuis cet épisode, l'administration du Canard enchaîné a laissé une plaque commémorative dans ses locaux à l'endroit où les agents avaient percé un mur pour y installer leurs équipements. Elle serait même devenue lieu touristique...

L'affaire des « plombiers » ou Watergaffe (comme on l'avait surnommée à l'époque), par son retentissement, a indirectement conduit le Premier ministre, Pierre Messmer et le président de la République, Georges Pompidou, deux mois et demi après les faits, à permuter les ministres de l'Intérieur et de l'Agriculture lors de la formation du troisième gouvernement de Pierre Messmer, le 1er mars 1974 : Raymond Marcellin, jusque-là ministre de l'Intérieur et ayant la tutelle de la DST, a ainsi échangé son poste avec celui de Jacques Chirac, ministre de l'Agriculture et du Développement rural. L'arrivée de Jacques Chirac au ministère de l'Intérieur a eu un effet non négligeable dans la campagne

pour l'élection à la présidence de la République du successeur de Georges Pompidou, décédé le 2 avril 1974, l'affaire des plombiers devenant ainsi, parmi d'autres, l'un des éléments qui ont contribué à la victoire de Valéry Giscard d'Estaing lors de l'élection présidentielle de 1974.

Liaison numérique / numérique :

Dans le cas d'une liaison numérique de bout en bout, le piratage à peu de frais devient impossible si à la place d'un poste analogique on installe un poste numérique. Chaque constructeur de PABX dispose de sa propre signalisation pour alimenter ses postes téléphoniques numériques. Ils ne sont donc pas interchangeables. Un professionnel des écoutes sera contraint de réaliser un adaptateur spécifique s'il veut écouter à distance un poste numérique. La solution la moins coûteuse et la moins compliquée techniquement consiste par exemple à remplacer le combiné d'origine du poste numérique du constructeur par un autre combiné qui lui, aura été trafiqué à l'avance en y incorporant un sucre émetteur. Nous allons donc retrouver les mêmes inconvénients que cité plus haut.

Si l'accès est impossible au poste souhaité, il ne reste plus qu'une connexion pirate sur la ligne RNIS en amont du TNL qui contient les MIC du PABX. On ne peut croire à cette solution pour diverses raisons. En plus d'être coûteuse, plusieurs centaines de milliers de francs, ce type de matériel nécessaire est peu discret et nécessite un emplacement sûr pour son camouflage et à l'abri des intempéries. Il est aussi nécessaire de disposer de très bonnes connaissances techniques. Dans ce cas, ce matériel est immédiatement repéré. Je ne vois pas de professionnels des écoutes illégales installer un matériel aussi volumineux et coûteux dans les souterrains ou une cabine de sous-répartition.

L'équipement en plus doit être de qualité et raccordé en très haute impédance. Toutes dégradations de ligne entraînent des erreurs qui seraient immédiatement détectées par le central et même l'utilisateur. Des appareils comme les analyseurs dont le bas de gamme commence à 40 000 F ne permettent d'écouter qu'un seul IT (canal), alors qu'un MIC en comporte 30. En plus, un abonné derrière un PABX n'utilise jamais le même IT, il faut donc enregistrer les 30. En clair, même en 95, un équipement sophistiqué avec enregistrement des 30 canaux ne pouvait pas coûter moins de 200 KF et encore en faisant preuve d'ingéniosité. Aujourd'hui, même si on sait se connecter sur la liaison à peu de frais, il reste toute la partie traitement à réaliser derrière, pour sélectionner et écouter les conversations nécessaires. Avec un autre surcoût, on peut prendre un analyseur de protocole de l'IT16 de signalisation, qui permet d'enregistrer l'abonné après détection de son numéro sur n'importe quel IT. Il faut en plus être certain qu'il utilise toujours le même poste. Il faut donc être un bon ingénieur, compter de 30 à 50 KF, et développer son propre logiciel pour faire une interception efficace sur un MIC T2.

On ne peut donc croire à ce type d'écoutes illégales sur les installations des grosses sociétés. Même une liaison pour une écoute légale ou illégale réalisée par un service officiel sur un MIC, peut entraîner des perturbations. Pour les gros sites dépassant les 4 MIC, il est possible de demander un raccordement sur un ROF s'il y en a un de disponible dans le quartier. Il s'agit d'un raccordement en fibre optique. Les spécialistes comprendront ici qu'il n'est plus question de faire un branchement pirate avec une épissure dans ce type câble, car c'est impossible. Avec une solution en ROF, une écoute ne peut s'effectuer qu'au niveau du central (CPE).

Écoutes téléphoniques sauvages par les fonctions soft

Ces méthodes sont encore plus vicieuses, car non détectables.

Écoute par la fonction de décroché automatique :

C'est une autre méthode moins connue, qui peut permettre de faire des écoutes illégales à l'intérieur d'un local en toute discrétion, en intervenant par le biais d'une programmation. Il n'y a aucune intervention physique comme le câblage d'une bretelle sur une ligne. Cette fonction est inutilisable avec des postes téléphoniques simples sur tous les types de PABX. Par contre, on peut programmer cette fonction sur certains calculateurs, pour que des postes numériques décrochent automatiquement et se mettent en mode mains libres tout seul, au bout d'un nombre de sonneries défini. Ce moyen est dangereux, car il permet une écoute insidieuse à l'intérieur d'un bureau. Il est possible d'affecter un autre numéro de ligne sur une touche de fonction inutilisée d'un poste numérique. Cette méthode a l'avantage de permettre à la ligne de l'utilisateur de rester disponible pour ses appels extérieurs et il ne peut donc détecter la supercherie. Il n'est pas impossible que des pirates, des officines non autorisées, ou même des services de renseignements étrangers, tentent ou utilisent cette fonction à l'insu des utilisateurs. Il ne faut pas oublier que des systèmes téléphoniques complexes ont une origine étrangère. On ne peut connaître la totalité de toutes les fonctions disponibles même pour les meilleurs techniciens. Pour cela, il faut des ingénieurs systèmes capables d'éplucher les programmes des calculateurs. Plus les systèmes sont complexes, plus ils sont dangereux, car moins facile à maîtriser. Seule une quantité limitée d'ingénieurs des constructeurs respectifs connaissent la totalité des fonctions disponibles, pour avoir participé à la réalisation des programmes. Rien ne peut garantir à un utilisateur que ce type de fonction n'existe pas sur les postes numériques RNIS, ou qu'un jour, un pirate, un service de renseignement étranger trouvera une parade pour déclencher le poste et espionner en toute impunité sur n'importe quel type de système. D'où la nécessité de système d'observation de trafic pour les appels entrant sur une société. La taxation dans ce cas précis ne sert à rien puisque les appels entrants ne sont pas facturés, puisque cela ne se réalise que sur des appels sortants. Il faudrait être inconscient pour affirmer à 100 %, que ce moyen n'existe pas sur les systèmes présents sur le marché. Cette fonction peut autoriser l'écoute des conversations des syndicalistes, s'ils sont dans une salle réunion dotée d'un poste numérique.

Écoute téléphonique par la fonction conférence :

La fonction conférence permet normalement à plus de deux interlocuteurs de dialoguer sur une même ligne. L'appelant compose les numéros de ses (x)correspondants et appuie sur la touche conférence afin de permettre le dialogue dans tous les sens à travers le téléphone, donc le PABX de son site.

Un technicien de bon niveau par diverses astuces peut déclencher cette fonction sur certains PABX afin de réorienter la communication entre deux interlocuteurs ou plus, vers une autre ligne afin de réaliser une écoute ou un enregistrement pirate. Ce moyen est possible sur les postes numériques, mais aussi analogiques, et à condition que le PABX dispose d'assez de cartes électroniques dotées de circuits conférence. Sur certains PABX, le calculateur est capable de faire appel aux circuits conférence disponibles dans tous les châssis, si le châssis du poste demandeur n'a plus de circuit disponible. Un utilisateur ne peut donc découvrir l'anomalie. Par contre, d'autres systèmes imposent la limite de 2 ou 5 correspondants par (x)demandeurs dans un châssis. Dans ce cas, lors d'essais en faisant plusieurs appels simultanés, il est possible de découvrir la supercherie.

Ce moyen peut se repérer assez vite par l'exploitant de l'installation contrairement au cas précédent.

Si la conversation est réémise simultanément sur une deuxième ligne parallèlement à celle du demandeur, nous aurons une double trace sur le système de taxation téléphonique, avec une date et une heure d'appel identique à chaque fois sur deux lignes différentes. Ce procédé peut cependant passer inaperçu, si l'auteur a pris la précaution d'intervenir sur le filtrage des tickets de taxation du PABX, ou sur le système externe de taxation téléphonique. Il est rare que l'on arrive un tel point de sophistication dans le piratage soft. Il est en effet plus facile de mettre une bretelle. Il est aussi possible de réorienter l'appel par ce biais vers un enregistreur magnétique, raccordé sur une ligne analogique interne à la salle PABX. Là, nous sommes dans le cas où le PDG de la société fait écouter et enregistrer les communications de ses salariés.

Il faut savoir que très souvent, les communications des salles de marchés des grandes banques ou bourses, sont enregistrées afin de limiter ou d'empêcher les malversations.

Écoute par la fonction double appel :

La fonction double appel, connue par les utilisateurs sous la touche R2, permet aussi de réaliser des écoutes illégales. Dans la réalité tout dépend des fonctions disponibles dans les logiciels des calculateurs des PABX, et même des bugs logiciels inconnus de leurs concepteurs, qui peuvent permettre, par l'addition d'astuces successives, de faire une écoute illégale, par le biais d'une programmation pirate par la voie de la télémaintenance. Le principe est en effet le même que précédemment, mais inverse. Au lieu d'avoir un appelant qui appelle sur deux lignes deux correspondants extérieurs, nous avons ici deux personnes extérieures qui vous appellent l'une après l'autre. Il y a donc deux lignes au niveau du central, si l'une a été programmée pour permettre une écoute illégale, vous ne pourrez jamais prendre le deuxième interlocuteur.

Écoute par fonction priorité d'appels vers l'extérieur :

Un procédé permet de rendre un poste prioritaire comme celui des exploitants techniques ou des directeurs par exemple, pour appeler l'extérieur, lorsque toutes les lignes réseau sont occupées. Il suffit pour cela de déclarer les postes concernées en prioritaires. Ils prendront automatiquement une ligne extérieure, et couperont les communications en cours des postes non prioritaires.

Cependant, ce procédé présente un risque. Il permet aussi d'écouter une communication en cours à l'insu des deux interlocuteurs. Cette fonction n'est pas à installer par exemple dans un immeuble qui utilise le même PABX pour plusieurs sociétés. Cet inconvénient peut provenir d'un bug logiciel, mais peut être aussi volontaire pour prévenir les personnes en communication, qu'on va les couper pour récupérer leur ligne. Cette fonction se retrouve le plus souvent sur le poste opérateur de la standardiste ou des exploitants, afin qu'ils puissent appeler l'extérieur en cas d'urgence, effondrement d'un réseau pour cause de surcharge, incendie, panne électrique, etc. C'est ce qui permet aussi à certaines standardistes d'écouter les conversations internes des salariés, des cadres de direction et PDG.

Affaires contemporaines d'écoutes téléphoniques :

Un roman-feuilleton policier à l'américaine l'affaire du **Watergate** est le plus grave scandale politique qu'aient jamais connu les États-Unis.

Il contraignit le président en place à démissionner, et modifia pour longtemps les rapports d'influence entre le président et le Congrès, tout comme le prestige attaché à l'institution. Jamais une affaire policière n'avait eu de telles répercussions à l'échelle de la politique intérieure. Et pourtant, tout avait commencé comme une « tentative de cambriolage de troisième ordre » (selon un porte-parole de la Maison Blanche)...

En effet, le 17 juin 1972, à une heure du matin, le gardien de l'immeuble du siège du Parti démocrate, le Watergate, fait sa ronde de nuit. Il remarque que deux portes, qu'il avait pris soin de fermer quelques temps auparavant, ont été forcées. La police, discrètement alertée, saisit cinq hommes en flagrant délit dans les locaux du parti. Une banale

arrestation.

Banale ? Pas si sûr. À y regarder de plus près, ces cinq cambrioleurs ne ressemblent guère à des cambrioleurs ordinaires. On trouve sur eux de l'argent liquide leur appartenant, un impressionnant arsenal de matériel électronique d'écoute et d'espionnage, qui les fait plus ressembler à des agents secrets qu'à des voleurs.

Tout de suite se pose la question : d'où cet argent vient-il ? Flairant le scoop, deux journalistes du Washington Post, Carl Bernstein et Bob Woodward, vont mener tambour battant une enquête qui va très rapidement les amener jusqu'au CRP (Comité pour la Réélection du Président), et, par delà cet organisme écran, le proche entourage de De son côté, l'enquête judiciaire met rapidement en lumière le rôle occulte joué par la CIA, ainsi que ses collusions avec le CRP. C'est alors que les têtes commencent à tomber. Un homme de main, Hunt, puis le président du CRP, parti « s'occuper de sa famille ». Mais bien d'autres questions restent sans réponse. La plus importante d'abord, pourquoi les cinq hommes se sont-ils introduits dans le quartier général du Parti démocrate ? Pour poser des micros, semble-t-il, mais au profit de qui ? Pour voler des documents, peut-être, mais lesquels ? Ah ! si du moins l'on connaissait le nom du responsable de l'opération, de celui qui a donné le feu vert...

De son côté, le 22 juin, le président Nixon a fait une déclaration publique : « La Maison Blanche n'a aucune part dans cet incident précis ». Et l'intérêt pour l'affaire s'affaiblit lentement. Rien de sensationnel à annoncer ou à lire dans ce magouillage politique. Un relenti qui se dégage de la vie politique, rien de plus. Mais le Washington Post, influent bien informé, empêche que le scandale soit étouffé. Il révèle que des sommes colossales ont été blanchies par le CRP pour soutenir tout un tas d'actions à la légalité plus que douteuse.

Le Watergate, c'est déjà en 1972 un scandale qui souligne le financement parfois illégal de la campagne électorale des républicains.

Cependant, l'élection présidentielle est un véritable triomphe pour Nixon. Il en conclut que sa victoire vient de balayer le dernier souffle du scandale et les dernières semaines de 1972 lui donnent raison.

Le réveil de 1973 n'en est que plus brutal.

C'est le 8 janvier que s'ouvre le procès des cinq « plombiers » du Watergate, plus deux de leurs commanditaires. L'un d'eux, McCord, cède sous la pression et les activités illicites du CRP apparaissent au grand jour. Le juge Sirica reporte la sentence de McCord en espérant que les choses vont se calmer et les langues se délier, mais voilà que le Congrès s'en mêle. En janvier, le chef de la majorité démocrate confié au sénateur Sam Erwin la présidence d'une commission spéciale d'enquête sur la campagne présidentielle. Mais avant même le début de ses travaux, le bruit du scandale commence à remonter jusqu'aux proches du président. De rebondissement en rebondissement, le Watergate se présente comme la révélation de pratiques gouvernementales qui, en utilisant l'abus de pouvoir, ne visent ni plus ni moins qu'à saper les fondements du régime démocratique.

C'est l'heure du grand chambardement. Nixon décide enfin d'agir. Le 30 avril, il prononce une allocution télévisée pour faire savoir que ses plus proches collaborateurs, Dean, Ehrlichman et Haldeman démissionnent. Ceci a pour effet de leur coller l'étiquette de coupable sur le dos. S'ils sont responsables, il est innocent. Le reste n'est que manipulation de l'opinion. Mais ce sacrifice reste vain.

Car, de son côté, la commission Erwin va de surprise en surprise. Son rôle est déterminant, mais il faut en saisir les limites. Le Congrès peut créer, à sa guise, des commissions d'enquête, les doter de crédits de fonctionnement et les transformer ou non en commissions permanentes. Il arrive qu'elles reçoivent le droit de subpoena, le droit de réquisition judiciaire qui les autorise à faire comparaître des témoins.

Subpoena : une Citation, c'est « une commande d'apparaître à un certains temps et endroit pour donner le témoignage sur une certaine question.

En ce cas, les témoins déposent sous la foi du serment et sont susceptibles, s'ils mentent, d'être inculpés pour faux témoignage.

Ces commissions ne sont cependant pas des tribunaux. Elles ne jugent pas et ne condamnent pas.

Mais elles sont redoutables et redoutées. Dans le passé, elles ont servi à débusquer les gaspillages du gouvernement fédéral, les réseaux de gangstérisme, les infiltrations communistes. Leur puissance fait d'autant plus peur que leur composition repose sur des fondements politiques. Leurs auditions étant télévisées, les Américains ont ainsi l'impression qu'ils participent au fonctionnement de la démocratie. Et force est d'admettre que le spectacle les passionne. Les chaînes alternent retransmissions et commentaires sans regarder sur le temps d'antenne. La commission entend des témoins tout à fait inattendus.

Assistants auprès du président, anciens membres du cabinet, responsables des services de renseignement, animateurs du CRP... Leur fidélité à Nixon ne fait aucun doute. Mais l'heure n'est plus à l'héroïsme. Il faut parler, sous peine d'être contredit par le suivant et poursuivi pour faux témoignage. En un mot, c'est le sauve-qui-peut général. Le témoignage de Dean est accablant, mais il est contredit par Ehrlichman, et les preuves irréfutables manquent.

Et le miracle finit par se produire. Alors qu'elle interroge un des collaborateurs de Haldeman, la commission lui produit une note transmise par les services du président, sur une conversation avec Dean. La note est précise, trop précise pour être un résumé. Et le collaborateur, d'une voix calme, d'annoncer que la conversation est extraite d'un enregistrement. D'un enregistrement ? Oui, le président enregistre tous ses entretiens à l'insu de ses interlocuteurs. Le système est complexe. Les bandes magnétiques se mettent en route dès que les voix sont audibles. Pas de bouton à pousser, pas de levier à actionner. Émotion.

« Nixon espionnait ses propres bureaux », titre le New York Times. Les Américains découvrent que leur président espionne, dissimule, ne cesse de mentir.

À la vérité, le contenu des bandes devrait faire progresser l'enquête. On saura enfin ce que Nixon a appris, dit et ordonné depuis plus d'un an. C'est pourquoi la commission sénatoriale et le procureur ont demandé immédiatement qu'un certain nombre de bandes leur soit communiquées. Nixon hésite sur la conduite à tenir. Il ne peut plus détruire ces bandes. Faut-il les donner au Sénat et à la Justice ? Non, car l'Exécutif n'a pas à livrer au Législatif des documents confidentiels qui touchent la sécurité nationale. La Maison Blanche fait traîner la procédure, au point que l'Attorney General (équivalent du juge d'instruction) et le procureur spécialement mis en place démissionnent.

Les journalistes s'empressent de trouver une expression qui fait mouche : « le massacre du samedi soir ».

La réaction des médias frise l'hystérie. On parle d'Apocalypse, de coup d'État, on parle de « la nuit des longs couteaux ». Impossible pour la Maison Blanche de dissimuler davantage. L'opinion en a assez des mensonges, elle veut savoir.

Pour peaufiner le tableau, le vice-président, Spiro Agnew, a été contraint de démissionner, par trop mouillé dans une affaire de corruption.

Et c'est alors que le Sénat met en route une procédure mal connue, mais qui va faire parler d'elle, et qui constitue son atout majeur dans le contrôle du Législatif sur l'Exécutif : la **procédure d'Impeachment**. Elle a été déclenchée le 31 juillet 1973 par un représentant, mais est restée sans effet.

Lorsque se posa aux constituants américains la délicate question du contrôle des diverses responsabilités du président des États-Unis, il fut opté pour la reprise pure et simple d'une procédure traditionnelle britannique, qui, sans trop démettre la séparation des pouvoirs, donne au Législatif un certain contrôle sur l'Exécutif.

L'**Impeachment** est donc une invention anglaise. Au départ, il s'agissait, conformément à la tradition, d'une procédure pénale, destinée à sanctionner un ministre ayant commis dans l'exercice de ses fonctions, une infraction. La Chambre des Communes l'accusait et la Chambre des Lords le jugeait. Sur ce fondement, deux ministres de Charles Ier (Stanford et Laud) furent exécutés. Aussi, à la fin du XVIII^e siècle, la simple menace d'Impeachment suffit à provoquer la démission du cabinet : en 1782, le ministre présidé par Lord North donne sa démission à la suite d'une motion de défiance votée par la Chambre des Communes et considérée comme susceptible d'entraîner la mise en œuvre de la procédure d'Impeachment. À partir de cette période, on peut considérer que la responsabilité pénale et individuelle se transforme en responsabilité politique et collective du cabinet.

La responsabilité politique se traduisait par une perte du pouvoir. Cette procédure est double : tantôt le premier ministre prend l'initiative de vérification, et pose la question de confiance. Tantôt, au contraire, l'initiative du débat est prise par les membres de l'assemblée, qui déposent une motion de censure. Signalons que le gouvernement dispose toutefois d'une arme de dissuasion : le droit de dissolution contre le parlement. C'est de même une procédure de contrôle du Législatif sur l'Exécutif qui a été mis en place dans la procédure américaine.

Aux États-Unis, l'Impeachment est la procédure selon laquelle le Congrès a la possibilité de mettre en cause la responsabilité du président, en le destituant, lorsque, dans l'exercice de ses fonctions, il est reconnu coupable, aux termes de la section IV article 2 de la constitution de 1787, de trahison, corruption ou autres délits graves. Cet article 2 souligne le caractère exceptionnel de la procédure, qui ne s'applique qu'au président, au vice-président, des États-Unis et à tous les fonctionnaires civils. Dans le droit américain, tous les crimes sont soumis au jugement d'un jury, sauf ceux qui entraînent l'Impeachment.

L'Impeachment se déroule en deux temps. La Chambre des représentants (l'équivalent de l'Assemblée en France, par sa composition) prend l'initiative. Il suffit que l'un de ses membres dépose une proposition d'Impeachment qui est transmise à la commission des affaires judiciaires (commission permanente formée dans le but de déterminer l'éventuelle responsabilité des membres du Congrès dans l'exercice de leurs fonctions). Si la commission émet un avis favorable, l'assemblée se prononce, à la majorité simple, sur sa mise en accusation. Dans le cas d'un vote positif, la Chambre assume le rôle de procureur général et délègue à plusieurs de ses membres, les managers, le soin de présenter l'affaire aux sénateurs. Le Sénat se transforme alors en Haute Cour. Il se prononce sur le dossier qui lui a été soumis, après avoir entendu l'accusation, les témoins et la défense. Si la condamnation est votée à la majorité des deux tiers, le coupable est démis de sa charge. Si la majorité des deux tiers n'est pas atteinte, l'acquittement est prononcé. Reste à savoir, et c'est là un problème que les Américains ne cessent de débattre, ce que sont « la trahison, corruption ou autres crimes et délits » qui déclenchent la procédure. Ce flou a débouché sur une pratique extrêmement hésitante.

C'est au lendemain du 20 octobre que l'opinion réclame que le Congrès agisse.

Quatre-vingt-quatre membres de la Chambre signent une motion d'Impeachment. Malgré les concessions de Nixon sur l'accès aux bandes magnétiques, malgré une opération « Honnêteté » que monte la Maison Blanche pour prouver une fois de plus que la page du Watergate a été tournée, la procédure est lancée. Dès la fin d'octobre, la motion est transmise à la commission des affaires judiciaires que préside Peter W. Rodino, un démocrate du New Jersey. À ses côtés, 20 autres démocrates et 17 républicains. La commission s'entoure d'une centaine d'experts, dont 45 avocats, reçoit de la Chambre un crédit d'un million de dollars pour mener l'enquête et, le 6 février 1974, se fait

attribuer par la Chambre (410 voix pour, 4 voix contre) le droit de préparer un rapport sur L'Impeachment et de citer à comparaître les témoins indispensables. Il ne reste plus au président Nixon qu'à renforcer l'équipe de ses défenseurs et à promettre sa collaboration « dans les limites des devoirs de sa charge ».

Pour mener à bien sa mission, la commission ne manque ni de moyens, ni de pouvoirs. Elle obtient la communication du dossier qui a été préparé par le grand jury (jury d'assises qui avait suivi l'instruction du procès des cinq « plombiers »). Elle bénéficie de l'aide de la presse. Mais il lui faut, en plus, une source indispensable qui lui permette de juger de la sincérité du président : les bandes magnétiques.

Jusqu'à la fin de juillet 1974, Nixon livre bataille, cède pied à pied du terrain et concentre involontairement l'attention de tous, y compris la sienne, sur le contenu des enregistrements. Le procureur spécial avait réclamé 9 bandes. Nixon est contraint de lui nommer un successeur, Leon Jaworski, et de promettre que les 9 bandes seront transmises au juge qui occultera, lui-même, les secrets de la défense nationale. Un geste de conciliation de la Maison Blanche. Et puis, l'on apprend que sur l'une des bandes, la conversation capitale entre Nixon et Haldeman à propos de l'effraction alors toute récente, est amputée de 18 minutes. Les spécialistes précisent qu'il s'agit d'un effacement par opération manuelle. Qui est responsable ? Avec dévouement, la secrétaire particulière du président, Rose Mary Woods, s'accuse de maladresse dans la manipulation des bandes. L'explication passe mal. D'ailleurs, la commission des affaires judiciaires demande maintenant à la Maison Blanche des documents et d'autres bandes magnétiques. La commission se fâche, rappelle qu'elle dispose du droit de citation à comparaître et que tous les Américains, quelle que soit leur fonction, sont contraints de s'y soumettre. Nixon croit alors avoir une idée géniale, qui en fin de compte lui coûtera cher.

Le 30 avril, le voici de nouveau devant les caméras de télévision. Le ton est solennel. Un an jour pour jour après la démission de Dean, Ehrlichman et Haldeman, le président annonce la nouvelle qui devrait mettre fin à l'agitation des esprits. La Maison Blanche a transcrit 46 conversations sur le Watergate. Elle publie la transcription en un volume de 1.300 pages, qui porte le sceau officiel. Une sorte de Livre Blanc définitif. Définitif, peut-être, incomplet, très certainement. Et surtout, très révélateur sur la personnalité de Richard Nixon, l'atmosphère de la Maison Blanche, le goût du secret et de la manipulation qu'expriment Nixon et ses collaborateurs. À lire le texte de ces conversations impromptues, sans fard ni précautions, les Américains apprennent que leur président se croit entouré d'ennemis, qu'il n'a qu'un souci, se tirer par n'importe quel moyen du mauvais pas dans lequel le Watergate l'a fait glisser.

D'innombrables « exclamations supprimées » témoignent de l'exactitude de la transcription et de la violence du ton. Le Chicago Tribune, qui a soutenu Nixon depuis 1968 résume l'opinion générale :

« Nous avons, au cours du premier mandat, vu l'homme public et nous avons été impressionnés. Maintenant, nous venons de voir l'homme privé et nous sommes atterrés ». Nixon perd bataille après bataille. Ce n'est pas qu'il ne dispose pas d'atouts. Sa politique extérieure connaît des succès appréciables depuis 1974 : le Moyen-Orient, l'URSS et l'OPEP sont des victoires diplomatiques incontestables, mais tout ceci ne sert à rien. Pour trois raisons :

1 — L'année 1974 est celle où les séides, puis les proches de Nixon sont condamnés. C'est la longue litanie des peines de prison qui frappent ces hommes, hier tout-puissants, aujourd'hui réduit à quêmander la clémence des juges. Ils tombent les uns après les autres : les sept du Watergate, puis les proches de Nixon de l'époque. Leur chute ne peut que susciter deux questions. Le vrai responsable, n'est-ce pas leur chef ? Et Nixon n'a-t-il pas déclaré plusieurs fois qu'il assumerait l'entière responsabilité ? Les procès, longs et détaillés, ont retenu l'attention. L'Amérique mène une œuvre de purification. Elle en oublie le monde.

2 — Les tribunaux fédéraux manifestent une incontestable indépendance. La liste des condamnés l'atteste et l'on se rappelle la détermination du juge Sirica, même si ses méthodes, voire sa brutalité inspirent des réserves. Le plus remarquable, toutefois, reste l'attitude des juges de la Cour Suprême.

En 1974, quatre de ses membres, y compris le Chief Justice Warren Burger, ont été nommés par Nixon avec l'approbation du Sénat. On a donc parlé d'une « Cour Nixon » qui aurait les mêmes idées conservatrices que le président et ne nourrirait qu'un seul désir : faire plaisir à Richard Nixon. Pure calomnie. Les magistrats ont montré une inébranlable rigueur. Ils ont dû donner leur avis sur l'accès aux bandes magnétiques. Le 24 juillet, ils sont unanimes (8 voix pour, 0 contre, 1 abstention) à déclarer que le président ne peut refuser la demande du procureur spécial.

C'est une décision capitale qui brise les dernières résistances de Nixon. Le 5 août, le président livre la transcription des trois conversations du 23 juin 1972 avec Haldeman. Il en ressort que Nixon a tout fait pour empêcher la poursuite de l'enquête judiciaire, et qu'il a dissimulé à ses propres avocats une partie de son rôle. La guerre est perdue. Nixon se résigne à la reddition sans condition. La décision du 24 juillet confère aux tribunaux fédéraux, à la Cour Suprême en particulier, un prestige exceptionnel. Ils ont contribué, eux aussi, à sauver le régime démocratique.

3 — Le rapport des forces politiques fait pencher définitivement la balance. C'est le temps des élections législatives et les nixonniens ne peuvent plus tirer profit de leur fidélité pour le président. Le navire coule. Il est temps de quitter le bord.

Dès la mi-juillet, il est évident que la Chambre des représentants votera la mise en accusation. Quant à la commission des affaires judiciaires, elle passe à l'élaboration de son rapport. Elle adopte un à un les articles établissant les chefs d'accusation. Ces articles, la Chambre doit les examiner dès la séance du 19 août. Le Sénat, de son côté, se prépare à se transformer en Haute Cour. Que peut faire Nixon ? Ses amis au Congrès le lâchent. Il pourrait décider de se battre jusqu'au bout. Somme toute, pour n'être pas démis de ses fonctions, il lui suffit que 34 des 100 sénateurs lui soient favorables. Mais ces 34 voix, il ne les a pas. Et puis, si le procès a lieu, les États-Unis seront paralysés pendant plusieurs mois et le président sortira de l'épreuve vaincu ou affaibli. S'il démissionne, il reconnaît implicitement sa culpabilité. Et depuis le 5 août, il a reconnu qu'il avait tout fait pour étouffer l'affaire. Le 7 août, la rumeur circule avec insistance : le président va démissionner. Le lendemain soir, Nixon annonce à la télévision qu'il quitte la Maison Blanche dans les 24 heures.

Le 9 août à midi, le président Ford prête serment et devient président des États-Unis. Nixon se retire en Californie.

L'épilogue a lieu le 8 septembre, quand le président Ford prend une décision très impopulaire : il accorde à Nixon « son pardon pour toutes les offenses commises ». Ce pardon présidentiel évite un procès en bonne et due forme qui aurait éclairé les dessous de table du scandale, résolu les énigmes et établi les véritables responsabilités, qui appartiennent désormais à l'Histoire.

L'affaire des écoutes de l'Élysée

L'affaire des écoutes de l'Élysée est une affaire d'écoutes téléphoniques illégales qui s'est déroulée sous le premier septennat de François Mitterrand (de 1983 à 1986).

La cellule antiterroriste de l'Élysée dirigée par Christian Prouteau et créée par François Mitterrand en 1982 serait impliquée.

Cette affaire, fut révélée pour la première fois par le quotidien Libération le 2 avril 1993.

Elle aurait selon le dossier concerné 150 personnes, dont 7 dans des conditions contestables. Près de 3000 conversations auraient été enregistrées entre janvier 1983 et mars 1986. Les écoutes, que les initiés appellent les « bretelles du président », ont apparemment cessé au moment de la victoire de la droite aux élections législatives de mars 1986 qui a entraîné une période de cohabitation.

Comme la presse l'a rapporté, ce ne furent pas les premières écoutes téléphoniques effectuées par les services de la république...

Le procès des écoutes de l'Élysée sous Mitterrand débute le lundi 15 novembre 2004.

Le procès des écoutes de l'Élysée, portant sur l'existence d'un « cabinet noir » qui écoutait illégalement des centaines de personnalités entre 1983 et 1986, lors du premier septennat de François Mitterrand, s'ouvre lundi 15 novembre 2004, à Paris, avec douze prévenus à la barre.

Douze personnes comparaissent, à partir de 13 h 30, devant le tribunal correctionnel de Paris dans le cadre de l'affaire des écoutes illégales par l'Élysée de centaines de personnalités entre 1983 et 1986, sous le premier septennat de François Mitterrand.

Au cœur de cette affaire : la cellule antiterroriste de l'Élysée, officine créée en 1982 à l'initiative du chef de l'État. Mais sous prétexte de défense de la sécurité nationale, la cellule a surtout cherché à étouffer certaines affaires compromettantes pour le pouvoir ou taire les secrets d'alcôve du président, écoutant des personnalités aussi diverses que l'actrice Carole Bouquet, l'écrivain Paul-Loup Sulitzer ou l'avocat Jacques Vergès.

Parmi les principaux prévenus, poursuivis pour les fonctions qu'ils occupaient entre 1983 et 1986, figurent Gilles Ménage, 61 ans, ex-directeur adjoint de cabinet du chef de l'État, et Christian Prouteau, 60 ans, ex-chef du Groupe d'intervention de la gendarmerie nationale (GIGN), directement chargé de la cellule.

Après s'être longtemps réfugiés derrière le secret-défense, les deux hommes ont fini par admettre, devant le juge chargé de l'instruction, certaines des écoutes qui leur étaient reprochées, tout en les jugeant légitimes et en soulignant avoir agi sur ordre de leur hiérarchie.

Parmi les prévenus figureront également Michel Delebarre, 58 ans, directeur de cabinet de l'ancien premier ministre socialiste Pierre Mauroy de 1982 à 1984, aujourd'hui député, maire (PS) de Dunquerque (Nord), ainsi que l'actuel PDG de Renault, Louis Schweitzer, 62 ans, directeur de cabinet de l'ancien premier ministre socialiste Laurent Fabius de 1984 à 1986.

Parmi les mis en examen comparaitra aussi Paul Barril, 60 ans, ex-équipier de Christian Prouteau à l'Élysée et acteur central du scandale des Irlandais de Vincennes,

l'arrestation en 1982 de prétendus dangereux terroristes, qui apparaîtra en fait comme une manipulation orchestrée par ses soins.

(En arrivant en 1981, François Mitterrand fait appel aux gendarmes du GIGN pour constituer sa garde présidentielle, plutôt qu'aux policiers. Le 29 août 1982, à 21 h 30, des membres du GIGN emmenés par le capitaine Paul Barril font irruption dans l'appartement d'un nommé Michael Plunkett, à Vincennes. Les gendarmes avaient apporté eux-mêmes des explosifs dans l'appartement de Vincennes. C'est le début de l'affaire des Irlandais de Vincennes... Après l'attentat de la rue des Rosiers, le commandant Christian Prouteau est chargé de coordonner la lutte anti-terroriste, après s'être vu confier, un mois plus tôt, la réorganisation de la sécurité présidentielle. Après les neuf mois de détention des

Irlandais de Vincennes, libérés fin mai 1983, l'affaire des Irlandais de Vincennes est devenue celle des gendarmes de l'Élysée.)

Quant aux huit autres prévenus, il s'agit principalement des « opérateurs » de la cellule, de hauts gradés de la direction de la surveillance du territoire/contre-espionnage (DST),

des renseignements généraux (RG) ou de la gendarmerie, directement chargés de fichier, écouter et retranscrire les conversations de leurs « cibles ».

Deux personnalités en particulier seront au cœur des débats devant le tribunal correctionnel, pour avoir fait l'objet d'une surveillance particulièrement serrée : le journaliste Edwy Plenel, aujourd'hui directeur de la rédaction du quotidien Le Monde, et l'écrivain Jean-Edern Hallier, décédé en 1997.

Selon l'accusation, le premier menaçait les intérêts du pouvoir par ses enquêtes, notamment sur l'affaire des Irlandais, le second par un chantage constant sur le locataire de l'Élysée, concernant principalement la révélation de l'existence de sa fille cachée, Mazarine Pingeot.

Le principal délit retenu à l'encontre des prévenus, « atteinte à l'intimité de la vie privée », leur fait encourir une peine maximale d'un an d'emprisonnement.

Le Monde (15 novembre 2004) « grandes oreilles de l'Élysée »

Vingt ans après les faits, le procès des « écoutes de l'Élysée » s'est ouvert lundi devant le tribunal correctionnel de Paris. Douze personnes, anciens collaborateurs du président François Mitterrand ou ex-militaires de haut rang, figurent dans le box des accusés.

Essentiellement poursuivis pour « atteinte à la vie privée », les 12 prévenus du procès des « grandes oreilles » de l'Élysée ont fait leur entrée au Palais de justice de Paris, lundi après-midi (15 novembre 2004).

Parmi eux, Christian Prouteau, 60 ans, ex-chef du GIGN et « patron » de la cellule antiterroriste de l'Élysée, a déclaré attendre « sereinement » l'issue du procès.

Son avocat, Me Francis Szpiner, a traité l'affaire, qui remonte à une vingtaine d'années, d'« archéologie judiciaire ». « On reproche à mon client d'avoir fait son devoir », a-t-il ajouté.

De son côté, Paul Barril, 58 ans, ex-équipier de Christian Prouteau, a simplement affirmé : « tout va bien se passer ». Son défenseur, Me Jacques Vergès, a dit attendre du procès que « sorte la vérité concernant tout le monde, même les plus haut placés : qui a ordonné, qui a manipulé tout ça en faisant porter le chapeau à d'autres ? ».

Les politiques convoqués

Lors des interrogatoires d'identité, les prévenus ont fait état de reconversions et de revenus disparates :

Christian Prouteau est préfet sans affectation à 5.000 euros par mois, Louis Schweitzer touche 165.000 euros par mois de Renault, Paul Barril anime une société de sécurité privée et gagne 7.000 euros par mois.

Le tribunal de Paris a décidé d'entendre comme témoins les deux anciens Premiers ministres socialistes Pierre Mauroy (1981-1984) et Laurent Fabius (1984-1986) qui, s'étant déclaré « totalement étranger à cette affaire », ne souhaitait pas déposer. À la demande de la défense, les juges ont aussi convoqué Raymond Barre, Premier ministre de 1976 à 1981. Seront également entendus l'ex-ministre des Affaires étrangères Roland Dumas et Paul Quilès, ancien ministre de la Défense.

« Une lourde atteinte à un droit fondamental »

Les prévenus se voient reprocher d'avoir utilisé la « cellule antiterroriste » de l'Élysée pour faire écouter entre 1983 et 1986 les conversations d'environ 150 journalistes, écrivains, avocats et personnalités du show-business.

Deux personnalités « victimes » seront particulièrement au cœur des débats devant le tribunal correctionnel pour avoir fait l'objet d'une surveillance particulièrement serrée : le journaliste Edwy Plenel, ensuite directeur de la rédaction du Monde, et l'écrivain Jean-Edern Hallier, décédé en 1997.

M. Plenel a indiqué qu'il avait « décidé de ne pas (s)'exprimer durant tout ce procès sauf devant le tribunal ». « Nous avons attendu 11 ans, 11 ans d'instruction. Tout le monde va se défendre, va argumenter, la justice se fait aux yeux de tous, ce n'est pas la peine que j'en rajoute », a-t-il dit. Il s'est porté partie civile et son avocat, Me Jean-Pierre Mignard, a estimé que « tous les Français comprendront l'enjeu de ce procès puisqu'il s'agit d'une lourde atteinte à un droit fondamental ».

TF1 (17 novembre 2004) « Les petites oreilles » de l'Élysée à la barre

Au troisième jour du procès dit « des écoutes de l'Élysée » en correctionnelle à Paris, le président Kross s'est attaché à mieux connaître ses autres prévenus. La veille, il avait entendu le chef, Christian Prouteau, à la tête du cabinet noir, cette cellule antiterroriste voulue par le président Mitterrand pendant son premier septennat. L'ancien patron du GIGN commandait alors une douzaine de personnes, aujourd'hui accusées d'avoir participé à un vaste système d'écoutes illégales sur de nombreuses personnalités dont le président de la République soupçonnait qu'elles le menaçaient.

Les excuses de la « secrétaire » font rire toute la salle Prouteau et son numéro deux, le capitaine Barril, avaient alors constitué leur équipe. Un recrutement particulier, comme en témoigne par exemple le profil de Marie-Pier Sajous, 45 ans, une grosse dame dont personne ne se méfierait.

Comment cette ancienne étudiante en lettres a-t-elle bien pu passer d'obscur employée à l'Institut de dessalement de l'eau de mer à la cellule où elle était supposée faire des synthèses sur le terrorisme ?

« J'ai envoyé des CV », répond-elle. Le président cassant : « Ah oui, alors qu'on sait dans la procédure que votre père était militaire et que votre mère était secrétaire au ministère de la Défense, au GIC ! » Le GIC, fameux groupe interministériel de contrôle qui justement réalisait les écoutes...

« Mes parents ne parlaient pas de ça à la maison », lâche alors Marie-Pier Sajous, suscitant l'hilarité dans la salle tout entière. Nouvel éclat de rire quelques instants plus tard, lorsqu'on apprend au détour d'une question qu'elle était salariée de Gaz de France, comme d'autres membres de la cellule, qui bénéficiaient « d'emplois fictifs » de la Poste ou d'Air France. « Et les lettres MP, MPier ou MPS, qui figurent sur nombre d'écoutes ? » insiste le président Kross, qui sait que les initiales apposées étaient celles des petites mains qui dépouillaient et analysaient les écoutes transcrites au GIC : « On a pu utiliser mes initiales », se défend-elle : « Je ne m'occupais que de dépouiller la presse, je faisais des photocopies d'articles pour des dossiers, c'est tout. »

« Et vous n'avez jamais vu passer une écoute ? » lui lance une avocate des parties civiles. La dame nie. Prouteau vole à son secours : « Elle ne devrait pas être là, elle n'était qu'une secrétaire », proteste-t-il.

Le Parisien, jeudi 18 novembre 2004, « Dès le départ, il y a eu des dérapages »

Comme une échelle un peu raide qu'on grimpe marche après marche, le président Kraus, qui dirige les débats du procès dit des écoutes de l'Élysée, essaie de comprendre la chaîne des responsabilités pour établir le rôle des douze prévenus, accusés d'avoir mis sur écoutes des dizaines de personnes, avocats, hommes politiques, journalistes et vedettes de cinéma, entre 1984 et 1986.

Hier (24 novembre 2004), il s'agissait de savoir ce « qu'en haut » on faisait exactement des branchements illégaux. C'est-à-dire à Matignon, lieu centralisateur de toutes les autorisations d'écoutes, où s'apposait la dernière signature, feu vert aux « grandes oreilles » du GIC (groupement interministériel de contrôle) chargé de l'enregistrement proprement dit.

Avant de recevoir les explications des deux « politiques » prévenus, à savoir Christian Delebarre et Louis Schweitzer, successivement directeurs de cabinet à Matignon, le tribunal a entendu l'ancien Premier ministre Pierre Mauroy, cité comme témoin.

Une audition instructive puisque l'on y a su que le « premier Premier ministre de François Mitterrand de 1981 à 1984 » avait appris à son proche collaborateur Delebarre « un petit jeu taquin ». « Lorsque mon directeur de cabinet est venu me voir, excédé par une demande d'écoutes de l'Élysée, je lui ai dit :

« La première fois, tu ne réponds pas, la seconde non plus. Et à la troisième... bon ben, il y a une hiérarchie dans la République, on était obligés d'accepter », soupire Pierre Mauroy, en levant les bras avec l'air de celui qui en a vu d'autres.

Par exemple, accepter « sans plaisir » qu'après la vague d'attentats terroristes en France en 1982 son projet de loi sur la légalisation des écoutes soit abandonné (il sera repris par Rocard). Ou encore avaliser « avec réticence » la création de la cellule de Prouteau et Barril, que le témoin assassine d'un mot : « Dès le départ, il y a eu des dérapages, des dysfonctionnements manifestes ! »

Les responsables de toute cette affaire ? demande le président : « Ceux qui ont signé les cartons d'écoutes, qui ont voulu un branchement et qui doivent savoir expliquer pourquoi. Ne me faites pas le coup de la responsabilité du directeur des chemins de fer obligé de démissionner parce que le garde-barrière a provoqué un accident ! » tonne Mauroy, pour qui la responsabilité est clairement du côté des soutiers.

Louis Schweitzer : « Il y a eu un effort pour me masquer la réalité »

Puis vient le tour en soirée de Delebarre et Schweitzer, qui avaient par délégation la signature de Matignon sur cette délicate question des écoutes. Une tâche pas facile. « Lorsqu'il s'est agi de renouveler l'écoute de Jean-Edern Hallier, raconte pour sa part Louis Schweitzer, pour moi c'était un cas limite.

Alors j'en ai parlé au Premier ministre, puis j'ai vérifié que c'était bien une demande du président de la République, en questionnant directement Jean-Louis Bianco à l'Élysée, je crois. Lorsque j'ai eu la confirmation que c'était une demande du président, je me suis renseigné sur la légitimité des motifs. Puis j'ai autorisé le renouvellement. » Mais l'actuel PDG de Renault d'expliquer, amer, les limites du système : « Les motifs invoqués étaient parfois succincts : trafic d'armes ou proxénétisme. Et j'ai aussi l'impression que lorsqu'on a utilisé un autre nom que celui de la cible, c'était pour me tromper. Il y a eu un effort pour me masquer la réalité. »

Le Parisien, jeudi 25 novembre : Le commandant Beau tient sa revanche

Pour cette troisième semaine du procès dit des écoutes de l'Élysée, il sera fidèle au poste. Assis au deuxième rang, à droite, sur les bancs des victimes, le militaire à la retraite Jean-Michel Beau veille au grain. Pas une seule explication des témoins ou des prévenus ne lui échappe.

Et si d'aventure l'un d'entre eux avance une imprécision ou marque une hésitation, il se lève aussitôt, rectifie in petto. Le colonel a imposé au fil des audiences, qui doivent durer jusqu'en février, sa présence intempesive, sa large stature enveloppée de costumes gris, et sa grosse voix de fumeur de brunes. Le président Kross, qui mène les débats fermement, a bien compris qu'il avait là un « adjoint » de choix dans la recherche de la vérité. Ce qui ne l'a pas empêché de lui rappeler discrètement, par l'intermédiaire de son avocate, Me Courregé, qu'il lui fallait se montrer parfois moins agressif.

L'affaire des Irlandais de Vincennes refait surface

Il faut dire que cet ancien gendarme de 61 ans tient là une revanche trop longtemps attendue contre Barril et Prouteau, les principaux prévenus de ce procès, qui l'ont manipulé dans la fameuse affaire des Irlandais de Vincennes, première dérive des deux super-gendarmes de l'Élysée.

À l'époque, en 1982, le commandant Beau, de la section de recherches de Paris, est appelé sur les lieux lors de l'arrestation de trois terroristes de l'Inla dans un appartement de Vincennes, opération menée par Barril. À la demande pressante du duo alors tout auréolé de sa proximité avec le président Mitterrand, et parce qu'il croit faire son devoir de militaire, Beau accepte de cacher à la justice le fait que la perquisition ne s'est pas déroulée dans les formes procédurales.

Il ignore alors que l'interpellation elle-même et les armes saisies étaient un coup monté par le capitaine Barril, qui avait lui-même déposé l'arsenal dans l'appartement de cette bavure gendarmes ?

Prouteau relaxé, Barril jamais poursuivi. Seul le soldat Beau, le « cocu », comme il l'a dit alors, trinque : douze mois avec sursis. Carrière brisée, déshonneur assuré, ce fils de militaire plonge dans l'amertume.

Et l'enquête — ce qui lui vaut semble-t-il de faire partie des « écoutés » de la cellule — pour découvrir la vérité sur les Irlandais de Vincennes, qui finit par éclater dans la presse, à défaut de venir dans les prétoires.

Pour voir Prouteau et Barril rendre des comptes à la justice, Beau devra attendre des années que le « dossier des écoutés », autre gros scandale lié à la cellule, arrive enfin devant des juges. Il tient donc aujourd'hui sa dernière « chance » : voir ses anciens compagnons d'armes répondre de leurs actes. Son honneur depuis longtemps perdu lui donne des ailes, il connaît le dossier par cœur : ses questions incisives, documentées, fouillent dans la mémoire de ceux qui viennent à la barre.

Mercredi dernier, l'audience a fait un saut décisif. Le témoin du jour, outre l'ancien Premier ministre Mauroy, était surtout le capitaine Marie, qui suivait les autorisations d'écoutes à Matignon et qui s'est souvenu que la production de la cellule était vraiment faible, ne se rappelant avoir vu presque aucun nom de la longue liste des « écoutés ». Laisant entendre que la cellule avait mis au point un circuit pour déjouer les procédures habituelles.

Beau a préparé ce procès comme si sa vie s'y jouait. C'est un peu ça d'ailleurs. Il n'est sorti de la dépression qui le ronge que pour assister à la dernière scène d'un drame qui l'a broyé il y a vingt ans et obtenir enfin la vérité. On ne se méfie jamais assez d'un militaire injustement humilié.

Le Parisien, lundi 29 novembre 2004, Écoutes : Quilès n'a rien vu, rien entendu

Au procès sur les branchements élyséens, l'ex-ministre de la Défense se défausse. Ministre de l'Équipement envoyé à la Défense le 20 septembre 1985, Paul Quilès découvre des « constructions particulières » sur les lignes téléphoniques des terroristes ou des trafiquants d'armes.

Mais pas seulement. Jean-Claude Kross, le président du procès des écoutés de l'Élysée, a rappelé hier à ce prétendu « novice » en la matière, qui signe sans barguigner « des piles de fiches » d'autorisation, que les « constructions » interdites sur les avocats, les journalistes et parlementaires ont été édifiées en masse sous son règne de six mois, achevé le 20 mars 1986. Joël Galipapa et Gérard Ecorcheville, amis politiques de Charles Pasqua, ont été espionnés avant l'alternance, les journalistes Edwy Plenel, Hervé Brusini, Michel Cardoze et Jean-Marie Bourget ont été souvent surveillés pour traquer les auteurs de fuites dans l'affaire Greenpeace.

Mais Paul Quilès n'a rien vu, rien entendu.

Il a débarqué « à l'improviste » à la Défense pour remplacer Charles Hernu, limogé à cause du sabotage par des agents de la DGSE du bateau de Greenpeace en Nouvelle-Zélande, « sans connaître ce milieu » et sans un brin de curiosité. Paul Quilès se familiarise vite fait avec les us et coutumes de la Maison, chausse les bottes de son prédécesseur Hernu, apprend du chef du bureau réservé de son ministère que vingt lignes d'écoute sont dévolues à l'Élysée, sans s'en étonner outre mesure et sans même soi-disant connaître l'existence de « la cellule » : « Sur le coup, j'ai pris le système tel qu'il était. Mes préoccupations majeures étaient l'état de déliquescence de la DGSE et le rapatriement des deux agents de Nouvelle-Zélande. »

Sondages.

Donc, « dix minutes à un quart d'heure par semaine », le ministre de la Défense Quilès paraphe à la chaîne les demandes d'écoute de ses services et de « l'Élysée », et « pose de temps en temps une question. par sondage pour savoir pourquoi » telle ou telle personne « inconnue » de lui se retrouve surveillée. Sans plus. Il ignore que la construction au nom de Lapierre visait Edwy Plenel qui a révélé dans le Monde l'existence de « la troisième équipe » de la DGSE ayant coulé le Rainbow Warrior.

Une note de son bureau réservé retrouvée dans les archives de Christian Prouteau, ex-chef de la cellule, indique pourtant que « M. Plenel vit avec Mme Lapierre », souligne Me Francis Szpiner. Mais cela aussi a échappé à Quilès. Sinon, il aurait « fait cesser » ce branchement « instantanément ».

Jean-Edern Hallier.

Il n'est pas plus au courant de « la maladie de François Mitterrand et de l'existence de Mazarine » :

« J'ai appris tout cela par la presse », rétorque ce témoin fort mal tuyauté pour un ex-ministre des services secrets.

La révélation imminente de la vie privée du Président par Jean-Edern Hallier a pourtant suscité des écoutés tous azimuts sur l'écrivain. Dans l'hypothèse où Paul Quilès serait responsable de quelque chose dans ces affaires de plomberie et de constructions, ce serait éventuellement « de [sa] signature », dit-il.

À l'en croire, il s'agit d'une simple formalité, d'un gribouillis au bas d'un carton blanc qui... permet des écoutés : « C'est un des éléments, un des maillons de la chaîne », minimise-t-il. Certes, feu son prédécesseur Charles Hernu ne s'est pas contenté de jouer au sourd et à l'aveugle, signant à tour de bras et approuvant en connaissance de cause tous les desiderata de la cellule présidentielle ou de son complice François Mitterrand.

Mais Hernu et Mitterrand ne sont plus.

Et Quilès se défausse. Me Olivier Metzner, qui défend Pierre-Yves Gilleron, ancien de la DST reconverti à la cellule, toujours bouche cousue par le secret défense, ne comprend pas bien : « Vous avez une aversion pour les écoutés, pourquoi n'avez-vous pas cherché à contrôler plus ? » « Vous n'imaginez pas l'emploi du temps d'un ministre de la Défense ! » Les douze prévenus pour « atteinte à l'intimité de la vie privée » boivent du petit-lait et ironisent en aparté : « Bel exemple de courage politique ! »

Liberation, mercredi 01 décembre 2004, Écoutes : au service secret de sa majesté Mitterrand

Le général Esquivié, alias Aramis, a nié toute activité répréhensible.

Les « mousquetaires » de l'Élysée qui ont espionné des gens de la presse, du barreau, de la politique et du spectacle pour le compte de François Mitterrand de 1983 à 1986 manquent de panache. Vingt ans après l'épopée tragi-comique de la « cellule » dite antiterroriste installée à demeure rue de l'Élysée par le président de la République, les huit anciens serviteurs du « roi » jugés pour « atteinte à l'intimité de la vie privée » entretiennent encore un indécrottable culte du secret, même sur des combines minables et des pseudo bidons.

Ainsi, le général Jean-Louis Esquivié, 63 ans, habit gris passe-muraille, cheveux crantés poivre et sel, refuse encore d'admettre qu'il a signé Aramis une tribune dans le Monde en 1985, plaider pour domo en faveur de la police parallèle de l'Élysée : « Il s'agit bien d'une nouvelle aventure des légendaires mousquetaires, écrivait Aramis. Ils servaient le roi, ils servent aujourd'hui le chef de l'État. Ils étaient chassés par les gardes du cardinal, ils sont aujourd'hui la cible de tous ceux que le pouvoir du Président dérange [...] Ils étaient fidèles, ils sont aujourd'hui toujours fidèles, n'ont aucun état d'âme [...] » Il comparait la cellule à « la cote de maille du Président », à un indispensable « entourage-rempart ».

Riposte.

Patelin mais mordant, l'homme de robe Jean-Claude Kross, qui préside à Paris le procès des écoutés de l'Élysée, croise le fer avec Aramis. Quatre prévenus ou témoins, son supérieur Prouteau, le capitaine Barril, le général Gervais et même le journaliste Edwy Plenel ont désigné Esquivié. « Je sais comment a été construit le texte mais je ne suis pas propriétaire d'Aramis, M. Plenel peut se tromper comme sur le financement du PS », riposte Esquivié.

Voilà que son voisin à l'audience, Gilles Ménage, accusé lui aussi d'écoutes illégales, le dénonce sur le champ. L'ex-directeur de cabinet de François Mitterrand explique qu'à l'époque il avait été pris à tort pour Aramis, et qu'il avait essuyé les « reproches épouvantables » du ministre de l'Intérieur, Pierre Joxe.

« Je pense qu'Aramis se trouve à côté de moi », accuse Gilles Ménage. Le président jubile, « cinq à zéro, monsieur le général Esquivié », et sort du dossier d'autres « détails » qui, mis bout à bout, attestent le rôle majeur de Jean-Louis Esquivié, numéro 2 de la cellule et chef de l'informatique.

Fiches.

À la barre, Aramis sert des explications fumeuses : il travaille dans le bureau de Christian Prouteau « à cause du manque de place ». Il ratifie des ordres de mission et des demandes d'écoute : « J'ai signé les yeux fermés et par gentillesse pour mes camarades, en l'absence de Prouteau. » Sans rien regarder du tout.

Il n'a pas non plus installé le logiciel Filing d'IBM à la cellule pour intégrer les transcriptions d'écoutes téléphoniques et ficher les gens par centaines en 1983.

(Révélée par Hervé Gattegno, l'affaire est digne d'un scénario de film policier. Mi-janvier, donc, une femme se présente devant les grilles du Palais de Justice de Paris et remet à un gendarme en faction une enveloppe à l'attention du juge chargé du dossier des « écoutés de l'Élysée », qui, un mois auparavant, a mis en examen, pour « atteinte à la vie privée » Gilles Ménage, ancien directeur de cabinet du président de la République et actuel président d'EDF ; le préfet Christian Prouteau, ancien chef de la cellule antiterroriste de l'Élysée ; le général de gendarmerie Jean-Louis Esquivié ainsi que le capitaine Pierre-Yves Guézou et l'ancien commissaire de la DST Pierre-Yves Gilleron. À l'intérieur de l'enveloppe, le magistrat instructeur — bien en peine, malgré tout, de détenir des éléments imparables sur les pratiques de la cellule —, trouve 5 disquettes d'ordinateur portant chacune la mention « backup », et étiquetées de 1 à 5. Le 16 janvier, il confie à un expert informaticien la tâche de les décrypter. Ce qui ne va pas le plus simplement du monde, car leur contenu n'est pas directement lisible à l'aide d'outils logiciels standards ou de grande diffusion. Le juge Valat doit alors se souvenir d'une information rapportée par « le Monde », partie civile dans cette affaire après que l'un de ses journalistes, Edwy Plenel, eut été écouté. Il suggère à l'expert de recourir à un programme de traitement de texte élaboré par IBM, le logiciel Filing, utilisé par la cellule pour enregistrer ses données.

Miracle des technologies : là, grâce à Filing, l'expert voit apparaître sur son écran d'ordinateur 5.184 fiches, réparties en 26 fichiers, dont 23 sont constitués d'écoutes téléphoniques concernant autant d'individus. Selon le rapport d'expertise, « la quasi-totalité de ces fichiers auraient été créés avant le 25 octobre 1985, et au plus tard le 21 mars 1986 ». La thèse du maquillage, invoquée par les différents protagonistes de l'affaire depuis la publication, dans « Libération », de 16 comptes-rendus d'écoutes effectuées par ce service, prend un sérieux coup dans l'aile. Elle est carrément anéantie. Difficile maintenant de soutenir qu'il s'agit d'une grossière manipulation tendant à discréditer le gouvernement socialiste de l'époque, en lui attribuant des pratiques de fichage politique).

Pourtant, dans une note datée du 27 avril 1984 et exhumée des archives de Prouteau, la cellule demande à l'Élysée une audience pour le dirigeant d'IBM qui « a élaboré son informatique gracieusement, efficacement et dans la plus grande discrétion ». Esquivié n'en démord pas. L'informatique, ce n'est pas son truc. Lui, il multiplie les missions de lutte antiterroriste, monte des « opérations très secrètes » en Corse et au Pays Basque, œuvre à la libération des otages français au Liban : « J'ai rencontré tout ce qui bouge, le chef du Hezbollah, le patron des pasdarsans, négocié dans la plaine de la Bekaa, ramené des messages en arabe pour le Président, et ça, c'est écrit nulle part, j'ai même une petite blessure au pouce. »

« Actif »

Le mousquetaire se fait moins flamboyant lorsqu'il s'agit de répondre de la protection à outrance de la vie privée du chef de l'État et de « la tranquillité personnelle de Mme Mitterrand », dit le président Kross, de sa note sur l'homme politique Philippe de Villiers (« un Rastignac de province »), de ses « dîners » hebdomadaires avec Jean-Edern Hallier et de ses signatures pour reconduire des branchements interdits. Le président le sermonne : « On attend de serviteurs de l'État la vérité d'un dossier, vous devez ça à votre justice, si on cumule tous ces éléments, vous n'êtes pas un obscur et un sans-grade. » Esquivié :

« Il n'y en avait aucun à la cellule. Je me suis investi un maximum. » « Vous aviez un rôle important. »

« Actif », corrige Aramis. « Quelle affaire de haute trahison de l'État alliez-vous traiter ? » demande le président. Aramis baisse la garde : « Plenel. Heuh, je ne devrais pas dire cela, Farewell » (du nom d'une taupe au sein du KGB) .

Une révélation : « Actez, Mme la greffière ». Fine mouche, maître Christine Courrégé, pour une partie civile, demande à Esquivié « si la question de Mazarine relevait du secret défense ». Affirmatif :

« Le souci d'un père pour sa fille, ça, c'est de l'intimité. Imaginez un chantage sur le Président qui peut déclencher l'atome, l'arme nucléaire, oui, ça relève du secret défense. »

L'avocate du gendarme Beau, lui aussi victime d'écoutes, décoche une dernière flèche : « Vous n'avez pas eu l'occasion de vous poser des questions sur les limites ? »

Remercié pour ses bons et loyaux services à la cellule présidentielle par un galon de général de division, Esquivié persiste et signe : « Non. Je n'ai jamais douté personnellement ».

Libération, vendredi 03 décembre 2004, Écoutes de l'Élysée :

Joxe charge Mitterrand et pleure. L'ex-ministre de l'Intérieur puis de la Défense témoignait hier au procès. Tout d'un coup, Pierre Joxe s'est mis à sangloter.

L'ancien ministre de l'Intérieur puis de la Défense de François Mitterrand est interrogé comme témoin par Me Olivier Metzner, avocat de l'un des anciens membres de la cellule antiterroriste de l'Élysée, en quatrième semaine du procès des écoutes.

Jusqu'à-là, Joxe avait fait du Joxe. Politique, critiquant Mitterrand tout en faisant mine de respecter sa mémoire : « Occasionnellement, il recommandait de respecter la loi. (...)

J'ai essayé parfois de l'empêcher de commettre des choses illégales, sans réussir, mais le pourcentage est faible. » Erudit, citant Sophocle :

« Il existe des lois ineffaçables mêmes si elles ne sont pas écrites. » Protestant rigoureux : « Cette cellule ne pouvait provoquer que des ennuis, et on aimerait employer un autre mot. »

Mais on s'attendait à tout sauf à ce que Pierre Joxe verse une larme au terme de sa déposition. On en était à une digression sur l'affaire Ben Barka, indépendantiste marocain enlevé en 1963. Joxe évoque son karma personnel, son père Louis, ministre de De Gaulle, lui jeune militaire chargé de renseignements.

« Ben Barka, je l'avais vu quelques jours avant sa mort. J'aurais pu l'éviter, car j'avais des informations.

Le Sdece [les services secrets, rebaptisés DGSE] faisait ce qu'il voulait. C'est en me rappelant le passé que je sais qu'un service de renseignement, s'il n'est pas tenu, peut mal tourner. »

« Système bâtarde »

Auparavant, Joxe était revenu sur la création en 1982 de la cellule de l'Élysée, composée de policiers et de gendarmes en dehors de tout cadre légal. « J'ai prévenu Mitterrand que ce système était bâtarde, tordu, parallèle, sans hiérarchie claire. » Il dit son peu de goût pour les écoutes téléphoniques : « Il est tentant de s'en servir, tentant d'en abuser. » Charge la barque : « Il n'y a pas seulement les écoutes, mais l'archivage des fichiers ; là, c'est contraire à toute déontologie policière. » Revient sans cesse à l'ancien président de la République : « C'est malheureux à dire, mais ce truc a été organisé par Mitterrand. »

Le tribunal visite l'histoire sombre du mitterrandisme, notamment l'affaire du Rainbow Warrior, bateau de Greenpeace coulé en 1985 à Auckland (Nouvelle-Zélande) par des agents de la DGSE, avec mort d'homme à la clé (un photographe portugais de l'association écologiste, en lutte contre les essais nucléaires français dans le Pacifique).

Pierre Joxe revient sur la personnalité de Charles Hernu, ministre de la Défense en perdition : « Un vieil ami qui a perdu la tête. Je lui disais pourtant que les services spéciaux, par construction, peuvent conduire à des bavures, qu'il y en avait déjà eu dans le passé et qu'il y en aurait encore. Contre tout bon sens, de bonne ou mauvaise foi, Hernu a tout nié en public. »

Joxe relate son propre rôle au ministère de l'Intérieur : « On a su très vite que la DGSE était dans le coup. C'est malheureux à dire, mais je m'occupais de retarder les mesures d'identification de nos agents. » Il n'est pas peu fier des résultats de son « inertie feinte » vis-à-vis des autorités néo-zélandaises :

« D'autres [agents] n'ont pas été arrêtés. »

Le tribunal cherche surtout à savoir en quoi l'affaire Greenpeace, après l'affaire des Irlandais de Vincennes, a motivé l'écoute de journalistes en charge de ces affaires qui fâchent, la cellule de l'Élysée, délaissant sa mission initiale antiterroriste, se focalisant désormais sur la traque des fuites.

Joxe joue sa propre partition : « L'important, ce n'était pas les fuites, mais les faits. Un mort, un crime » Justement, il est soupçonné, à tort ou à raison, d'avoir informé la presse au nom d'une sombre manœuvre intragouvernementale. Joxe réfute l'honneur : « Il était fatal que l'affaire Greenpeace soit totalement publique un jour. » Il évoque pourtant ses liens avec Edwy Plenel, journaliste au Monde qui a levé de nombreux lièvres sur ces affaires. « Il écrivait alors du bien de ma politique policière, mais ce n'est qu'ultérieurement qu'on est devenus amis. »

Retour sur certaines obsessions de François Mitterrand :

« Pour des raisons que je n'ai jamais pu éclaircir, il était braqué contre Plenel, enragé contre le Monde. François Mitterrand, malgré tout mon dévouement à son égard, a quand même commis quelques erreurs dans sa vie.

À cette époque, il avait une mentalité obsessionnelle contre tout ce qui était imprimé dans la presse, pour des raisons politiques et personnelles. C'était pourtant contraire à tout ce qu'était et nous disait François Mitterrand, ancien avocat. Une part d'ombre. » Puisqu'il est question d'obsession, Pierre Joxe en revient à la sienne, en concluant sur la cellule de l'Élysée : « On ne peut pas concilier efficacité policière et respect des droits de l'homme avec une équipe de mousquetaires. C'est incompatible. »

Libération, 23 février 2005 Le procès des écoutes de l'Élysée, Les oreilles de Mitterrand ne rougissent pas

Défense, hier à Paris, de Christian Prouteau, ancien chef de la cellule.

Pour Christian Prouteau, Me Francis Szpiner a plaidé hier « l'honneur du soldat » contre « la lâcheté de l'État et l'hypocrisie du parquet ». Le procès des écoutes devant le tribunal correctionnel de Paris s'est achevé avec la défense de l'ancien chef de la cellule élyséenne, jugé pour 33 écoutes illégales entre 1983 et 1986.

Dans sa plaidoirie, Me Szpiner dénonce l'absence sur les bancs des prévenus de Pierre Mauroy et Laurent Fabius, anciens Premiers ministres ; il parle même de ces morts qui ont « joué un rôle central, François Mitterrand et Charles Hernu », ex-ministre de la Défense. Ne reste donc que le commandant de gendarmerie Prouteau, « homme de devoir et de courage », chargé d'une « mission » de lutte contre le terrorisme en 1982, après l'attentat de la rue des Rosiers. « Il ne s'agit pas d'une structure illégale ou d'une police parallèle, Prouteau a été régulièrement installé à la présidence de la République et a reçu 20 lignes d'écoutes sur les 924 effectuées au GIC », le centre officiel du gouvernement. Un petit nombre de lignes « facile à contrôler » par Matignon, qui signe les demandes d'autorisation de branchement. Il conteste tout détournement de procédure pour abuser les services des Premiers ministres successifs. Il ne voit « pas de dissimulation » des véritables identités des « cibles » d'écoutes lorsque la cellule indique les noms de leurs compagnes, Nicole Lapierre pour masquer le journaliste Edwy Plenel ou Blandine Vecten pour l'avocat Antoine Comte, « mais parce qu'elles sont titulaires des lignes ».

« Pas écouté, ni enregistré, ni transmis »

Très en verve, Me Szpiner dégage un argument juridique massue. Poursuivi pour « atteinte à l'intimité de la vie privée », Christian Prouteau n'a pourtant « pas écouté, ni enregistré, ni transmis » de transmissions, ce que punit le Code pénal, « c'est le GIC, c'est l'État qui l'a fait, Prouteau n'avait pas le casque sur les oreilles ». Il a certes demandé des branchements aux directeurs de cabinet de Matignon qui les ont signés et permis. « Il n'est pas complice par fourniture de moyens ni par instructions données », assène Szpiner, pour qui « les poursuites auraient dû être engagées » pour l'exploitation et la conservation de documents issus d'écoutes illégales.

« Car, en 1993, tout était prescrit »

Il évoque la question de la prescription qui se pose pour les multiples branchements de Jean-Edern Hallier jusque dans son bistrot de la place des Vosges et son restaurant de prédilection, la Closerie des Lilas. Car les conversations téléphoniques piégées du polémiste indiquent « non seulement qu'il se savait écouté », a souligné mardi Me Olivier Metzner, avocat de Pierre-Yves Gilleron, membre de la cellule, « mais aussi par qui ». L'écrivain provocateur contacte en effet, en 1983, le colonel Gervais, discrètement chargé à Matignon de réceptionner les comptes rendus d'écoutes, pour s'entretenir avec lui de ce sujet qui le vise directement. Une affaire de date essentielle, car, en matière de l'intimité de la vie privée, la prescription démarre le jour où la victime apprend le délit. Or, feu Jean-Edern Hallier n'a déposé plainte qu'en 1993, après la révélation scandale par Libération. Tout comme le journaliste du Monde, Edwy Plenel.

À son tour, Me Patrick Maisonneuve, pour l'ex-directeur de cabinet adjoint de l'Élysée Gilles Ménage, a recensé « 23 interceptions » de Plenel en 1984 et 1985, « permettant de penser raisonnablement que M. Plenel est informé de l'écoute ». Ainsi, l'investigateur explique à sa compagne : « Ménage, c'est le conseiller de Mitterrand, c'est celui qui nous écoute là. »

Or, si l'enquêteur du Monde et le polémiste Hallier se savaient espionnés à l'époque, ils auraient dû porter plainte dans un délai de trois ans, « car, en 1993, tout était prescrit ». Au fil des 32 audiences, Plenel a objecté que ces allusions au téléphone ont valeur de « plaisanteries », qu'il n'y croyait « pas vraiment ».

Troisième problème.

Edwy Plenel s'est désisté en fin de procès de sa plainte contre Louis Schweitzer, ancien directeur de cabinet à Matignon. Une bourde juridique. Me Szpiner s'en empare et signale que, dans deux cas, « la diffamation et l'atteinte à la vie privée », ce sont les plaintes des victimes qui déclenchent les poursuites, pas le procureur. Le retrait de plainte de Plenel à l'égard d'un prévenu entraîne, selon lui, « l'extinction de l'action publique à l'égard de tous ses coauteurs et complices ». Contre les douze qui risquent aujourd'hui entre quatre et douze mois de prison avec sursis, assortis d'amendes.

Libération, Novembre 2005 Le procès des écoutes de l'Élysée

Prison avec sursis pour les grandes oreilles de Mitterrand

Pour le tribunal correctionnel de Paris, c'est l'État qui doit être tenu pour responsable. Faute de pouvoir condamner François Mitterrand en personne, le tribunal correctionnel de Paris a distribué hier des peines symboliques aux anciens membres de la cellule de l'Élysée.

De la prison avec sursis pour ses principaux responsables (huit mois pour le commandant Prouteau, six mois pour le général Esquivié, trois mois pour le commissaire Gilleron), relaxe pour les moins gradés.

Dans la même veine, deux anciens directeurs de cabinet à Matignon, Michel Delebarre et Louis Schweitzer, sont condamnés, mais dispensés de peine.

Rendant à César ce qui lui appartient, le jugement est très clair : « Les faits ont été commis sur ordre soit du président de la République, soit des ministres de la Défense » (notamment Charles Hernu, également décédé). Mieux, il précise que les éventuels dommages et intérêts dus aux victimes d'écoutes sauvages devront être réclamés devant le tribunal administratif, les fautes commises par la cellule n'étant « pas détachables du service », compte tenu de sa « soumission à la volonté présidentielle ».

C'est donc l'État (donc les contribuables) qui devra réparer les basses œuvres mitterrandiennes. L'ancien directeur de cabinet de Mitterrand, Gilles Ménage (six mois avec sursis), est le seul de son entourage à payer.

Le tribunal a également réduit considérablement le nombre de personnes placées sur écoute téléphonique (150 personnes et 1 368 interlocuteurs, dont de nombreux journalistes) pouvant exiger réparation. Son jugement note bien « le caractère intolérable d'une réelle atteinte à la liberté de presse du fait de la dérive de la cellule de l'Élysée », théoriquement chargée de la lutte antiterroriste, mais de plus en plus obsédée par ce qui se disait de Mitterrand dans les journaux.

Cela ne relèverait pas d'une atteinte à l'intimité de la vie privée (le délit formellement poursuivi), mais seulement d'une ingérence dans leur activité professionnelle.

Au final, seuls quatre écoutés ont été retenus, avec leur proche entourage respectif : l'avocat Antoine Comte, défenseur des Irlandais de Vincennes, le pamphlétaire Jean-Edern Hallier, qui menaçait de révéler l'existence de Mazarine, le journaliste du Monde Edwy Plenel, en pointe dans l'affaire Greenpeace, et Joël Galipapa, collaborateur de Charles Pasqua aujourd'hui décédé.

Ce tri sélectif fait hurler Jean-Michel Beau, ancien colonel de la gendarmerie, partie civile, qui crie vengeance « depuis vingt-trois ans », plongeant seul dans l'affaire des Irlandais pour avoir protégé d'anciens membres de la cellule.

Sa voix de ténor a brusquement interrompu la lecture du jugement : « Je sors de la salle devant cette injustice inique et je vous emmerde. Poursuivez-moi donc pour outrage à magistrat. » Dans les couloirs, le général Esquivié philosophe : « Tout agent qui travaille dans l'antiterrorisme doit accepter de se retrouver un jour devant un tribunal. On devrait l'apprendre aux nouvelles recrues. »

Venger.

Le grand perdant est le capitaine Barril, condamné à six mois de prison avec sursis. On lui reproche d'avoir voulu se venger de la cellule, avec laquelle il était en conflit, en piratant sa mémoire informatique sous forme de disquettes et en la diffusant anonymement (dans la presse et auprès du juge d'instruction) pour se venger.

Les juges n'ont pas de preuve formelle contre lui, le parquet ayant même requis la relaxe. Ils se sont quand même fait une religion fondée sur ses « mensonges manifestes qui ne peuvent avoir pour finalité que de tromper le tribunal ».

Libération, jeudi 10 novembre 2005, Écoutes téléphoniques : les leçons d'un procès

Après trois mois d'audience, le procès des écoutes téléphoniques touche à sa fin. Entre dénégations et faux semblants, les débats auront permis d'établir quelques vérités sur l'histoire de la fameuse cellule antiterroriste de l'Élysée.

Comme l'affaire du Watergate, le scandale des écoutes montre donc à quel point les contrôles hiérarchiques et administratifs sont nécessaires dès lors qu'il s'agit de protéger l'exécutif du pouvoir (sans limites ?) qui l'anime. Mais le parallèle s'arrête là. En France, ni la presse, ni les parlementaires, ni les juges n'ont été en mesure de mettre en cause les politiques. Comme si l'avertissement lancé en 1965, dans le Coup d'État permanent⁹⁵, restait valable quarante ans plus tard. En dénonçant le cabinet noir du général de Gaulle, François Mitterrand constatait : « Ce qui sort en surface est peu de choses au regard de ce qui reste caché. »

Le jugement

Douze ans après l'ouverture de l'enquête judiciaire, le Tribunal correctionnel de Paris, dans son jugement du 9 novembre 2005, a exposé les motivations de sa décision judiciaire :

Le tribunal releva ainsi que le président François Mitterrand s'était montré soucieux de protéger divers éléments de sa vie personnelle, notamment l'existence de sa fille naturelle Mazarine Pingeot (dont l'écrivain Jean-Edern Hallier, menaçait de révéler l'existence si le président n'effaçait pas son lourd redressement fiscal) — voire, selon la dépêche de l'agence Reuters rapportant la décision judiciaire, le cancer diagnostiqué fin 1981 et son passé à Vichy pendant la guerre (affirmations qui n'avaient pas paru jusqu'alors). C'est pour des « motifs obscurs » (dixit le tribunal) également que le compagnon de Carole Bouquet est écouté à cause de ses relations au Proche-Orient tout comme Edwy Plenel, journaliste au Monde ou encore l'avocat Antoine Comte.

Dans ses attendus, le tribunal a encore pointé du doigt François Mitterrand : « Les faits avaient été commis sur ordre soit du président de la République, soit des ministres de la Défense successifs qui ont mis à la disposition de (Christian Prouteau) tous les moyens de l'État afin de les exécuter ».

Selon le Tribunal, François Mitterrand a été « l'inspirateur et le décideur de l'essentiel ». Le dossier a montré que le président avait ordonné lui-même certaines écoutes et avait laissé faire pour d'autres.

Le tribunal néanmoins souligna que les autres écoutes administratives réalisées par les services secrets et la police n'avaient pas plus de cadre légal que celles de la cellule antiterroriste.

Sept anciens collaborateurs du président sont finalement condamnés dont :

— Gilles Ménage, ex-directeur de cabinet adjoint (6 mois de prison avec sursis et 5 000 euros d'amende pour « atteinte à l'intimité de la vie privée »)

— Christian Prouteau, dirigeant de la cellule antiterroriste (8 mois de prison avec sursis et 5 000 euros d'amende)

— Louis Schweitzer, ancien directeur de cabinet de Laurent Fabius à Matignon, pour le placement sur écoutes de l'écrivain Jean-Edern Hallier (dispensé de peines)

— Michel Delebarre, ex-directeur de cabinet de Pierre Mauroy à Matignon, pour le placement sur écoutes de l'écrivain Jean-Edern Hallier (dispensé de peines)

— l'ancien gendarme Paul Barril, condamné pour le recel des données secrètes de la cellule à six mois de prison avec sursis et 5 000 euros d'amende.

Quatre autres employés de la cellule ont été relaxés ainsi que le général Pierre Charroy, patron de 1982 à 1999 du Groupement interministériel de contrôle (GIC), organisme qui réalise pour le compte du gouvernement l'ensemble des écoutes téléphoniques administratives (extrajudiciaires).

Seules sept parties civiles sont ainsi reconnues comme victimes parmi lesquelles l'ex-journaliste du Monde Edwy Plenel, en pointe dans l'affaire Greenpeace, l'avocat Antoine Comte, défenseur des Irlandais de Vincennes, Jean-Edern Hallier (décédé) ainsi que sa famille et Joël Galipapa (décédé), collaborateur de Charles Pasqua aujourd'hui décédé alors que 22 autres plaintes sont jugées infondées dont celles des journalistes Hervé Brusini et Michel Cardoze et celle de l'actrice Carole Bouquet.

Par ailleurs, le tribunal déclara que les fautes n'étaient pas « détachables du service de l'État ».

Aucune partie n'ayant fait appel du jugement, il a eu force exécutoire, mais les sanctions seront amnistées en vertu de la loi votée après l'élection présidentielle de 1988, et donc non inscrites au casier judiciaire, si les condamnés paient les amendes.

Constantin Melnik, conseiller de Michel Debré à Matignon, qui coordonna les services secrets entre 1959 et 1962 expliqua en octobre 1996 dans Le Monde que les écoutes

pratiquées sous François Mitterrand lui apparaissaient comme « des jeux d'enfants improvisés par rapport à ce qui était pratiqué systématiquement durant les premières années de la Ve République », en pleine guerre d'Algérie.

Le 13 mars 2007, la Cour d'appel de Paris a accordé à l'actrice Carole Bouquet un euro de dommages et intérêts et au lieutenant-colonel Jean-Michel Beau 5.000 euros, pour atteinte à l'intimité de leur vie privée dans cette affaire .

Djokhar Douaev tombe dans le piège

Le 9 avril 1996, cela fait presque seize mois que la sale guerre de Tchétchénie se poursuit dans le Caucase, lorsque Djokhar Douaev, ex-général de l'Armée rouge et dirigeant de la résistance tchétchène, annonce à quelques journalistes réunis pour une conférence de presse improvisée dans les montagnes du sud de la Tchétchénie, qu'il n'est disposé à négocier qu'avec le président Boris Eltsine lui-même. Il va être entendu... Dans la nuit du 20 au 21 avril, il réunit quelques fidèles dans une ferme du village de GekhiTchou où il attend une communication, par téléphone satellitaire, avec l'un des médiateurs proposés par Boris Eltsine. A l'heure prévue pour cette communication, ses gardes du corps déploient, dans un champ proche de la ferme, l'antenne parabolique nécessaire à l'établissement de la communication. Quelques minutes plus tard, Douaev est tué dans un bombardement.

Depuis le début de la guerre, le FSB cherchait le moyen d'éliminer le rebelle. Plusieurs tentatives d'assassinat s'étaient déjà soldées par un échec, mais les hommes de la Loubianka ne renoncent jamais.

Et, une nuit de printemps, leur heure était enfin venue. Chamil Bassaev, l'un de ses adjoints, responsable des forces spéciales de la résistance tchétchène, prétendra quelques jours plus tard que ce sont des missiles guidés par les ondes émises par son téléphone cellulaire qui ont tué le président et mettra en cause une puissance occidentale qui aurait placé ses satellites au service du FSB pour cette opération.

Une explication passionnante, mais fausse. Car si le schéma d'ensemble est bien réel, les choses se sont cependant déroulées un peu différemment. Et pour cause le missile anti-téléphone, comme des experts français de la guerre électronique le déclareront au journal Le Monde, n'existe pas : "S' il existe des missiles antiradars qui se guident sur les ondes émises par leurs cibles, le missile anti- téléphone n'a pas encore été inventé".

L'activation du téléphone portable du président tchétchène aurait, en revanche, permis sans beaucoup de problèmes à un Illiouchine équipé de matériel ELINT (Electronic Intelligence) de repérer en quelques secondes l'origine de l'émission du signal. Il suffisait dès lors de dépêcher sur place un ou plusieurs hélicoptères de combat en vol dans la région pour éliminer Douaev en tirant quelques missiles air-sol.

Mais l'important, en ce qui nous concerne, n'est pas là. Ce qui importe, bien entendu, c'est que le FSB ait jugé bon d'utiliser le prétexte de négociations au plus haut niveau pour attirer le loup tchétchène dans le piège qui lui sera fatal. Un procédé qui a porté ses fruits, mais qui discrédite dangereusement le pouvoir politique russe. Il y a fort à parier que, placés dans des circonstances identiques dans un avenir plus ou moins lointain, d'autres rebelles y regarderont à deux fois avant de croire à la sincérité de leurs interlocuteurs se réclamant du Kremlin...

Cambriolage à France Télécom

Le 3 mars 2000, il a été constaté qu'il y avait eu des visiteurs dans un dans un immeuble de France Télécom, et que les clés du responsable avaient été utilisées. Comme il n'y avait eu aucun vol, la gendarmerie et autres services d'investigation n'avaient pas été alertés.

Le lundi de Pâques, 24 avril, la direction de la téléphonie mobile à Montrouge dans les Hauts de Seines, Avenue de la Marne, s'est fait là, carrément piquer un coffre fort de 50 kg. Il contenait 360 fiches téléphoniques classées Secret Défense. Il y avait aussi un autre listing de demandes d'interceptions en cours, et 200 fiches d'écoutes datant de mi-décembre 1999, qui auraient dû être détruites et ne l'avaient pas été.

Elles concernaient des écoutes de téléphones portables dont les demandes émanaient de services comme la PJ, DST, DGSE, gendarmerie, les douanes, mais aussi DPSD... Elles sont roses pour la DST, jaunes pour la PJ...

Le cambriolage de France Télécom a été réalisé visiblement par des professionnels, qui en plus connaissaient très bien les lieux.

La sécurité de l'immeuble est réalisée par deux sociétés, une de télésurveillance, et l'autre de maîtres chiens. Ce lundi matin de Pâques, il y a d'ailleurs eu une intervention pour programmer le système de contrôle d'accès en jour férié. Un peu plus tard, un véhicule avec trois personnes arrive et rentre dans le parking souterrain en utilisant un badge magnétique. Ils évitent les caméras du rez-de-chaussée, puisqu'ils ne s'y arrêtent pas. Elles ne sont de toute façon pas branchées sur le réseau, et on peut même se demander s'il y a un magnétoscope qui enregistre ce qui se passe en permanence dans l'immeuble. Ils utilisent l'ascenseur pour monter directement du sous-sol au premier étage, qui n'a pas de caméra. Ils passent le sas avec leur badge, pour rentrer dans le service des écoutes. Il y a seulement 20 personnes qui peuvent y pénétrer avec un badge. Les cambrioleurs vont vers le bureau des deux responsables des écoutes habilités secret défense. Ils ne fracturent pas la porte blindée, mais démontent la paroi vitrée de côté.

C'est paradoxal à France Télécom, mais on va « durcir » quelque chose en y mettant le prix, et avec des cabinets d'études qui pensent à tout, alors qu'en passant par derrière si je puis m'exprimer ainsi, n'importe qui peut neutraliser un moyen qui a été coûteux à la réalisation.

Ensuite ils n'ont pas fait de détail, ils ont carrément embarqué le coffre avec eux, car il n'était pas scellé. Là, plus moyen de faire autrement, France Télécom a été obligée d'informer la gendarmerie. L'enquête a été confiée à la DST. C'est la preuve que la sécurité à France Télécom a de sérieuses lacunes. Ce n'est pas une grande surprise, quand on sait comment fonctionnent et sont dirigés certains départements.

Cette opération commando rappelle le cambriolage de la brigade financière sur les documents de l'affaire ELF, rue Château des Rentier dans le treizième.

Le feuilleton continue, un salarié découvre le jeudi 27 que son tiroir a été forcé durant la nuit. À la suite d'une fuite, le Journal du Dimanche du 30 avril 2000 a révélé ce cambriolage. Ce cambriolage a été confirmé le 3 mai 2000 par le secrétaire d'État Christian Perret.

Des opérateurs non contrôlés :

Un opérateur peut mettre n'importe qui sur écoute en toute impunité.

Il y a des naïfs qui pensent qu'il s'agit d'un cambriolage capuleux, dont le but était de voler des cartes téléphoniques. Soyons sérieux. Mieux on peut aussi lire que des concurrents avaient peut-être un but qui était celui de porter atteinte à l'image de France Télécom. La plaisanterie est quand même un peu grosse.

Mais on peut se demander aussi si le dirigeant d'un groupe ou d'une société concurrente à une des filiales du groupe France Télécom, n'a pas voulu vérifier tout simplement par ses propres moyens, s'il n'avait pas été mis sur écoute par l'opérateur. Cette hypothèse vaut aussi bien la précédente.

On peut aussi se dire qu'un très haut politicien, un ministre par exemple, ou un diplomate a voulu vérifier si son numéro de portable n'était pas sur écoute, en faisant cambrioler France Télécom par un service secret. Autre hypothèse qui tient aussi la route.

Il faut savoir que des chercheurs qui travaillent sur les effets du téléphone portable sur la santé, peuvent aussi avoir été mis sur écoute. De là à penser qu'il en est de même pour les politiciens qui travaillent sur des sujets qui dérangent les opérateurs, on peut se demander qu'est-ce qui peut empêcher ce dernier de les écouter en France.

N'importe quel politicien par exemple qui voudrait faire passer un texte de loi qui irait contre les intérêts des opérateurs pourrait se retrouver mis sur écoute sans le savoir, et sans que les services de l'État ne le découvre, puisqu'il n'existe aucun moyen, ou aucune structure officielle de contrôle, capable de vérifier ce fait et l'éthique de nos opérateurs. Ils peuvent faire des écoutes en toute impunité, puisqu'il n'y a aucune commission de contrôle pour vérifier leurs agissements. Ce fait est valable pour tous les opérateurs sans exception, y compris pour ceux d'internet, pour le courrier électronique.

Le CNCIS (Commission Nationale de Contrôle des Interceptions) épingle les officines et opérateurs :

Actuellement n'importe qui peut faire des écoutes quand ce n'est pas les opérateurs eux-mêmes qui commettent des actes illégaux en se livrant à des interceptions illégales. En Effet, des actions réalisées en marge de la légalité par des opérateurs ont été dénoncées par la CNCIS en 1998, qui s'est plainte de ne pas pouvoir les sanctionner. Le journal le Parisien du 30/04/98 publiait un article de Fabrice Lhomme sur le contenu du sixième rapport de la CNCIS. On retiendra que les écoutes clandestines sont estimées à 100.000 par an. Mais on apprend surtout :

« La CNCIS redoute qu'une insuffisante coopération institutionnelle avec les opérateurs de télécommunications et les industriels, conduise à la multiplication d'initiatives en marge de légalité ».

On ne peut être plus clair. Le CNCIS a jugé utile par exemple de retirer en début d'année 1998 à certaines sociétés, l'habilitation dont elles disposaient pour faire des écoutes, en raison du non-respect de la loi. Cette commission a aussi regretté, ce qui est tout à son honneur, que des poursuites ne soient pas engagées à l'encontre de ceux qui avaient violé cette législation en vigueur. On peut donc s'étonner que dans une république, que des politiques puissent accepter sans engager de poursuites, la violation de la constitution française, des droits des citoyens, l'atteinte à la vie privée, mais aussi de leurs droits.

Il n'y a en effet aucun service de l'État qui vérifie si les opérateurs de téléphonie ou Internet ne réalisent pas des interceptions illégales pour leur propre compte. Début avril une réunion a eu lieu au CNCIS en présence :

— du Conseiller d'État, Dieudonné Mandelkern,

— du Député PS Jean-Michel Boucheron,

— du Sénateur Centriste Pierre Fauchon,

Dans les coulisses, on déclare un certain agacement à l'égard de France Télécom Mobile, dont on dit volontiers qu'il se préoccupe plus de son chiffre d'affaires que de la sécurité des écoutes. Dans le rapport public du 8 juin, un chapitre concerne les problèmes liés à la téléphonie mobile. À partir de 1995, il a été imposé que les opérateurs

prennent les dispositions nécessaires, pour permettre les écoutes sur les mobiles. Elles coûtent 5 fois plus cher que les écoutes filaires. Chez certains opérateurs comme Bouygues, on attend que l'État paye ses dettes avant de refaire d'autres écoutes. Il est vrai que quand l'État vous réclame les impôts, il n'est guère patient .

Les « grandes oreilles » de la France

Le Ministère de la Défense se dote de satellites espions capables d'intercepter les communications téléphoniques, fax, e-mails... pour écouter le monde entier. *Par Serg BROSSELINE*

Au milieu des années 90 au siège parisien d'un groupe industriel français, tous les hauts responsables ont été convoqués par leur président qu'accompagne le directeur de la sécurité. Aucune des « huiles » conviées à la réunion n'a préalablement été informée de la raison de ce surprenant rendez-vous matinal.

Le chef de la sécurité met en marche un magnétophone. Stupeur des invités ! Ce sont leurs propres communications téléphoniques, interceptées à partir de leurs téléphones portables, qu'ils entendent !

Depuis, ces cadres dirigeants appelés à traiter les informations stratégiques sont sensibilisés aux risques des interceptions électromagnétiques.

Car, inutile de le préciser, ce que les « grandes oreilles » du ministère de la Défense français ont intercepté, le réseau d'écoute américain *Echelon* de la National Security Agency (NSA), dont le siège est à Fort Meade, dans le Maryland, en a eu également connaissance. Interception de mobiles, de télécommunications civiles (courrier électronique, fax, téléphone...) et militaires, recueils des caractéristiques des fréquences de fonctionnement des radars militaires ou des conduites de tir de batteries de missiles, tout s'écoute à partir de l'espace !

« Gouverner c'est prévoir », donc plus que jamais à l'ère de la communication généralisée, c'est avant tout, savoir. Voilà pourquoi le ministère français de la Défense va mettre en service en 2003 (voir dans la section traitant du réseau mondial d'écoute Echelon) un système d'écoute électronique spatial que seuls les États-Unis et la Russie possèdent aujourd'hui.

Les moyens d'enregistrement téléphoniques :

La justice peut se demander légitimement pourquoi et dans quel but des opérateurs de télécommunications filaires ou portables, s'équipent avec des systèmes d'enregistrement aussi sophistiqués, que même nos services officiels ne peuvent se payer. On peut douter que ces derniers sous-traitent ce genre d'activité sensible à des opérateurs, sinon on retomberait une fois de plus dans des contingents d'écoutes non déclarées, donc une fois de plus dans les écoutes illégales .

Il serait certainement très instructif d'écouter les justifications des uns et des autres.

Les nouveaux équipements disponibles chez divers constructeurs, permettent d'horodater et d'enregistrer 2 MICs simultanément. Cela correspond à 60 conversations téléphoniques et les deux canaux D respectifs. On peut sélectionner les conversations par les numéros des appelés ou appelants, par bornage d'une date et d'un créneau horaire. Toutes ces informations sont en effet contenues dans les canaux D.

En utilisant un dispositif externe de reconnaissance vocale, on peut extraire une communication à partir d'une empreinte vocale pour déclencher un enregistrement à partir de ces derniers. L'autre moyen possible consiste à utiliser les mots clefs pour déclencher une action. Comme exemple, nous pouvons prendre le logiciel *Voice-Assist* qui était livré à une époque avec la carte sonore SoundBlaster pour les ordinateurs IBM/PC.

Après avoir enregistré des mots clefs sous une ou plusieurs intonations, on programme pour chacun, une action ou fonction particulière interne ou externe au système.

L'ordinateur reconnaît ensuite le mot prononcé et déclenche l'action appropriée.

Pour en revenir aux enregistreurs, ils peuvent utiliser des cassettes S-VHS, DAT dont la durée pourra atteindre 500 heures en fonction du temps d'utilisation des canaux du MIC. Certains de ces appareils sont assez bien conçus pour n'autoriser qu'un accès sélectif à plusieurs techniciens qui auront chacun un mot de passe et leur propre journal d'accès au système horodaté. On peut autoriser ainsi un technicien à n'écouter que certains numéros. Ils comportent aussi bien évidemment un mot de passe ingénieur système ou encore appelé super-utilisateur. Plusieurs appareils peuvent être gérés en réseau à partir d'un seul ordinateur. Ils peuvent fonctionner en mode cyclique ou ping-pong ou dès l'apparition d'une communication sur un canal. Quand la bande est terminée sur un, un autre appareil prend la relève et enregistre.

Le nombre de constructeurs pionniers pour ce type de matériel est assez limité.

Le problème, c'est que si les services officiels ont acheté ce type d'équipement, ils n'ont malheureusement pu que les acheter en nombre réduit. En effet si on considère que le prix d'une unité est de l'ordre de 200 à 270 KF en fonction des constructeurs, tout le monde comprendra qu'il est impossible d'en installer dans chaque ville. Alors qu'en est-il dans ce cas pour les téléphones portables, réseaux auxquels la gendarmerie n'a pas accès. Ce qui est contraire aux opérateurs qui peuvent faire ce qu'ils veulent sans le moindre contrôle en plus. Leurs ennemis n'ont plus qu'à bien se tenir ou changer de mode de communication. C'est ce qui a peut-être justifié l'apparition de système de cryptographie pour le GSM à une époque. Les politiciens et services officiels, éditeurs journalistes, concurrents n'ont pas en effet à être écoutés par ces curieux d'un nouveau genre. Le nombre de constructeurs étant très limité, un juge n'aurait aucun problème à définir la liste des clients et compter le nombre vendu aux opérateurs.

Le principe de fonctionnement est le suivant : plusieurs abonnés sont reliés sur un central PABX. Les communications des suspects sont réorientées, par programmation vers un faisceau MIC sortant qui sera transmis vers le PABX d'un centre d'écoute officiel comme le GIC. Car en effet contrairement à un lien physique dédié à chaque fois à un seul abonné, ici on peut enregistrer 100 ou 300 abonnés différents sur le même enregistreur. Il ne faut seulement pas dépasser la limite de 30 communications simultanées. S'ils téléphonent donc chacun à tour de rôle, c'est ce qui permettra d'augmenter le nombre des suspects sur un seul système. Pour les téléphones portables, cela est plus complexe en raison de la mobilité des utilisateurs. Rien ne peut se faire sans passer par les divers opérateurs. Le groupe se retrouve donc automatiquement directement informé des actions engagées contre les dirigeants d'une de ses filiales. Voilà pourquoi la justice, les juges, les services de police auront plus de difficulté qu'avant pour faire leur travail.

Système d'interception ou d'écoute électronique téléphonique automatique :

C'est ce que nous pouvons appeler des écoutes automatiques. Il n'y a aucune intervention physique sur les installations. Elles sont totalement indétectables. Le principe consiste à réorienter dès la détection de mots clefs préprogrammés ou à partir d'une reconnaissance vocale les conversations automatiquement vers un centre d'écoute.

Le développement de ce genre d'autocommutateur téléphonique a commencé à être étudié et réalisé à partir de 1980 par la firme Pressley. Elle travaille pour le Département de la Défense Américain qui est un de leur client. Il permet précisément de tout numériser, tout sauvegarder, tout réorienter vers un centre pour une écoute et un traitement ultérieur ou voire même immédiat. Ce genre d'installation est disponible et opérationnelle chez British Telecom en Angleterre. Quand un opérateur s'installe sur notre territoire, il vient avec son propre matériel, avec ses PABX, ses logiciels de base et options plus ou moins connues.

Nous n'avons aucune garantie que des opérateurs n'utilisent pas ou n'utiliseront pas ce genre de système en France permettant de réorienter certaines communications de diverses firmes françaises vers leur pays. J'attire l'attention de notre gouvernement sur ce point particulier. Il n'y a en effet aucune différence matérielle ou modification, tout est géré et traité au niveau des logiciels. Je ne vois donc pas comment on découvrirait la supercherie sauf en espionnant tout ce qui transite sur les tuyaux en direction de l'étranger et encore. Si le traitement se fait sur place avec un système d'analyse en langage pivot, que l'on compresse et l'on crypte le tout, on n'y verra que du feu.

Des informations capitales pour notre économie ou nos recherches peuvent ainsi transiter. Il en est de même sur le réseau Internet. Un message que j'expédie à mon voisin peut très bien se retrouver à la NSA à Fort Meade tout simplement parce que j'aurai utilisé des mots dans mes phrases sans le savoir qui auront été programmé dans leur système.

On ne peut que conseiller à nos industriels des très hautes technologies d'être très prudent sur l'utilisation des réseaux comme Internet.

Nouveau service France Telecom : l'espionnage gratuit !

Article paru dans Le Virus Informatique 26 (juin 2004)

Qui n'a pas au moins une fois rencontré la Messagerie Vocale ? C'est un service gratuit de France Telecom qui, à l'instar d'un répondeur téléphonique, enregistre les appels. Il s'active au bout de quatre sonneries dans le vide ou lorsque votre téléphone est déjà occupé par une autre communication. Pour prendre connaissance des messages déposés, l'abonné doit simplement composer le 3103 depuis son combiné. Il connaîtra au surplus, la date d'appel et le numéro de téléphone de l'appelant. Mais, le saviez-vous ?

L'offre Messagerie Vocale comprend en outre des options pratiques, notamment l'alerte par e-mail. Elle vise en première ligne les gros consommateurs du net ou les itinérants.

Chaque jour, dès qu'un message est laissé sur votre répondeur France Telecom, un mail vous informe que « vous avez reçu dans votre messagerie 0142xxxxxx au moins un nouveau message le 09/06/2004 à 17:26:06 ». Pour l'activer, rien de plus simple : il suffit soit de téléphoner à un automate, soit d'envoyer un mail à l'adresse lamessagerievocale.3103@francetelecom.com. Dans l'objet, indiquez seulement votre numéro de téléphone et laissez le corps vide. Si tout se passe bien, un mail de confirmation vous annoncera dans les 48 heures la mise en route du système. Mais, grosse surprise, il n'y a aucune vérification de la légitimité des demandes !

Quiconque peut envoyer la demande d'inscription depuis n'importe quelle adresse e-mail et, surtout, mentionner le numéro de téléphone de n'importe quel abonné ! En toute discrétion, une personne mal intentionnée peut donc savoir si son voisin, ami, ennemi, patron, collègue, conjoint (etc.) a reçu des appels sur sa ligne. Il saura du même coup si, à l'heure indiquée dans le mail, il était absent ou occupé, car en week-end ou en vacances ! Les seules contraintes, aussi maigres que naturelles, consistent à connaître le numéro et espérer que la victime soit abonnée à la Messagerie Vocale... Bref, un bien bel outil d'espionnage offert par France Telecom !

Contactée, la société nous a remerciés, mais a également relativisé, car « très peu de clients utilisent l'avis de message par mail » (sic). Elle souligne, un peu gênée, que la procédure normale exige bien une validation par téléphone « mais trop souvent les clients oublient cette étape et se plaignaient que cela ne fonctionnait pas ». Pour « faciliter

cet usage, le service compétent procédait lui-même à l'activation, dans la foulée de la réception du mail. Nous allons donc restaurer la procédure initiale ». Virus, le premier magazine qui pourrit la vie des abonnés France Telecom ! (Source : David F. Gal lagher)
Marc Rees

Le Busch à oreilles...

Bush défend les écoutes téléphoniques (Article publié le 20/12/2005 dans RFI Actualités)

Patriot Act ou écoutes électroniques, le président américain continue à justifier des mesures exceptionnelles par la guerre contre le terrorisme.

Le président des États-Unis, George W. Bush, continuera à autoriser les agences d'espionnage à faire de l'écoute électronique aux États-Unis sans mandat de la justice. Samedi, dans son message radio hebdomadaire, il avait admis avoir autorisé plus de 30 fois des opérations d'écoute de plusieurs centaines, voire plusieurs milliers de personnes aux États-Unis. La loi interdisant aux États-Unis d'espionner des conversations d'Américains, le président a assuré qu'il s'agissait d'appels internationaux faits depuis les attaques du 11 septembre 2001.

Dans sa conférence de presse de lundi, George Bush a assuré que ces mesures étaient légales, relevant de sa « responsabilité constitutionnelle » de protéger le pays.

Revendiquant le secret ayant protégé l'opération, il a annoncé l'ouverture d'une enquête pour déterminer l'origine des fuites qui ont révélé la pratique de ces écoutes dans les colonnes du New York Times. C'était un « acte honteux » selon lui que de révéler les opérations d'écoute « en temps de guerre » allant jusqu'à assurer que « le fait qu'on discute de ce programme aujourd'hui aide l'ennemi ». Il a dressé un parallèle avec la responsabilité de la presse qui aurait révélé la façon dont Oussama Ben Laden communiquait par téléphone portable, ce qui, après publication, aurait poussé le chef d'Al-Qaïda à changer ses habitudes.

Un appel pour le Patriot Act

C'est encore au nom du 11 septembre et de « la guerre contre le terrorisme » que le président américain s'en est vigoureusement pris aux sénateurs qui bloquent le renouvellement du Patriot Act, une loi d'exception étendant les pouvoirs des forces de l'ordre dans le cadre de la lutte contre le terrorisme.

Lorsque la loi avait été adoptée dans la foulée des attentats du 11 septembre, tous les sénateurs sauf un l'avaient soutenue. Quatre ans plus tard, la quasi-totalité de l'opposition démocrate, rejointe par quatre élus du Parti républicain du président Bush, émet des réticences à sa reconduction dans la forme actuelle.

George Bush leur a rappelé leurs contradictions : « La plupart des sénateurs qui bloquent actuellement le Patriot Act l'avaient adopté en 2001. Ces sénateurs doivent expliquer pourquoi ils pensaient que le Patriot Act était un outil crucial après les attentats du 11 septembre et pourquoi maintenant ils pensent qu'il n'est plus nécessaire. » Interrogé sur la chaîne ABC lundi soir, le vice-président Dick Cheney est allé un peu plus loin dans les accusations vis-à-vis des sénateurs opposés à sa prolongation : « Ce qui me préoccupe, c'est qu'à mesure que l'on s'éloigne du 11 septembre, il semble que certains soient de moins en moins engagés à faire le nécessaire pour défendre le pays. »

Tensions entre la Maison Blanche et le Congrès

Ces remarques ont remis de l'huile sur le feu entre la Maison Blanche et le Congrès. En ce qui concerne les écoutes controversées, le président a fait valoir qu'il avait eu l'aval du ministre de la Justice pour les écoutes, mais il n'a pas mentionné l'autorisation du Congrès. Tout comme pour l'existence de prisons secrètes à l'étranger, ses élus (à l'exception des chefs de file qui n'ont pas été autorisés à partager l'information) n'ont pas été informés des écoutes. « Le président croit qu'il a le pouvoir de passer outre les lois que le Congrès a votées », s'est plaint le sénateur démocrate Russell Feingold, « le président ne choisit pas quelles lois il décide de suivre. Il est le président, pas un roi. » Pour les démocrates, l'affaire des écoutes est symptomatique des libertés que le président s'autorise vis-à-vis du pouvoir législatif. Ils reprochent à la majorité républicaine de ne pas laisser le Congrès jouer son rôle de contre-pouvoir et d'avoir signé des chèques en blanc au président Bush, sans lui avoir demandé de compte sur 14 dossiers, allant du scandale des fuites sur la couverture de l'espionne Valerie Plame, aux attributions de contrat en Irak à Halliburton, l'entreprise dont le vice-président Dick Cheney était employé.

Ces prérogatives que s'est attribué George Bush font aussi grincer des dents sur des bancs conservateurs traditionnellement méfiants vis-à-vis du pouvoir du gouvernement fédéral et de son intrusion dans la vie privée des Américains.

Les portables aussi...

Les radiotéléphones :

Il existe à ce jour divers systèmes comme le Radiocom 2000 dont l'activité devrait s'arrêter dans très peu de temps. Le plus répandu aujourd'hui étant le cellulaire ou [GSM](#). Il y a aussi le [Bi-Bop](#) qui n'a pas connu le succès du GSM. Il semble que ce dernier ne soit pas la solution en terme de confidentialité.

Sinon pourquoi des industriels ont-ils estimé nécessaire de produire des systèmes de cryptographie pour ce mode de communication ?

Il y a une raison. Il ne faut pas oublier que pour réparer ou régler ces appareils, des bancs radiotéléphone ont été créés. Même s'ils sont coûteux, en matière d'espionnage industriel, on ne regarde pas à la dépense. Ce type de banc à un coût qui oscille entre 100 et 200 KF, mais comporte une multitude de protocoles de communication numériques ou analogiques. Ces appareils permettent normalement de régler tout ce que l'on veut à condition d'y mettre le prix. Mais on peut aussi écouter en faisant quelques modifications, et en le couplant à une informatique assez lourde.

Mais il faut aussi avoir des complicités chez les opérateurs pour connaître certains numéros. Ce n'est évidemment pas à la portée du premier venu. Le problème c'est que les portées radio des portables sont réduites, donc l'écoute est possible pour un sédentaire, pour un pigeon voyageur, il est sûr que l'interception est beaucoup plus délicate. Il faudrait autant de systèmes d'interception radio qu'il y a de cellule.

Par contre, l'opérateur pourra lui écouter tout ce qu'il veut au niveau des MSC98, même s'il n'en a pas le droit, qui ira le contrôler ?

Aussi aberrant que cela paraisse, il n'y a en effet aucun organisme de contrôle qui vérifie si nos opérateurs respectent une certaine déontologie, et n'y dérogent pas pour effectuer des écoutes pour leur propre compte, sur les portables de leurs concurrents, des personnalités politiques gênantes, juges, ou brigade financière qui pourraient les déranger. Ils peuvent s'aménager en toute tranquillité un autre sous-sol, ni vu ni connu, faire en sorte que l'ascenseur ne puisse jamais l'atteindre sans un code spécial et une clef, et y installer tous leurs dispositifs d'enregistrement. Il installera des systèmes de traitement destinés à extraire les conversations à partir de mots-clés, d'empreintes vocales, ou des numéros des abonnés appelants ou appelés. Ce n'est pas sans raison que Matra Communication a développé le Matracom 9600 présenté à Millipol 96, qui est un réseau cellulaire numérique sécurisé et crypté, destiné aux services gouvernementaux.

1-Micro espion GSM (Fiche du revendeur)

« Micro espion » dernière génération conçu à partir d'un téléphone mobile cellulaire. À la différence des « Micro Espions » ordinaires qui utilisent les ondes radio classiques, l'émetteur GSM transmet sans limites de distance (couverture de la téléphonie mobile) ; il n'est plus nécessaire de posséder un récepteur scanner pour capter les émissions.

Indétectable par les appareils anti-micro espion.

Allumé, il peut être utilisé comme un téléphone portable ordinaire qui permet d'effectuer ou recevoir des appels téléphoniques.

Lorsqu'on l'éteint après avoir composé un code un secret il se transforme en redoutable micro espion GSM capable de transmettre les sons captés dans un rayon de 7 mètres.

Pour effectuer une écoute, il suffit d'appeler le numéro de la carte SIM (non fournie) à partir de n'importe quel téléphone (fixe, cabine, mobile) dans le monde ; l'appareil décroche automatiquement sans aucune sonnerie ; l'écran reste éteint.

Sans attirer l'attention il est alors possible d'écouter l'activité et les conversations du local où l'appareil a été installé.

Recommandé pour la surveillance audio d'un local, d'une cible en mouvement (une voiture ou caravane par exemple), d'une marchandise. Appareil d'investigation idéal pour détective privé ou pour usage personnel (surveillance audio de la maison par exemple), recherche de preuves, filature...

Livré avec batterie et chargeur.

Autres systèmes en vente libre : INTERCEPTEUR PASSIF GSM MULTIBANDE

IP-GSM-06

Ce système d'Interception de la téléphonie mobile convient pour travailler avec tous les réseaux GSM car il opère dans toutes les bandes attribuées (850/900/1800/1900 MHz).

Il intercepte passivement les objectifs, pouvant enregistrer tous les appels et messages de texte (SMS) émis ou reçus.

Ce système opère avec les données extraites de la MSC du réseau à explorer, donnant les données d'interception dans l'air (IMSI/TMSI).

L'algorithme y est incorporé COMP128 pour l'encryptement A5.0, A5.1, et A5.2, qui va effectuer le désencryptage en « temps réel ».

Il génère les registres d'activité des cellules explorées, avec les données correspondantes aux usagers enregistrés, permettant de « capturer » ceux-ci en tant qu'objectifs.

Il génère tous les registres d'activité des objectifs, tant des conversations effectuées, comme des SMS interceptés, avec registre de date, heure, durée, trant/sortant, identification d'abonnées, etc.

Il permet un « suivi en ligne » et la possibilité de convertir en fichiers MP3 (compressés) encryptables avec la possibilité d'être envoyés par courrier électronique.

Le système basique permet d'explorer en simultanément 2 Cellules avec 4 canaux audio d'opération, apte pour 2 objectifs en simultanément, et ce système peut « augmenter » jusque 12 Cellules (24 canaux audio), 12 objectifs.

Forme de travail :

Le système permet de contrôler plusieurs récepteurs selon la configuration et de visualiser sur l'écran l'activité des cellules explorées, obtenant ainsi les données d'interception : IMSI et KI de l'objectif, sans devoir utiliser sa SIM (puce) car ils s'obtiennent par le biais d'une application API de manière entièrement passive dans l'air.

Le système permet d'observer sur l'écran l'activité des cellules, les canaux et l'identification des usagers se trouvant temporellement dans la cellule explorée et par le biais d'une application on peut déterminer que l'un de ces usagers devient « objectif » ou charger dans la base d'objectifs, ceux en mode « spécifique ».

La configuration physique du système Basique (2 cellules 4 canaux audio) est autocontenue dans une valise où le « contrôleur » est un ordinateur du type Laptop (Notebook), Pentium IV, de nouvelle génération, contenant les programmes de contrôle du système et un module de RF et logique contenant le reste de logiciel, les plaques DSP et les récepteurs spécifiques multibandes, plus batterie, source d'alimentation et autres éléments.

Tout le système est facile à opérer et nous avons des plates-formes en base à Windows et Linux, selon demande expresse et possède une procédure d'utilisation permettant à un opérateur de pouvoir travailler avec tous les paramètres principaux en quelques heures d'apprentissage.

On peut aussi appliquer un logiciel spécifique pour la localisation de l'objectif par le biais du système LAI, que les réseaux GSM incorporent afin de minimiser les tâches de recherche de l'objectif.

Ce logiciel est supplémentaire et permet de pouvoir retrouver un « objectif » dans le Réseau GSM avec une précision allant entre 100 et 300 mètres, suffisant pour s'approcher et faire la capture.

On dispose aussi de dispositifs accessoires permettant d'augmenter considérablement la zone d'opération de ce système d'interception, par le biais d'un écran de cellules portatif « IC-GSM-01 », antennes directionnelles de gain élevé et amplificateurs d'antennes.

Comment fonctionne le Système :

Le système d'interception « multi-cellule », est basé sur le principe du besoin et de l'opérabilité d'un système efficace pour les propos destinés à ces fins, devant couvrir les attentes quant à leur réalité de fonctionnement d'un Réseau GSM.

Le diagramme de couverture d'un Réseau GSM est basé sur les principes basiques de besoins d'un système d'« interconnexion » entre les usagers de ce réseau, où les devises suivantes règnent :

- Densité d'usagers par zone géographique
- Situation réelle de zone géographique
- Réseaux d'alternative (concurrence)

Tout réseau GSM a un maximum de capacité allant jusqu'à 992 usagers (canaux) par cellule, cela veut dire qu'il ne pourra jamais donner plus de 992 interconnexions sans fil avec les téléphones mobiles (usagers), et si on prend aujourd'hui par exemple la zone d'un « centre commercial », avec la grande incorporation de « nouveaux usagers » au système de téléphonie mobile, on peut même avoir une zone de +/- 40.000 m² (quatre hectares) quelques 600/700 usagers actifs.

Tout système d'interconnexion (API) en un réseau GSM envisage que chaque BTS (cellule) n'admet pas plus de 60% de sa capacité, ce qui donne quelques 595 usagers maximum par cellule, cela veut dire qu'une zone de 40.000 m², où l'on dépasse le nombre d'usagers présents, « automatiquement » le réseau partage ces usagers avec les 2 cellules les plus proches. Ces usagers sont « répartis » spontanément et de manière « aléatoire », car l'attribution la donne la BCCH (qui désigne chaque canal à chaque usager), qui désigne la MSC, à chaque cellule, sur un rang ne dépassant pas 40.000 m², quelques 600/700 usagers.

Si on essaie d'interpréter cette situation, un système « approprié » pour travailler sur un rayon d'action appréciable où on considère qu'on aura toujours le « uplink » ou le « outgoing », c'est-à-dire que le signal généré par le « mobile » ou « station mobile » (on considère la voix de la personne propriétaire du mobile), qui sera toujours limité à un rayon ne dépassant pas les 500/800 m. Dans les meilleures conditions ce système devrait avoir la possibilité d'intercepter avec une capacité minimum de 3 cellules pour un rayon de +/- 200/300 m ou de 6 cellules pour la limite de rayon +/- 500/800 m de notre objectif.

Dans ces conditions, on considère une limite de capacité du réseau GSM, cela veut dire qu'on s'approche de la limite de sa capacité d'interconnexion. Cela ne se passe pas dans les zones où le nombre d'usagers diminue et une cellule ne peut pas recevoir pas plus de 150 ou 200 usagers permanents et pas plus de quelques 200 usagers qui « passent » par la zone c'est-à-dire qu'ils font « roaming » et n'occupent que de manière transitoire la cellule leur donnant service.

Dans les conditions les plus favorables (très peu d'usagers enregistrés) et avec une très faible densité, on pourra obtenir d'un objectif le maximum de capacité d'interception qui sera proche des 2 km dans les zones urbaines et de plus de 5 km dans les zones sous-urbaines.

Conception d'un système :

Si nos objectifs se maintiennent tous dans une zone géographique de moins de 50000/60000 m², avec un système de 6 cellules on pourra avoir l'interception simultanée de jusque 2 objectifs dans 100 % des appels car dans le rang des possibilités, on va toujours disposer de plus de 6 récepteurs pour le début de l'interception, 4 d'entre eux travaillant tout en interceptant et 2 autres explorant les cellules restantes pour ne pas perdre la communication.-

Avec ces devises, la conception d'un système multicellule doit envisager les caractéristiques suivantes :

1. Nombre d'objectifs
2. Emplacement géographique des objectifs
3. Mobilité des objectifs (déplacements)
4. Nombre d'usagers dans la zone à opérer
5. Mobilité du système intercepteur

Analysant selon le besoin de chaque situation en particulier on pourra penser un système nous permettant d'intercepter le plus efficacement possible, car avec un système passif, il est impossible d'intercepter à plus de distance ou avec grand pouvoir d'interception, car pour cela il devrait s'agir d'un système d'interception actif ou « enkysté » dans le réseau ou si on peut intercepter massivement la totalité des usagers sans importer les distances du système vers les objectifs.

On observe ici où on peut intercepter, de manière active, un objectif et pour cela, on doit compter avec l'approbation de la partie prestataire et une autorisation judiciaire pour le faire.

C'est différent lorsqu'on opère avec un réseau comme le GSM de manière passive, car l'action doit rester sans évidence de l'interception et donc sans avis au prestataire du service.

Comment opérer un système d'interception passif :

Dans la zone délimitée, on peut observer où travaille un « intercepteur passif » et toute l'information extraite et capturée, il le fait depuis l'air de manière complètement invisible.

L'Intercepteur actif « IA-GSM4 », tel qu'énoncé par le modèle, est un Intercepteur des réseaux GSM capable d'intercepter les conversations téléphoniques de jusqu'à quatre (4) téléphones cellulaires de façon simultanée, permettant en outre d'activer le microphone de ce téléphone pour pouvoir écouter les conversations qui se déroulent aux alentours, d'intercepter tous les messages de texte — aussi bien ceux reçus que ceux émis par chaque téléphone — et, finalement, de recevoir des messages de texte (SMS) avec toutes les données enregistrées chaque fois que le téléphone est éteint ou allumé, ou chaque fois qu'une quelconque donnée est ajoutée dans le carnet d'adresses.

Toute cette activité est totalement invisible puisqu'elle ne laisse aucune trace dans le téléphone cellulaire « espionné » et son propriétaire ignore totalement que l'ensemble de son activité est enregistrée anonymement, de façon permanente et sans limites de distance.

Ce système d'interception utilise le même réseau GSM que celui de la cible sans laisser de traces, peut importe si la cible se trouve dans une ville ou un pays différent, puisqu'à partir du moment où il utilise le service, il peut être intercepté.

Ce système possède des qualités uniques puisqu'il dispose des quatre bandes de fréquence utilisées par le système mondial de communication avec les mobiles, et qu'il est possible d'étendre son activité à l'ensemble de la planète. Pour couronner le tout, peut importe le protocole de cryptage utilisé, le système s'adapte à toutes les normes de tous les pays possédant des réseaux GSM (A5.0, A5.1, A5.2 et A5.3).

Composition du système :

Le système se compose des matériels suivants :

- Un PC équipé d'un processeur PENTIUM 4 double cœur à 2,4 GHz, de 512 Mb de mémoire RAM, d'un disque dur de 140 GB, d'un écran plat TFT 17", d'une carte d'interface RS232 (4 ports COM RS232) exploitant le bus PCI, d'une carte son (4 canaux actifs), d'un clavier, d'une souris, d'un jeu d'enceintes puissantes, d'auriculaires, de câbles d'interconnexion et d'accessoires.
- Un module GSM à 4 canaux actifs quadribande, programmables, livré avec interface audio et signal d'activité, batterie rechargeable, antennes multibandes, câbles et accessoires d'interconnexion, chargeur de batterie automatique et logiciel d'activation intégré (firmware).
- Un logiciel de contrôle « IA-GSM4 » codé et personnalisé pour chaque utilisateur, encapsulé dans une clé USB de 1 GB et avec blocage électronique.
- Un manuel d'utilisation du système (incluant la maintenance préventive), qui est remis à chaque client avec un cours de formation personnalisé.
- Quatre (4) logiciels de contrôle pour téléphones cellulaires tournant sous Symbian OS 7.0, 8.0 ou 9.0, personnalisés avec le numéro IMEI de chaque appareil.

Fonctions du système :

Le système IA-GSM4 permet de mener un registre total de toute l'activité de chaque téléphone cellulaire « objectif », en générant des registres de tous les messages texte et un registre de toutes les conversations ou écoutes ambiantes réalisées. Toute l'activité peut être stockée dans la clé USB fournie, dans un CD-RW ou dans un CD simple ; elle peut aussi être renvoyée de manière automatique par courrier électronique partout dans le monde.

Les registres du système se présentent sous forme de fichiers .txt pour les messages de texte (SMS) et sous forme d'archives .wav ou .mp3 compressés pour les fichiers.

Tous les registres sont générés automatiquement, mais la décision d'intercepter va dépendre directement de l'action de l'opérateur du système. Pour cette raison, notre entreprise prépare efficacement l'opérateur du système, qui devra en outre être informé sur le travail d'intelligence mené sur l'objectif.

Les écoutes officielles :

Elles sont réalisées le plus souvent au niveau des centraux téléphoniques.

Les communications sont réorientées vers le Groupement Interministériel de Contrôle (GIC) dont l'essentiel des installations se situe sous les Invalides. Son existence officielle a été légalisée le 10/07/91. La durée normale d'une écoute est de 4 mois renouvelable. Il est relié à une cinquantaine de centraux téléphoniques de Paris par une trentaine de MICs (1 MIC=30IT) minimum, ce qui donne l'équivalent de 900 lignes téléphoniques. Le reste est complété par des lignes analogiques pour arriver en 92 à un total de 1180 lignes donc d'écoutes simultanées.

Pour Paris il y avait 680 lignes et la proche province en comportait 530.

Aujourd'hui on peut penser en raison des risques terroristes que ce centre a multiplié le nombre de lignes par 4 en raison de la miniaturisation des équipements et de ses performances.

La salle d'enregistrement disposait de 4 rangées de 200 enregistreurs minicassette et de 2 de 120. Une autre rangée comportait 6 ordinateurs serveurs équipés chacun avec 1 MIC permettant d'intercepter un total de 192 lignes de télécopieur. Un système de gestion et de traitement permet l'horodatage, l'archivage, la destruction et l'extraction des fax utiles par repérage de mots-clés programmés. Je suppose que le principe de traitement est similaire au système Taïga. Cinq cents personnes permettent à ce site de fonctionner 24 h sur 24.

En 1992, le ministère de l'Intérieur devait utiliser 950 lignes, 300 pour la PJ, 300 pour la DST, 300 pour les RG approximativement. Le ministère de la Défense a environ 250 lignes et les finances utilisent celles qui restent, une quarantaine peut-être. Ces chiffres ne prennent pas en compte les infrastructures non officielles comme la cellule élyséenne qui n'existe plus normalement aujourd'hui. Dire qu'il dispose de moyens assez importants est faux, parce que beaucoup de ces équipements sont dépassés. Mais un gouvernement ne peut se permettre de le renouveler annuellement en raison du coût de telles installations. On peut dire que nos services officiels, du moins pour certains, sont moins bien équipés que les groupes industriels de notre pays. Sinon comment expliquer que la presse télévisée, a, elle, pu donner le nombre de 100 000 à 200 000 écoutes illégales.

D'où vient cette information ? Des services officiels eux-mêmes ? Ce chiffre est-il estimé à partir des ventes de matériel ?

En réalité, il n'y a pas que le GIC qui fait des écoutes. Les militaires, les divers services spéciaux, certains groupes industriels, ont leurs propres centres d'écoute téléphonique ou radio, à divers endroits toujours planqués dans des sous-sols. Certains services n'ont pas d'existence légale de même que leur personnel. C'est pour cette raison qu'il dispose de double, triple, ou quadruple identité, toutes plus vrai l'une que l'autre. Même le numéro de matricule de certains véhicules, ne permet pas de connaître les utilisateurs ou services véritables. Les services sont tellement cloisonnés, que les hiérarchies peuvent ignorer qu'elles sont aussi surveillées parfois. Ils ont leurs propres codes, leurs propres réseaux de communication filaire, fibres optiques, ou radio comme Tigre, Panthère, Syracuse, Rita pour les militaires, Saphir pour la gendarmerie, etc. Chaque armée a ses structures indépendantes des unes des autres tellement la confiance règne. Si entre services de l'ordre, on s'écoute, il en est de même avec, et entre les militaires, les politiques, ou polices politiques. La guerre des polices est loin d'être inexistante.

Ce qui m'intrigue le plus dans cette histoire, c'est comment et par quel canal, la presse a pu affirmer qu'il y a plus de 100.000 écoutes illégales

par an. Même s'il y a forcément des officines gouvernementales inconnues, on ne peut affirmer un tel chiffre, alors qu'il n'y a aucune trace, aucun recensement ni organisme de contrôle.

Les écoutes illégales tombent sous le coup de l'article 114 du Code pénal pour entrave aux libertés.

Mais les preuves étant impossibles à avoir, aucune plainte n'arrive en justice. Les plaintes déposées finissent sans suite, quand la victime ne se retrouve pas elle-même poursuivie pour dénonciations calomnieuses. Dans ce cas, il ne reste qu'une solution, pour quelqu'un qui a de gros moyens, la Cour Européenne de justice des droits de l'homme.

La France est un tel désordre dans ce domaine, qu'il a fallu faire passer un autre décret au journal officiel pour réglementer le contrôle des 40 sociétés privées s'occupant d'écoutes téléphoniques. Le business du renseignement comporte 50.000 personnes au minimum, et continue à se développer. On serait d'ailleurs plus près de la vérité en disant 100.000 personnes, si on compte les anciens policiers, les détectives, les électroniciens, les petits installateurs en téléphonie, les gardiens, tout ce beau monde qui arrondit ses fins de mois au noir.

Conclusion :

Les opérateurs de téléphonie n'ont pour mission que d'acheminer correctement ce qui est envoyé sur leur réseau.

La sécurité et le secret de vos conversations, c'est VOTRE affaire .

Les moyens hertziens et la perte de confidentialité des communications :

Les ondes, le moyen le moins sûr de communiquer.

À l'évidence, n'importe qui peut capter une émission radio, quelle que soit la fréquence utilisée. De plus, l'écoute et l'enregistrement d'un signal radio ne laisse pas de traces et est parfaitement indétectable.

L'histoire, en particulier la Deuxième Guerre mondiale regorge de faits de « Renseignement ». La possibilité de localiser un émetteur par goniométrie obligeait les résistants à des émissions de courte durée.

Le codage est de rigueur, nous développerons ce sujet plus loin, mais relisons quelques pages d'aventure vécue...

La tragique affaire Szek

Si les parents d'Alexandre Szek n'avaient pas vécu en Angleterre, le jeune radio n'aurait sans doute pas trahi l'Allemagne. Et le cours de la guerre aurait pu en être changé...

D'origine autrichienne, fils d'un familial de l'empereur, parlant couramment cinq langues, Alexandre Szek est un jeune ingénieur brillant.

Le déclenchement de la Première Guerre mondiale ne l'empêche pas de poursuivre, à Bruxelles où il se trouve alors, des recherches sur les communications par voie hertzienne. Indirectement, sa passion le perdra.

Le 27 novembre 1914, en effet, une panne généralisée paralyse les moyens de transmission de la Kommandantur allemande de la capitale occupée. Pour déceler les origines de l'incident et remettre en état le matériel défectueux dans les meilleurs délais, l'état-major réquisitionne tous les spécialistes radios sur lesquels il est possible de mettre la main, et Szek est bien entendu du nombre. Les qualités dont il fait montre, autant qu'une de ses récentes inventions dont le commandement a eu vent un appareil de réception radiotélégraphique capable de s'adapter à toutes les longueurs d'onde — incitent le gouverneur militaire de Bruxelles à recruter le jeune homme et à l'affecter définitivement au service de T.S.F. de son quartier général. Chaque nuit, jusqu'en février 1915, Szek dirige donc, depuis ses bureaux situés rue de la Loi, non loin du Palais Royal, dans le centre de Bruxelles, l'interception du trafic radio allié.

Londres écoute

Nous savons tous à quel point ce sont s'affrontés les services secrets allemands et anglais.

Et nous avons pu comprendre l'importance de l'interception et du décodage des communications allemandes par le S.R. britannique. Cette opération, menée sur une grande échelle, sera l'un des secrets les mieux gardés de la Grande Guerre (il ne sera d'ailleurs révélé qu'en 1931). C'est au cœur de la Naval Intelligence Division — le S.R. de l'amirauté — dirigée par l'amiral Hall que se niche la section que l'on désigne par le numéro de son bureau : Room 40, Old Building ou 40 O.B. C'est dans ces quelques pièces que travailleront, quatre années durant, les briseurs de code anglais. Dès le début de la guerre, la marine britannique a dépêché au large du continent quelques discrètes unités navales chargées d'une mission qui l'est tout autant : l'Opération cisaille. En une ou deux nuits, les câbles télégraphiques sous-marins allemands ont été remontés à la surface, coupés et rendus à leur vie sous-marine. Désormais, les communications de l'Allemagne avec le reste du monde ne peuvent plus passer que par les câbles sous-marins des pays neutres ou, en T.S.F., par la voie des airs. Il devient donc possible de les intercepter.

Encore faut-il les déchiffrer. C'est là le rôle de la brillante équipe d'universitaires rassemblée par sir Alfred Ewing au 40 O.B. Un coup de chance va considérablement faciliter leur travail : au début de la guerre, la flotte russe a récupéré, sur le corps d'un officier du croiseur allemand Magdeburg, coulé dans la Baltique, le code de ce bâtiment qui a permis de découvrir la clé de chiffrement de l'amirauté. D'autres récupérations, entre autres celle menée à Bruxelles par Alexandre Szek, vont permettre aux Anglais, durant toute la guerre, de déchiffrer la quasi-totalité des dépêches envoyées ou reçues par l'état-major, le ministère des Affaires étrangères et les autres services officiels allemands : « On établit des stations d'écoute le long des côtes britanniques » écrit sir Basil Thomson dans ses mémoires, « leur moisson nocturne était envoyée à la Chambre 40 O.B. à l'amirauté pour y être déchiffrée : apprendre les plans secrets de l'ennemi de sa propre bouche valait mieux qu'une tonne de rapports envoyés par l'armée d'espions employés

par les Alliés. Peu de gens connaissaient l'existence de 40 O.B., on la cacha même aux ministres mariés. Les messages déchiffrés qui se montaient parfois à 2 000 par jour étaient soigneusement gardés et même les chefs des gouvernements qui profitaient de ces nouvelles ne connaissaient pas toujours leur source »

La Radio et la Résistance

À Londres, le deuxième bureau du Général de Gaulle se transforme progressivement, sous l'impulsion du Colonel Devawrin, en Bureau Central de Renseignement et de le BCRA. Le BCRA a pour mission de fournir à la Résistance Française le soutien extérieur et les moyens de coordination dont le plus urgent à résoudre consistait à établir des liaisons radioélectriques France-Londres.

Les premières étapes.

— 1940 : Le Capitaine de Frégate d'Estienne d'Orves réalise la première tentative de liaison en Bretagne. Il est arrêté le 22 janvier 1941 et fusillé le 29 août de la même année.
— 1941 : Les opérateurs parachutés « blind » (sans comité d'accueil au sol) sont presque tous arrêtés. Fin 1941, 12 postes de radio établissent des contacts. On compte trois opérateurs en entraînement en Angleterre.

— 1942 : Jean Moulin est parachuté accompagné de son radio « Monjaret » le premier janvier, c'est la naissance de « l'Action ». Des opérations d'atterrissages et de parachutages sont de plus en plus nombreuses. D'abord limitées à quelques maquis, ces opérations s'élargissent à l'ensemble des deux zones avec arrivée de radios recrutés en France groupés en un pool nommé « WT », (Wireless Transmission).

Arrestation de Jean Moulin et « WT » décapité, c'est une longue période de silence entre Londres et la France alors que l'effectif des maquis grossit du fait des appels au STO (Service du Travail Obligatoire) pour lequel la défection est totale.

La maturité.

— 1943 : juillet, Jean Fleury réorganise les transmissions et, avec l'aide de Jean Roy, met en œuvre de nouvelles structures.

— La séparation de l'émission et de la réception qui raccourcit beaucoup le temps des vacances réduit le risque de repérage par la radiogoniométrie allemande. La réception en France est assurée par la procédure « Broadcast » sur appareils de TSF ordinaires ou récepteurs miniatures « Biscuit » spécifique maquis. Ce poste permettait de recevoir toutes les gammes d'ondes par changement de bobines. Il était livré avec une pile offrant basse tension et haute tension dans le même élément avec 30 heures d'écoute.

— Instauration de nouveaux plans d'émission radio avec grand nombre de fréquences, horaires, endroits, indicatifs indéchiffrables. Mise en place de « quartz » interchangeables qui stabilisent les fréquences avec plan de fréquences.

— Une Inspection Nationale des Transmissions est créée avec un inspecteur et un adjoint.

— 2000 émetteurs et 1000 quartz sont fabriqués et parachutés sur la France où Claude Wolf (« Indien ») assure le recrutement et la formation des opérateurs radios.

Les opérateurs radio.

— On compte 159 opérateurs qui ont travaillé depuis la réorganisation avec un pseudonyme représentant qui une ville, qui une nation, qui un peuple, etc. Plus de la moitié a été recrutée en France. Pour la période 1940-1942, plus de 75 % ont été arrêtés alors que pour la fin de guerre seulement 25 % ont subi l'allemand. Dans les deux cas, 50 % ne sont pas revenus des camps de la mort.

— Le volume du trafic passe de quelques câbles quotidiens en 1940 à 150 par jour en 1943. Pendant la dernière année de guerre, 50000 messages sont transmis...

POSTE BP3 : construit à partir de 1943 il équipe les centres secrets de l'I.S. Appelé aussi poste polonais, il était de facture robuste et puissant. Bien qu'encore un peu lourd, il permettait des liaisons intercontinentales.

Le 31 mai 1942 à 2 heures du matin...

Quel vacarme après le silence du ciel ! Je reste caché dans l'herbe haute, pistolet à la main — une balle dans le canon, cran d'arrêt ôté — scrutant l'ombre des haies, tendu, prêt à défendre chèrement...

Il n'y a là rien de méchant, seulement les hôtes naturels de l'endroit, que mon arrivée n'impressionne pas, à leur aise et célébrant l'Amour dans la tiédeur du Printemps, et qui s'appellent sous la lune : « Cigale chérie, je suis ici ! Grillon de mon cœur, viens ! Ma grenouille, ah, je meurs ! »

Il me faut détacher la valise des suspentes. Les instructions sont de faire un paquet du parachute, de la combinaison de saut et du rembourrage de protection de la valise, puis d'enterrer le tout : j'ai même la pelle idoine attachée à la jambe de ma combinaison de saut.

Mais la terre est bien dure et il fait bien chaud. La gare de Romanèche-Thorins doit être à une dizaine de kilomètres. Creuser un gros trou dans ce sol sec, puis traîner ma valise dans la chaleur de la nuit sur une telle distance, va m'épuiser et me faire remarquer : ça ne me semble pas raisonnable. Il vaut mieux cacher le tout et revenir chercher mon bagage plus tard.

Je fais une boule de l'ensemble — ayant, bien sûr, retiré le Paraset de la grosse valise : avoir un poste émetteur au bout des doigts est ma raison d'être ici — bien recouvert de tissu camouflage, que je fourre au plus profond d'un buisson, pas trop près, en prenant soin de ne pas laisser de trace qui puisse relier la cachette à l'herbe écrasée par mon atterrissage.

(Le Paraset était un émetteur récepteur simple construit par les alliés pendant la 2e Guerre Mondiale. Il était utilisé par les services secrets britanniques ainsi que par les résistants belges, hollandais et français).

La route est là, à côté du pré. Une borne : Thoissey 3 km. Chapeau pour la navigation !

La route serpente à travers Thoissey. La lune et les étoiles éclairent le chemin. Chiens stupides qui aboient, malgré mes semelles de crêpe. Volets clos de la gendarmerie. Je m'en voudrais de déranger le sommeil de ses occupants.

Des champs s'étendent de part et d'autre de la route. Je marche dans la nuit chaude, les yeux et les oreilles aux aguets, entouré par le bruit des conversations des bestioles, mon Paraset toujours à la main.

Une autre borne me dit que la gare de Romanèche-Thorins est à cinq kilomètres. N'est-il pas bien tôt pour y arriver ? Et si je dormais un peu dans ce petit bois ?

Radio-valise utilisée par les résistants

Il fait jour, c'est dimanche. Déjà on travaille dans les champs à étaler les meulettes du foin entassé pour la nuit. Petit déjeuner avec une ration de survie : il y a là une tablette d'un mélange de chocolat et d'extrait de bœuf déshydraté, sans doute très nourrissant. Ce métier exige une grande largeur d'esprit.

Je traverse la Saône. Soleil radieux. La gare de Romanèche-Thorins. « Un billet aller pour Uzès, s'il vous plaît. » Arrivée de la locomotive : gros soupirs de vapeur. Le wagon est plein de gens avec des colis, des sacs, des valises : tous parlent ravitaillage, de toute évidence le sujet de première importance.

Il me faut changer de train à Lyon. Dans la gare de Perrache, une équipe de gendarmes scrute la foule, demande l'ouverture d'une valise particulièrement grosse, ou les papiers de celui qui a vraiment l'allure trop louche. Moi, j'ai l'air d'un bon petit et ma valise est pas grosse : je passe sans encombre avec le flot. Il me faut aussi changer à Nîmes, mais là, pas de train pour Uzès avant le lendemain.

Lorsqu'au matin on frappe à la porte de ma chambre d'hôtel pour me réveiller, je réponds : « Come in ! » Ça n'est pas perçu.

À Uzès, je trouve mon contact, un ami d'André Diethelm qui me donne l'adresse de celui dont je dois être le radio : Jacques Soulas — SALM — chef d'une mission pour le Commissariat à l'Intérieur, et dont l'objet est de prendre contact avec des personnalités de la vie politique française pour essayer de les persuader de rejoindre le général de Gaulle, qui se trouve un peu seul en Angleterre.

J'ai connu Jacques Soulas à Londres. Il était de ceux qui, prisonniers de guerre dans l'Est de l'Allemagne, s'étaient évadés vers l'URSS proche, d'où ils avaient rejoint les FFL en Angleterre, et qu'on avait surnommés : Les Russes.

La plupart des chefs de mission en France : renseignements politiques, économiques ou militaires, organisation de parachutages et d'atterrissage, de sabotage, de propagande, d'évasion, etc., étaient accompagnés d'un opérateur radio — dans la mesure où, denrée rare, il y en avait de disponible pour assurer les communications avec leur base en Angleterre.

Jacques Soulas habite Lyon, 10 Montée des Carmélites, avec sa femme et ses enfants. Il a repris son travail aux Câbles de Lyon, une couverture impeccable. Retrouvailles. Des télégrammes arrivés par le truchement d'un réseau polonais lyonnais lui avaient annoncé mon arrivée.

Je cherche une chambre meublée. J'en trouve une du côté de Bron, au deuxième étage d'un pavillon de banlieue tout en hauteur. J'achète un vélo d'occasion, objet rare, mais indispensable, payé son poids d'or, que j'utilise aussitôt pour aller chercher la valise cachée sous son buisson de mon terrain d'atterrissage près de Thoissey. Je la retrouve sans difficulté.

J'achète aussi un poste de TSF, qui sera l'alibi pour demander à mon propriétaire la permission d'installer un fil d'antenne en travers de son jardin : « La réception est tellement meilleure, n'est-ce pas, avec une antenne. »

Pour lui, je suis étudiant en droit. J'essaie, sans grande conviction, de m'inscrire en faculté, mais mon manque de connaissance de l'université me fait craindre d'y être trop maladroit et de me faire remarquer.

Émotion lorsque je vais au service du Ravitaillement. Je présente la carte qui me donne droit à ma ration de tickets mensuels de ravitaillement. Elle a été imprimée à Londres, mais il est écrit dessus qu'elle a été délivrée à Paris. « Quelle drôle de couleur ! » dit la préposée. « Vous trouvez ? Elles sont toutes comme ça à Paris. — Ah bon ! » dit la dame. Et me donne mes tickets.

Aussitôt installé dans ma chambre, j'essaie d'établir le contact radio avec l'Angleterre. En vain. J'appelle à tous les rendez-vous, six fois par semaine, trois de jour, trois de nuit. C'est décourageant. Soulas, via le réseau polonais, signale à Londres mes efforts infructueux. Le 20 juin, l'opérateur de la Centrale se réveille : les premiers télégrammes

passent dans les deux sens.

L'auteur à Lyon 1942/43

Le Paraset, le poste émetteur-récepteur que j'utilise, a pour principales qualités d'être petit et léger. La partie récepteur, d'un type dit « à réaction », est sensible et permet de recevoir des signaux faibles, mais son réglage, un peu acrobatique, varie au gré des fluctuations du voltage de la ligne du secteur électrique, et de la proximité de la main de l'opérateur. Il est peu sélectif : une station puissante, voisine de la longueur d'onde de votre correspondant, matraque facilement vos tympans et rend difficile la lecture Morse.

L'émetteur a une faible puissance : 4 watts. Sur ondes courtes, ça n'est pas un gros inconvénient, d'autant plus que mon correspondant en Angleterre dispose de récepteurs sophistiqués et des immenses antennes de la Centrale, la « Home Station », STS 53A, située à Grendon.

Écoute rituelle, aussi et toujours, de la BBC, pour entendre les nouvelles de la guerre, sur ondes courtes aussi, bien sûr, malgré le brouillage intense des Allemands.

Merveilleuses ondes courtes qui permettent aux faibles de se jouer des puissants !

Pas grand-chose à faire. Le travail de mon patron génère peu de trafic radio : environ cinq télé par semaine. Grandes balades à vélo dans la campagne alentour. Mes muscles à bicyclette, inutilisés depuis l'été 40, fonctionnent toujours bien. Les routes sont vides et je transpire sous le soleil. Je vais me rafraîchir sur les plages de la Saône : j'y retrouve parfois mon patron, sa femme, ses enfants.

Je découvre Lyon, les Lyonnais à l'abord grincheux, les ouragans de poussière de la place Bellecour, les tramways antédiluviens et leurs rails néfastes aux cyclistes, les splendides chevaux de Carpeaux sur la place des Terreaux, la Tour Eiffel à courtes pattes, et sa voisine Notre-Dame de Fourvière qui, comme le Sacré-Cœur de Montmartre, ressemble à un éléphant sur le dos ; et les petits restaurants où, avec un peu d'argent, guerrier sans vergogne, je mange au marché noir et à ma faim.

Vie sur une autre planète qui a pour nom solitude. Rares rencontres avec mon patron, la sécurité exige le cloisonnement, on communique par « boîtes aux lettres ». Je vais bientôt avoir 22 ans, je n'ai aucun ami, aucune amie. Je ne peux, je ne dois parler de rien à personne. Comment esquisser un début d'amitié, d'intimité en se tenant sans cesse sur ses gardes ?

Vigilant, l'esprit doit veiller à ce que rien de ce que je fais ne dépasse de la norme, qu'aucun objet, aucune attitude ou parole puisse susciter la curiosité des autres. Et sans cesse il doit déceler, évaluer dans l'environnement les signes que livrent hommes, voitures, mouvements, anticiper les situations, et m'éviter la confrontation, me guider vers le calme. Mais la solitude...

Par une belle journée du mois d'août, devant la librairie Flammarion, Place Bellecour : Daniel Cordier. Nous étions ensemble à la STS 52, l'école des radios de Thame Park. Je revois, un dimanche qu'un groupe de Français Libres étaient allés déjeuner au George, un excellent restaurant d'Oxford, le chic fou de l'uniforme — bleu, filet jonquille — et du képi d'officier de chasseurs, faisant sillage dans la mer des battle-dress kaki. Esprit vif, sens de l'humour, original, la parole un peu zozotante, c'était un des plus agréables compagnons.

Chacun sur son vélo, un pied-à-terre, on se regarde, on regarde alentour, visages de joueurs de poker, le temps de peser la chose, de déceler ce qu'il pourrait y avoir d'inquiétant dans l'environnement.

La sécurité aurait voulu que l'on ne se reconnût point. Le plaisir de se revoir, de rompre la solitude méfiante de notre vie — enfin quelqu'un à qui parler sans crainte de faux pas ! — on rit, on déjeune ensemble chez Colette, place Antonin Poncet, un petit restaurant tenu par une blonde opulente. Colette a un ami inspecteur de police, ce qui assure la quiétude du lieu. On s'y retrouve souvent.

Daniel Cordier — BIP W — a été parachuté à la lune de Juillet 1942. Destiné à être le radio de Georges Bidault — BIP — il est kidnappé par Jean Moulin — REX — qui discerne en lui les qualités qui en feront le secrétaire sans pareil de la Délégation du Général de Gaulle en France jusqu'en mars 1944.

Il m'emmène rôder parmi les rayons de la librairie Flammarion. Orgie de lecture. Daniel me fait découvrir Les Thibault, La Chronique des Pasquier, Les Hommes de Bonne Volonté, Les Copains, À la Recherche du temps perdu, le Journal d'André Gide, etc., etc.. Quel monde je rencontre là !... Moi à qui, enfant, on interdisait de lire Poil de carotte !

Au théâtre antique de Vienne, on joue Antigone. Nous allons voir un soir, mais nous n'osons quand même pas aller souper chez Point ...

Le Secrétariat manque de moyens. Daniel a si peu d'argent qu'il a faim. C'est souvent moi qui paie nos steaks-frites de marché noir, puisque mon patron dispose de fonds plus abondants.

Un jour, place de l'Opéra, nous sortons d'un restaurant : Horreur ! Tragédie ! Le vélo de Daniel a été volé. Oiseau à qui on vient de couper les ailes, il contemple, effondré, le désastre. Circuler est vital au secrétaire de REX, le prix d'une bicyclette au marché noir est exorbitant, quelles acrobaties en perspective pour en trouver une autre...

Le Secrétariat manque de liaisons radio. Deux opérateurs : Jean Holley — LEO W — parachuté d'Angleterre, et un radio — BIP Y — recruté en France, essaient en vain de prendre contact avec Londres. Hervé Monjarret — SIF X — le radio de Raymond Fassin — SIF — qui avait été le premier radio à transmettre des télégrammes pour REX — a quitté les transmissions pour être officier de liaison auprès de Francs-Tireurs.

Gérard Brault — KIM W —, un autre ancien de Thame Park, arrivé en Juin 1942, pour être le radio de Paul Schmidt — KIM —, officier de liaison auprès du mouvement de résistance LIBERATION, reste seul à assurer le trafic de son patron et celui du Secrétariat de Jean Moulin : jusqu'à six heures d'émission par jour ! Il est surmené au-delà du raisonnable et obligé de prendre des risques absurdes.

Situation saugrenue : au même moment, j'écoute mes télé en quelques minutes par semaine. Si peu que je ne m'inquiète pas d'un avertissement venu de Londres : une équipe allemande de radiogoniométrie s'installe dans la région.

Des messages échangés entre Londres, Jean Moulin et mon patron, Jacques Soulas, organisent mon transfert du Commissariat à l'Intérieur vers le BCRA. À la mi-septembre, l'écheveau bureaucratique londonien se démêle, et je passe au service de la Délégation du Général de Gaulle en France, où je commence par soulager Gérard Brault des télé de Georges Bidault, nombreux et longs.

Émission plusieurs heures par jour, parfois jusqu'à cinq ou six, de ma chambre à Bron, le jour. Les cristaux de quartz qui devraient me permettre d'utiliser mes fréquences de nuit sont défectueux. REX est conscient du danger ainsi couru par son nouvel opérateur, et donc par ses transmissions. Il voudrait bien améliorer mes conditions de travail, mais n'y parvient pas.

Il faut que le trafic passe. Il passe. Depuis l'âge de seize ans, radio amateur, je pourchasse les signaux rares et lointains sur des postes de ma fabrication. J'aime ce jeu qui allie l'acuité de l'ouïe à la subtilité technique, et lorsqu'en face de moi se trouve un opérateur de haut vol pour capter les quelques micro volts que je lui lance, écouter les télégrammes est un plaisir : satisfaction du travail bien fait, plus celle de David qui fait un pied de nez au Goliath Chleuh.

L'expansion fantastique des services radioélectriques en Angleterre crée une demande de personnel difficile à satisfaire. Il faut du temps pour former un opérateur. C'est une chose de lire le Morse dans une salle de classe, et c'en est une autre d'extraire ce minuscule signal de la jungle électromagnétique. Tous, l'armée, la Royal Air Force, la Royal Navy, les services secrets, se battent sauvagement pour avoir des radios. Notre centrale parfois bouche les trous avec des apprentis : rendez-vous manqués, répétitions lassantes, dangereuses — plus longue est l'émission, plus facile le repérage — dialogues de sourds, erreurs.

La température monte, la patience diminue : « La gonio est dans la rue et ces cons-là prennent le thé ! »

On décoche des télégrammes furibonds à l'adresse de la Home Station : « Je ne veux plus travailler avec l'opérateur du 2 août ses signaux sont illisibles ! » — « L'opérateur d'hier ne savait pas manipuler les chiffres 2, 3 et 4... » Moulin s'impatiente : « Voulez-vous demander aux Anglais s'ils se moquent de nous ? »

De l'autre côté, ils ne sont pas contents non plus : « Réduisez la durée de vos émissions qui sont beaucoup trop longues. Rappelons qu'EEL ne doit pas prendre contact tous les jours ni plus d'une heure... »

Ils n'ont pas tort : le principe, enseigné à l'entraînement en Angleterre, d'une demi-heure trois fois par semaine est devenu ici la pratique de plusieurs heures par jour. Je proteste bien auprès de ceux qui me submergent de télégrammes. « Il faut que ça passe ! Tu serais dans une tranchée avec une mitrailleuse en face de toi, tu refuserais d'aller à l'assaut parce que c'est trop dangereux ? » Je suis meilleur radio que dialecticien, alors je continue à émettre trop longtemps.

De Londres, début octobre 1942 : « BRANDY est en panne, aidez-le. » BRANDY est un réseau d'évasion conçu par le lieutenant d'aviation Christian Martell, qui est parti pour l'Angleterre en décembre 1941. Se rendant compte du grand besoin en mécaniciens de la Royal Air Force, il offre de revenir en France pour en recruter. Parachuté en avril 1942, il établit, avec l'aide de ses amis d'avant la guerre, une filière d'évasion qui part de Paris et va en Espagne. Avec le premier groupe de mécanos, il retourne en Angleterre rejoindre son escadrille, et laisse la direction du réseau à son frère Maurice (SIMON), qui ajoute au recrutement de mécaniciens d'aviation l'évacuation d'aviateurs alliés rescapés après que leurs appareils eussent été abattus lors de missions au-dessus de l'Europe.

L'adresse est Cours Gambetta. Il y a là un jeune radio, Jean-Louis Mérand, parachuté de Londres en août 1942, et qui ne parvient pas à prendre contact. Le poste qu'il possède est défectueux. Son plan d'émission — microphoto où figurent ses heures de rendez-vous, ses fréquences et ses indicatifs d'appel — a pour nom de code AMBRE. Je l'essaie sur mon poste. Cette fois encore, c'est évident, la Centrale n'est pas au rendez-vous. J'envoie les télé de SIMON sur mon plan.

Chez les radios, il ne s'est rien passé d'inquiétant depuis longtemps. La pression pour transmettre les télégrammes est intense. Le soutien logistique nécessaire — réseau de lieux pour émettre chaque fois d'un endroit différent, équipes de protection pour surveiller les alentours — est inexistant. Les comportements imprudents glissent vers l'absurde. Pendant ce temps la gonio Chleuh écoute et s'approche...

Radiogoniométrie.

Les Allemands sont entrés en zone « libre » avec un service spécial pour la détection des émetteurs clandestins, le Sonderkommando Kurzwellenüberwachung, le KWU.

DONAR est le nom de code de l'opération. Donar, dieu de la foudre dans le Walhalla, a été bombardé saint patron de la chasse aux radios clandestins. Cent six hommes, sept appareils de gonio mobiles montés sur camion ou sur quelques-unes de leurs 35 voitures. Leur « protection » est assurée par des inspecteurs de la Sureté Nationale française. L'appareil de radiogoniométrie est muni d'une antenne spéciale qui permet de relever la direction d'où provient une émission. Trois appareils, travaillant ensemble, mais

éloignés les uns des autres permettent de porter sur une carte trois relèvements qui se recoupent et dont l'aire de rencontre dessine un triangle. C'est là qu'est l'émetteur recherché. Les chasseurs s'en rapprochent, réduisant peu à peu la taille du triangle où se trouve leur proie. Finalement, gonio légère à la main, ils font du porte-à-porte, et c'est la curée.

Aux alentours du mois d'octobre 1942, les Allemands repèrent, et les policiers français arrêtent, dans la région lyonnaise, un radio polonais et deux anglais. Le 16 octobre, c'est le tour de Gérard Brault — KIM W.

Un autre jour d'octobre, vers 17 heures, au cours d'une liaison, alors que je passe à l'écoute de la Centrale après lui avoir transmis un télé, je l'entends, à peine, me dire ne m'entend plus du tout.

La propagation est chamboulée.

La propagation des ondes courtes est aléatoire. On peut, en général, compter sur elle pour franchir une certaine distance, si on choisit bien son heure et sa longueur d'onde. Mais de temps à autre un phénomène, exceptionnel — aurore boréale, tache solaire, orage magnétique, etc. — peut brutalement tout modifier.

Les instructions reçues en Angleterre m'ordonnaient de toujours conduire mes émissions comme si je menais une station commerciale. Habituellement respectueux de ces règles, j'aurais dû, puisque la liaison n'était plus possible, envoyer le signal : QRT de WNG104, et fermer la station. Paresseux ? Sixième sens ?

Ce jour-là je n'ai rien transmis.

Le Paraset rangé, puis caché sur le haut d'une armoire — comme on m'avait appris à le faire à l'école de radio — l'antenne transférée sur le poste de TSF-alibi, qui me donne un peu de musique, et je m'allonge sur le lit, un livre à la main.

Cavalcade dans l'escalier. Grands coups cognés dans la porte, qui s'ouvre violemment. « Police ! Haut les mains ! » Une dizaine de mecs, pistolet au poing. On se croirait dans un film. Il est évident qu'ils ont l'air surpris d'avoir devant eux un même, qui du lit où il était allongé, se redresse, l'air étonné, un bouquin au bout d'un de ses bras levés. Avec mon visage rieur, je fais plus jeune que les 18 ans de mes papiers d'identité. Ils fouillent, me fouillent, feuilletent les livres, cherchent sous le lit, sous le matelas, sous l'armoire, dans l'armoire...

On voit bien à leur figure qu'ils se sont trompés. La plupart ont l'air allemand, certains sont Français. Un des Chleuhs ne me quitte pas des yeux, des yeux gris, durs. Je n'ai vraiment pas l'air d'un espion, avec mes shorts, mon grand col ouvert et mon sourire de bonne volonté : « Que cherchez-vous donc ? Je peux peut-être vous aider ? » L'un d'eux a trouvé un papier sur ma table. Menaçant : « Ach ! Qu'est-ce que c'est, Monsieur ? — Ben, heu, vous voyez, c'est la liste des postes avec l'heure où ils donnent des nouvelles. Là, Radio-Paris, la Suisse romande, Stuttgart, la BBC... » Mais ils cherchent autre chose qu'un auditeur de la radio anglaise. Après un dernier coup d'œil, ils s'en vont.

Si je suis novice et naïf à ce jeu, eux aussi. Sur ma table : un quartz — ce cristal qui sert à stabiliser l'émission sur sa fréquence — oublié lors du rangement... Petit parallélépipède noir, qui leur faisait un clin d'œil qu'ils n'ont pas perçu.

Assis sur le lit, un tremblement irrésistible me saisit. Piégé par mes multiples infractions aux règles de sécurité (infractions obligées par le manque de soutien logistique : émissions beaucoup trop longues,

beaucoup trop fréquentes, toujours du même endroit, sans personne pour surveiller les abords), j'ai été QRT signifie : j'arrête mes transmissions, et WNG était l'indicatif de ma station. sauvé par une autre infraction, à la règle qui voulait que l'on se donne l'attitude d'une station commerciale : Dans la rue, l'équipe du KWU attendait, pour affiner son relèvement, que je revienne sur l'air.

Pendant ce temps je rangeais. Si j'avais, selon la règle, annoncé la fin de mon émission, ses hommes auraient aussitôt bondi, sans me laisser le temps de rien cacher. Ainsi retardés, les Chleuhs fouillent, sans certitude, une demi-douzaine de maisons le long de la rue.

En bas, dans sa cuisine, mon propriétaire est en proie à sa propre trouille : il vient de rentrer un sac de 50 kg de blé acheté au marché noir et il croit être la cible de ces messieurs. Comme ça lui donne l'air coupable, ils lui démontent quelques meubles.

Le calme revient. Je sors faire le tour du voisinage. Ils sont bien partis. Je descends le Paraset et mon pistolet du haut de l'armoire. Les sacoches pleines, j'enfourche mon vélo, pour ne plus jamais revenir.

Le cloisonnement avec le secrétariat est excellent. Nous n'avons de contact que par boîte aux lettres interposée, lorsque je n'ai pas de rendez-vous avec Daniel Cordier. Ils ne connaissent pas mon adresse, je ne sais pas la leur. Seuls endroits où je pourrais me réfugier : chez Jacques Soulas — SALM — mon ex-patron, ou chez Maurice Montet — SIMON — dont je viens de dépanner les transmissions. C'est lui que je choisis, car aller faire des vagues chez Soulas et déranger son excellente couverture, sa femme, ses enfants, ne me paraît pas indiqué. Pour être sûr de n'être pas suivi, je tourne, virevolte et traboules dans Lyon. Atterrissage cours Gambetta, accueil, épiluchage et examen des événements. Pour l'instant, je peux manger et dormir là.

Au Secrétariat, on n'est pas heureux. Après l'arrestation de Gérard Brault, et mon esquivage de la gonio, ils n'ont plus de liaison radio avec Londres. Un rendez-vous de repêchage — mis en place, justement, pour se retrouver lorsque les choses dérapent — me permet de reprendre contact avec Cordier. Mais ils n'ont toujours pas le moyen de me fournir un lieu sûr où habiter, ni des emplacements d'émission. La Résistance à qui on les demande, est sans doute occupée à répandre ses tracts.

Je passe un accord avec Maurice Montet, le patron du réseau BRANDY. J'assure ses transmissions, pas lourdes, mais qui lui sont précieuses, et il me fournit des points d'émission le long de sa filière d'évasion. Nous avons, son groupe et moi, des atomes crochus : j'habite avec eux. Leur ravitaillement est bien organisé, ce qui évite de s'exposer dans les restaurants.

En vérité, il n'est pas très orthodoxe de mélanger ainsi deux réseaux. Mais il faut faire avec ce que l'on a. Les volontaires aux côtés des Français Libres sont encore rares. Les gens ne croient guère à cette chimère qui nous agite : foutre dehors le tout-puissant Grand Reich.

« Ils ont battu tout le monde, pensez donc, même les Français ! » et « Pétain est un grand bonhomme ! », sont les clichés qui permettent de ne rien faire avec bonne conscience. Il faudra le débarquement américain en Afrique du Nord, et surtout la déroute de Stalingrad, pour que commencent à se réveiller ceux que leur bon sens avait engourdis.

La filière BRANDY traverse la ligne de démarcation près de Chalons-sur-Saône, avec l'aide de l'équipe d'André Jarrot, garagiste, ancien coureur motocycliste, de Raymond Basset, capitaine des sapeurs-pompiers, et de Pierre Guilhemon.

Je descends du train à Tournay. Dédé Jarrot est là. Je monte derrière lui sur sa moto, la valise du poste émetteur entre nous. On part à travers la campagne. Une ferme. Accents bourguignons : « Je vous ai apporté la chambre à air que vous vouliez pour le vélo de la p'tite. On pourrait pas s'installer une demi-heure dans un coin ? »

(Copyright (c) Maurice de Cheveigné)

En dehors de son charme bourguignon débordant, Dédé Jarrot savait la façon de s'attirer la bonne volonté des populations.

Étant garagiste, il pouvait importer de zone occupée des pièces détachées de vélo, à condition d'y exporter ensuite la quantité de vélos assemblés correspondante. Ce qu'il faisait consciencieusement. Mais dans le noir de la nuit, quittant sa casquette de garagiste pour celle de contrebandier, il ramenait quelques vélos en zone libre. Puis plus tard, redevenu garagiste, il les représentait une deuxième fois à la ligne de démarcation, obtenant ainsi, avec les mêmes bicyclettes, un nouveau crédit de pièces détachées ! Un excellent matériau d'échange...

Piratage et écoute d'une base TSF :

Beaucoup de français moyens utilisent des téléphones sans fil en le raccordant tout simplement sur une prise téléphonique. Il est possible de le raccorder aussi sur le joncteur d'une ligne analogique derrière un PABX. Que ces appareils soient homologués ou non, le principe de fonctionnement est le même pour tous sans exception.

La généralisation de ce type de matériel pose un grand problème en matière de confidentialité des communications. Les utilisateurs non avertis ignorent bien souvent que tout ce qu'ils disent à leur correspondant peut être intercepté par des récepteurs de surveillance radio larges bandes. Ils comportent souvent un dispositif, qui permet de déclencher un magnétophone automatiquement. On peut se demander légitimement aussi, si la généralisation de ce moyen de communication, n'est pas une volonté de nos gouvernements. Le but est de permettre aux grandes oreilles (stations de surveillance radioélectriques gouvernementales), d'espionner la vie des citoyens moyens, afin de connaître leurs aspirations ou préoccupations du moment, ou même leurs opinions politiques. Ces écoutes anodines, permettent de savoir à la veille d'élection, ce que la population pense de ses politiciens et de compléter les sondages.

En dehors des écoutes, il existe d'autres aspects encore plus sournois. Des particuliers peuvent appeler leur banque pour connaître la position de leur compte. Ils peuvent aboutir sur des serveurs vocaux qui peuvent leur demander de composer leur mot de passe et code confidentiel. Le téléachat à distance à travers ces serveurs commence à se développer en France. Les particuliers non techniques imprudents peuvent ainsi transmettre le numéro de leur carte bancaire par T.S.F. pour commander quelque chose.

Un individu en possession de ce type de récepteur, voire même d'un poste CB fonctionnant sur la bande A (ce qui correspond au double inférieur) peut intercepter de multiples communications téléphoniques. C'est ainsi que l'on peut voir des pirates en possession de numéros de carte bancaire qu'il ne devraient pas avoir. Ils peuvent ainsi passer des commandes pour leur propre compte qui seront payées par d'autres à leur insu.

Il faut savoir qu'aucun T.S.F. homologué en France ne peut être crypté. Ceux qui le sont viennent de l'étranger et sont interdits d'utilisation. Pour l'instant, on peut supposer que les écoutes systématiques ne sont pas utilisées par les groupes, ou seulement de façon occasionnelle. Mais rien n'interdit ce développement illicite.

Alors est-il normal que les vendeurs de ces matériels n'informent pas les acheteurs potentiels des risques possibles. On ne voit pas pourquoi il n'existerait pas un décret obligeant les fabricants à écrire sur leurs notices que la confidentialité des communications n'est pas assurée sur ces appareils. Pourquoi il n'est pas déconseillé ou même interdit d'utiliser ces appareils pour des transactions que l'on peut qualifier de financières. Par exemple, pour les jeux vidéo une mise en garde figure sur toutes les notices afin de mettre en garde les épileptiques sur les effets secondaires. Ce moyen de communication est le pire qui puisse exister. Il a en effet permis sur Paris un grand nombre de fuites dans tous les domaines, qu'ils soient politiques, financiers, industriels, scientifiques, voire même militaires. Il ne faut pas oublier que les ambassades sont des grandes oreilles

en puissance. Certaines disposent d'antennes assez remarquables, pour que l'on en devine leur utilisation.

Transmissions informatiques radio sans fil :

Les fonctionnaires de Bruxelles viennent de définir la norme IEEE 802.11 pour l'Europe). Elle consiste à autoriser les ordinateurs ou autres systèmes à communiquer entre eux de 0,3 à 1,35 Mbit/s dans la bande de fréquence de 2446,5 / 2483,5 MHz.

Deux techniques sur cette bande se dégagent. L'une est à fréquence fixe (DSSS) et l'autre à sauts de fréquence (FHSS). Cette dernière paraît un peu plus sûre que la première contre un risque d'écoute.

Mais de toute façon quoiqu'en disent les divers constructeurs du marché, ces solutions seront toujours moins sûres qu'une liaison par câble face à des espions.

Il faut en effet savoir que la cryptographie lourde est assimilée à une arme de guerre en France, comme dans beaucoup d'autres pays et est donc interdite. Les communications transiteront donc en clair et pourront être interceptées par n'importe quel récepteur fonctionnant sur la bonne fréquence.

Utilisé conjointement avec un analyseur de protocole ou encore ces nouveaux équipements appelés sniffers, un pirate pourra intercepter les adresses IP, les informations transitant sur un réseau.

La norme ETS300-652 (Hiperlan: High Performance Radio Lan) disponible depuis 97.

Ces systèmes utilisent les 5 et 17 GHz avec un débit de 10 à 20 Mbit/s.

Ces moyens présentent les sérieux inconvénients d'être écoutés sans aucune restriction comme pour les téléphones sans fil. Le pire, c'est que l'on ne saura jamais si effectivement toutes les données ont été captées par un espion. On peut donc supposer ici aussi qu'il y a une volonté des gouvernements, d'espionner ce qui transite sur les systèmes informatiques, sans connexion physique.

Le danger vient surtout de la possibilité de leurrer le correspondant initial et d'émettre à sa place un signal HF qui pourra comporter sous-programme invisible d'espionnages.

Ce type de programme généralement en assembleur ira se camoufler quelque part sur le disque dur et demeurera invisible même lors du listage du contenu du disque. Il attendra le moment opportun pour se charger automatiquement de lui-même. Il transmettra tout seul vers son propriétaire la première fois tout le contenu du disque dur.

Les fois suivantes, il se contentera de transmettre les nouveaux fichiers qu'il a réceptionnés d'un autre système informatique autorisé. Il émettra aussi les informations ou les ordres tapés sur le clavier qu'il stockera dans un fichier tampon en attendant l'heure d'émission.

Ce programme fera le nécessaire afin qu'il ne figure aucune modification ou trace dans le fichier historique. Il y a cependant deux problèmes qui permettent de visualiser ce genre de supercherie. Un autre ordinateur superviseur sur le site peut détecter l'activité du modem radio. L'autre problème peut apparaître lorsque le disque dur de l'ordinateur espionné est pratiquement plein. Si on souhaite enregistrer sur le PC un fichier 10 Mega-octets et que ce dernier vous dit que c'est impossible, alors qu'il nous signale qu'il reste une capacité disponible de 20 Mega-octets, on peut se poser des questions. Il y a dans ce cas un ou des fichiers invisibles quelque part.

Matra Grolier Network se lance aussi dans la bagarre du sans fil, en proposant ici des moyens de communication Internet par satellite pour un débit de 500 kilobits avec un tarif très intéressant. La société israélienne RDC propose un système complet de communication sans fil pour Internet sur 2,4 GHz.

Il permettrait d'évincer les opérateurs habituels du câble. Le fournisseur d'accès installe sur son serveur une passerelle qui est raccordée à une antenne omnidirectionnelle sur le toit. La portée possible serait un rayon de couverture de 35 km en fonction du relief avec un débit de 1 Mbit/s. L'abonné ou l'entreprise disposerait d'une antenne parabolique bidirectionnelle de 10 à 20 décibels avec un angle d'ouverture de 14 à 40° connecté sur une Unité de Communication Principale et raccordé à son réseau local. Il y a ici aussi des risques d'interception des transmissions avec des systèmes fonctionnant d'un côté en omnidirectionnel et de l'autre en bidirectionnel pour l'UCP, et omnidirectionnel pour les boîtiers. L'Internet par ces moyens, n'a qu'un objectif, court-circuite les opérateurs nationaux, en proposant des tarifs très bas. Malheureusement, tant que la cryptographie lourde ne sera pas autorisée, ces moyens sont voués à l'échec pour les sites ou sociétés très sensibles, et c'est valable pour n'importe quel fournisseur français ou étranger.

Les faisceaux hertziens :

Les communications micro-ondes se généralisent de plus en plus. L'intérêt réside dans le fait qu'ils permettent de relier deux sites entre eux sans passer par des câbles. Ils permettent ainsi le transfert de grosses quantités d'information numériques et analogiques dans des zones isolées ou ayant un fort relief accidenté. L'inconvénient, ici c'est que ces types de faisceaux peuvent être écoutés surtout par les services d'espionnage de gouvernements étrangers. Dans ce cas précis, ils préfèrent enregistrer toute la largeur de bande du faisceau et procéder au triage par analyse, ou sélection de mots-clés. Ils utilisent les fréquences ci-dessous :

- 1,5 GHz / 8 voies,
- 4,5 GHz / 1 voie à 2 Mbit/s,
- 8,5 GHz / 1 voie à 2 Mbit/s,
- 10 GHz / 8 voies ou 2 Mbit/s
- 13 GHz / 4 voies à 2 Mbit/s,
- 23 GHz / tout type, distance : 20 km.
- 31 GHz / 4 voies à 2 Mbit/s,
- 38 GHz / 4 voies à 2 Mbit/s, distance : 08 km.

Une chose que l'on sait moins, c'est que ces interceptions peuvent se faire par des satellites très sensibles spécialisés dans ce domaine. Les micro-ondes ont la particularité de se propager en ligne droite. Il est évident qu'il ne s'agit plus ici de travail d'amateur avec quelques milliers de francs, mais d'organisations avec des millions pour ne pas dire des milliards de dollars d'investissement. Si nous restons sur un plan terrestre, il est possible d'intercepter ces faisceaux avec des moyens moindres et de procéder à des réacheminements. Les spécialistes comprendront la méthode, il est inutile que de rentrer dans les détails.

Transmissions informatiques infrarouges (IR) :

Ces systèmes répondent à la norme IrDA1.1 permettant un débit de 115,2 Kb/s. La nouvelle norme Fast IrDA1.1 autorise un débit de 4 Mb/s et est utilisée par l'ordinateur portable Toshiba Satellite Pro 420. Mais il a un coût qui est malheureusement dissuasif.

Elles sont suffisamment intéressantes pour être mentionnées. Elles présentent l'inconvénient de ne pas franchir les murs ou autres obstacles qui se trouveraient dans son champ de vision. Mais c'est peut-être aussi un avantage. Les signaux ne pouvant franchir ces murs ne pourront être interceptés illégalement par un concurrent. De plus, nous ne sommes pas confrontés aux interférences entre les divers systèmes.

Il faut se rappeler que la HF et l'informatique ne font pas bon ménage ensemble. Les systèmes sans fil les plus pratiques pour les utilisateurs sont pour commencer les souris, les tablettes et les claviers comme ceux de Keytronic. Ensuite on a des portables comme Compaq ou Toshiba qui intègrent un module de transmission IR autorisant un débit de 1 à 4 Mb/s.

La société AB SOFT vend des modules que l'on peut raccorder sur les prises séries des ordinateurs et sur les prises parallèles des imprimantes.

EXTENDED SYSTEM commercialise la gamme Jeteye qui comporte des modules IR pour Ethernet en 10base T, 10base 2, pour port série et parallèle.

Certains dispositifs utilisant le procédé infrarouge sont utilisés aujourd'hui à des fins d'espionnages.

Ces systèmes permettent d'écouter les dialogues dans une pièce à condition que les diodes d'émission infrarouges puissent être orientées vers l'extérieur par une fenêtre. Ce type de signal contrairement aux ondes radio ne passe pas à travers les murs.

Les gadgets d'espionnage électronique

Les microémetteurs :

Il existe une multitude de moyens miniaturisés proposés dans les revues d'électroniques ou spécialisées dans la sécurité. Certaines boutiques dans des galeries situées sur les Champs Élysées proposent ce genre de matériel. Ils utilisent généralement une fréquence dans la bande FM. Ces gadgets peuvent être dissimulés dans les murs, le mobilier, l'installation électrique, téléphonique, informatique et même la plomberie. Pour ce dernier cas, je ne rentrerai pas dans les détails. Il n'est pas utile de donner des idées.

On les trouve sous les formes les plus diverses et parfois inattendues.

- sucre sur ligne PTT, - sucre sur ligne EDF,
- pastille téléphonique, - stylos émetteur,
- calculatrice émettrice, - bague émettrice,
- livre émetteur, - bouton émetteur,
- agendas émetteur, - montre émettrice,
- téléphone émetteur, - ou même combiné émetteur,
- prise PTT émettrice, - multiprise émettrice,
- prise EDF émettrice, - horloge émettrice.
- câble dont l'émetteur est dissimulé dans la gaine.

Tous les systèmes ci-dessus existent. Le fin du fin consiste à disposer d'un microémetteur que l'on déclenche sur commande afin de rendre la détection de ce type de matériel plus délicate. Mais si pour déclencher l'émetteur, on utilise un récepteur de radio-télécommande si je puis dire, son oscillateur local s'il est mal blindé va rayonner lui aussi une infime énergie, qui risque de trahir sa présence.

Dans le cas du téléphone, la dissimulation et la mise en route sont plus faciles.

L'émetteur ne peut se déclencher que lorsqu'on décroche le combiné, si on ne souhaite intercepter que les communications téléphoniques. On intercepte ensuite les conversations jusqu'à une centaine de mètres ou plus, tout dépend de la puissance du sucre émetteur et des obstacles présents, avec un récepteur radio équipé d'un enregistreur minicassette. Ce dernier ne se déclenchera que si le sucre émetteur capte une voix dans le local ou il se trouve.

Une autre méthode consiste aussi à piéger les équipements d'instrumentations destinés à un laboratoire.

L'intérêt de ce moyen consiste surtout à réémettre numériquement vers l'extérieur en priorité les résultats des expérimentations en cours du laboratoire. Si on allume l', on assimile ainsi les signaux captés à la multitude d'oscillateurs, d'horloges du système. L'appareil stoppé, l'émetteur est indétectable.

Les caméras CCD :

La nouvelle technologie miniaturisée permet l'utilisation d'appareils photographiques, mais aussi de caméras CCD miniatures dont les dimensions n'excèdent pas un cube de 25 mm de côté. Il y en a de plus petites encore, mais plus rares à des prix exorbitants et réservées pour des applications spécifiques comme dans le domaine microchirurgical. Elles peuvent être couplées à un émetteur d'une portée de 50 à 300 mètres. Ce type de matériel est généralement dissimulé dans un objet d'ornement qui sera installé sur un bureau, une cheminée, un buffet. On les trouve aussi intégrés sous les formes ci-dessous avec un émetteur. Leur réalisation est évidemment plus complexe et coûteuse. Leur utilisation ne se fait donc que dans les cas vraiment extrêmes.

- pommeau d'une canne
- dans une broche,
- dans une cravate,
- dans une montre,
- une horloge,
- une mallette,
- un livre,
- derrière un miroir sans tain,
- un objet d'ornement
- un radar infrarouge.
- caméra cachée dans un mur avec canne endoscopique,
- même dans des détecteurs incendie raccordés à une centrale de gaz halons, ce qui est ridicule et interdit, car ce type d'installation est soumis à des contrôles annuels obligatoires. D'ailleurs à plusieurs reprises des faux détecteurs ont été trouvés avec une caméra dans certaines entreprises déclenchant le mécontentement des syndicalistes. Ce qui est justifié.

Par contre, sur des sites sensibles, des centres de recherche, les accès aux laboratoires et non pas l'intérieur, ce genre de système me paraît parfaitement justifié. Ces espions optiques peuvent être repérés par un dispositif qui détecte le signal de balayage de ligne des caméras. Ce genre de matériel est plus rare, car il a un coût, un volume, et une consommation non négligeable malgré sa miniaturisation. Il faut cependant savoir que ce type de matériel existe. Nos dirigeants d'entreprises sensibles ne sont pas toujours préparés à ces nouvelles menaces, surtout face à des concurrents étrangers virulents dans le domaine militaire ou scientifique. Ce genre d'affaires n'est d'ailleurs pratiquement jamais dévoilé au grand public. La détection de l'émission HF se fait avec les mêmes moyens que pour les sucres émetteurs. Les spécialistes de ces activités sont souvent électroniciens et sont des as de la débrouille.

Des moyens variés :

D'autres méthodes consistent à utiliser des dispositifs d'émission et de réception infrarouge. L'inconvénient, c'est qu'il ne fonctionne qu'en portée optique, c'est-à-dire que si une personne passe devant ou qu'elle met un meuble sur la trajectoire du faisceau, elle coupe la transmission. Ils ont par contre l'avantage d'être indétectable, car même un radioamateur ne dispose pas de récepteur IR et il faut être dans l'axe de ce type de système. Bien que discret il est peut employé en raison de cette contrainte de portée optique. Il y a aussi des moyens non électroniques originaux dont certains sont connus des Russes depuis longtemps. Il y a le principe de la résonance d'un matériau. Un cendrier de cristal réalisé avec le matériau approprié et taillé d'une certaine façon peut vibrer en fonction des sons générés dans le local où il se trouve. Il peut vibrer de la même façon qu'un diapason dont le son sera modulé par les personnes qui parleront à côté. La qualité et la portée sera médiocres évidemment, mais c'est le genre de truc que l'on peut trouver dans les cas extrêmes. Il est évident que les détecteurs habituels de micro ne servent pas à grand-chose. On peut aussi utiliser des matériaux ferromagnétiques très denses qui donneront un résultat équivalent.

Un moyen plus connu concerne la réflexion d'un faisceau laser sur la vitre d'une fenêtre. La vitre vibre en effet en fonction des bruits générés dans le local. Après traitement du signal réfléchi, on peut écouter ce qui se dit dans un bureau. Les paroles sont des vibrations sonores qui excitent les vitres modulant en même temps le faisceau du laser. Le petit problème c'est que dans le cas d'un double vitrage, le système devient inopérant. Un autre moyen repose sur l'utilisation des micro-ondes. Ce qui peut s'appliquer à un faisceau laser, peut aussi s'appliquer à des hyperfréquences dont une partie de l'énergie traversera les obstacles. Si entre deux obstacles il existe une vibration sonore, les micro-ondes récupérées de l'autre côté, auront subi une modification lors de ce passage. Je ne rentrerai pas plus dans les détails. Ce moyen n'est pas sans effet sur la santé. Systèmes informatisés d'interception radio :

Nous arrivons ici dans la dernière génération d'équipement.

L'évolution technologique, l'informatique, le traitement numérique, permettent l'intégration de plusieurs fonctions pour le même coût. C'est maintenant la qualité des logiciels intégrés qui permet de faire la différence surtout au niveau des tarifs.

L'élément primordial est un châssis d'ordinateur dans lequel on va intégrer des interfaces d'interception radio. Le tout sera piloté par un ou plusieurs sous-programmes.

L'interface utilisateur standard de base est aujourd'hui le système Windows. Habituellement un système radio ou de mesure disposait d'une façade avant avec des boutons fixes immuables. Chaque appareil remplissait une fonction bien précise. Aujourd'hui, ce n'est plus le cas. Le principe modulaire permet de disposer d'un châssis dans lequel on rajoute des modules spécialisés. Le tout est ensuite piloté par une unité de traitement externe, un PC avec Windows sur lequel on fait apparaître les commandes nécessaires aux besoins du moment.

La façade d'un récepteur radio, d'un mesureur de champ, d'un système gonio, se retrouve ainsi affiché sur un écran d'ordinateur.

Il est évident que tout le matériel de laboratoire cité ci-dessus, bien qu'il soit destiné à la mesure ou l'étalonnage des systèmes, permet l'interception de pratiquement tous les types de communications. Un groupe et d'autres, disposant de spécialistes peut être tenté d'utiliser tous ces moyens à des fins d'espionnage pour contrer la concurrence. Face à des marchés porteurs qui se chiffrent aujourd'hui à plusieurs centaines de millions de francs, le risque de ce genre d'activité va en grandissant et semble être utilisé en raison de la baisse des prix, de la disponibilité du matériel, de son ergonomie et ses facilités d'utilisation.

Les capitales qui ont des ambassades et des consulats, sont les plus exposées à ces interceptions. C'est pour cette raison que tous les moyens sans fil représentent un danger pour les utilisateurs, qu'ils soient des particuliers ou des officiels. Quel est le juge, policier ou avocat qui pense à demander à son correspondant s'il utilise un téléphone sans fil ou poste fixe. Les moyens sans fil utilisés dans les villes où sont installées des ambassades, sont à l'origine d'un très grand nombre de fuites.

Les moyens d'enregistrement radio :

Les systèmes sophistiqués de réception radio comportent tous des sorties, prise d'écoute et prise de magnétophone. Ils disposent aussi de plusieurs prises FI (fréquence intermédiaire) standardisées aujourd'hui à 30 KHz/ 75 KHz/ 1,44 MHz/ 10,7 MHz/ 21.4 MHz. Cela permet le raccordement d'enregistreurs audio de divers types avec des durées variables qui s'échelonnent de 1 à 25h par piste à diverses vitesses. Les baies conventionnelles d'ancienne génération équipées de deux magnétophones de 40 pistes chacune avaient des durées de 25h. Maintenant on trouve des systèmes moins volumineux capables d'enregistrer la même capacité sur une bande vidéo. D'autres systèmes plus sophistiqués permettent d'enregistrer à partir de la FI tout une partie du spectre radio. La sortie FI d'un récepteur radio est envoyée vers l'entrée d'un convertisseur qui permet d'abaisser la fréquence d'une partie du spectre pouvant atteindre de 1 à 10 mégahertz, ensuite ce signal arrive sur un enregistreur large bande. Cette solution permet de traiter les données ultérieurement sur place ou ailleurs. Il suffit de repasser la bande en reconvertissant le signal dans l'autre sens et de l'envoyer vers l'entrée FI d'un récepteur ou d'un système d'analyse. On utilise aujourd'hui des ordinateurs de plus en plus sophistiqués et rapides. On peut donc enregistrer du son ou de l'image sur disques durs à ou autres supports à condition qu'il dispose des interfaces d'entrées nécessaires, comme la reconnaissance vocale. Ensuite s'il dispose de logiciel de traitement ou d'analyse de la voix, on peut lui demander de mettre à part les communications téléphoniques ou radio contenant des mots-clés particuliers. Il pourra au besoin transcrire la langue écoutée en texte. Ce texte pourra être classé dans un thème et traduit par un logiciel dans une autre langue. C'est dans ces cas précis que des logiciels d'analyses basés sur le langage-pivot comme Taïga trouvent leur intérêt. Il est en effet impossible à un opérateur d'écouter des centaines de conversations françaises ou étrangères sans des artifices. Ils permettent ainsi de faire un tri très sélectif et de ne retenir que l'essentiel. Il est aussi nécessaire de surveiller l'activité des opérateurs sur notre territoire.

Espionnage de tous les systèmes sans fil

Une mise en garde est aussi à effectuer sur tous les équipements sans fil :

- Clavier d'ordinateur sans fil,
- Téléphones portables, DCS, GSM, UMTS107,

- Téléphone sans fil, analogique ou DECT108,
- Boucle locale radio pour la téléphonie fixe,
- Boucle locale radio pour les échanges de données informatiques type Tetra
- Liaisons Wifi109
- Liaison Bluetooth110

Tous ces systèmes représentent des dangers d'espionnage très sérieux, surtout dans les grandes villes comme Paris. Nous avons pu constater une disparition des téléphones filaires dans les grandes surfaces, au profit des téléphones sans fil. Les dirigeants politiques en voulant encourager le tout sans fil surtout pour inciter la population à utiliser les systèmes ci-dessus, commettent une grave erreur, car ils vont favoriser l'espionnage à grande échelle. Non seulement ils vont se pénaliser eux-mêmes, mais vont aussi pénaliser notre économie et nos entreprises. De nombreuses ambassades dans les grandes capitales, disposent d'équipements d'interception radioélectriques destinés à faire de l'espionnage.

La bêtise des fans du gadget, c'est l'utilisation des claviers sans fil. Pour une certaine marque d'ordinateur, on a découvert que celui-ci transmettait toutes les informations tapées au clavier jusqu'à une distance qui dépassait largement les 250 mètres. Ou alors, cet ordinateur a été sciemment vendu avec cette défaillance, pour permettre l'espionnage des transactions à l'intérieur de cette société.

Dans le synoptique ci-dessous, nous avons mis en évidence les différents points d'interception possibles. Les ambassades peuvent être dotées de moyens lourds, récepteurs à large bande et enregistreurs, permettant d'enregistrer tout un spectre de fréquence. En effet, contrairement à ce que peut penser le néophyte, il n'est pas nécessaire de disposer d'un récepteur pour chaque fréquence que l'on souhaite écouter.

Il y a de plus en plus de moyens qui sont apparus et permettent de pirater les systèmes.

1°) au milieu des années 70, il suffisait de disposer d'un Minitel et d'une ligne téléphonique.

2°) à partir de 1990, il suffisait d'un PC avec un modem et une ligne téléphonique.

3°) à partir de 1995, il suffisait d'un PC avec un modem et une ligne téléphonique et Internet.

4°) à partir de 2000, il suffira d'un PC avec un dispositif radio pour accéder anonymement aux flux de données informatiques et aux gros systèmes, même les plus sensibles, via Internet.

Les boucles locales radio haut débit en 3,6 ou 26 GHz constituent une brèche importante que les services secrets étrangers peuvent exploiter contre les entreprises nationales françaises et autres. Il faut aussi rajouter les systèmes Tétra en 450 MHz.

Même s'il existe un système de protection des données, en réalité celui-ci est rarement activé par les administrateurs ou responsables informatiques, pour améliorer la compatibilité des transmissions entre le réseau informatique fixe de la société, et les ordinateurs portables des ingénieurs et commerciaux.

Les systèmes d'échange de données entre ordinateurs ou périphériques, permettent à n'importe qui disposant de bonnes compétences informatiques, de s'introduire localement dans les systèmes informatiques. Il est possible par exemple d'intercepter les fichiers destinés à un autre ordinateur ou même à une imprimante.

La cryptographie n'est pas fiable, ni le firewall, car la grande majorité a été testée par la NSA (entre autres), ce qui veut dire qu'ils connaissent les failles pour que leurs services de renseignement puissent pirater nos systèmes. De plus, comme nous le verrons par la suite, la réglementation en matière de cryptage est (en France en particulier) restrictive et limitante.

« ECHELON » Le réseau mondial qui vous écoute.

Principe général de fonctionnement du réseau ECHELON

Le réseau Echelon tel que nous le connaissons a été conçu et construit par la NSA dans les années 80. Il permet d'intercepter de manière non discriminatoire, des e-mails, des fax, des télex et des communications téléphoniques transportées sur pratiquement n'importe quel support (satellites, câbles sous-marins, etc.) et par n'importe quel réseau de télécommunication.

Ce système, à la différence des autres développés pendant la Guerre Froide, est avant tout à but non militaire : gouvernements, entreprises, individus sont devenus les cibles primaires du réseau Echelon.

Bien sûr, nous savons tous que dans chaque pays, les organismes d'espionnage et de contre-espionnage réalisent des écoutes sur leur propre territoire pour assurer la sécurité du pays. Mais ce qui est extraordinaire, c'est qu'Echelon fonctionne à l'échelle planétaire.

ECHELON n'a pas pour but premier d'intercepter des communications sous toutes ses formes d'un individu en particulier, mais plutôt d'intercepter des informations en masse pour réaliser ensuite le tri de ce qui est intéressant au moyen de super ordinateurs (les Crays) et des Dictionnaires.

Pour cela, comme nous le verrons par la suite, un réseau de stations d'écoute a été établi au niveau mondial pour permettre ces interceptions. Certaines stations écoutent des satellites, d'autres des communications terrestres, voire des communications radio.

Les antennes d'interception dans le monde Le réseau Echelon permet de relier toutes ces stations pour fournir aux États Unis, la possibilité d'intercepter un très grand nombre de communications transitant sur la planète.

— Sugar Grove — en West Virginia. Six paraboles sont pointées vers l'Europe et l'atlantique.

Sugar Grove se trouve à environ 300 Km au Sud-Ouest de Washington. Il serait dirigé par l'US Naval Security Group ainsi que l'US Air Force Intelligence Agency.

Méthode d'interception

Chaque station du réseau Echelon utilise des super ordinateurs par lesquels transitent tous les messages. Dans ces ordinateurs, des Dictionnaires contenant des mots clés préprogrammés. Ainsi, des mots relatifs à des sujets types, des villes, des noms, etc. permettent de réaliser des tris, afin de produire des dossiers cohérents.

Bien que des milliers de messages se déversent dans ces ordinateurs chaque minute, ces derniers sont lus et traités en temps réel. Le patron de la NSA, dans l'une des rares interviews affirmait que l'agence devait traiter toute les 3 heures, autant d'informations qu'il y en a dans la bibliothèque du Congrès Américain, la plus grande du monde.

Diagramme décrivant l'opération :

5 étapes sont nécessaires à l'interception :

— dans une station d'écoute d'un pays du pacte, tous les signaux, numériques ou analogiques (téléphone, GSM, ondes radio, signaux satellites...), sont captés par des stations d'écoutes ;

— ils sont ensuite amplifiés puis triés. Seuls les messages intéressants sont retenus ;

— ils sont ensuite passés à la moulINETte des super ordinateurs très puissants contenant les Dictionnaires. Chaque station possède d'ailleurs son propre dictionnaire afin de mieux coller à l'environnement local. Par un système de mots clés contenus dans ceux-ci (exemples : NSA, bombe atomique, C4, terrorisme, etc.), toutes les transmissions en rapport avec ces mots et ces concepts sont conservées, cryptées, puis transmises aux États-Unis ou aux partenaires ;

— au siège de la NSA, à Fort Meade dans le Maryland (près de Washington), les messages sont décryptés, analysés puis classés ;

— les écoutes ainsi traitées sont ensuite renvoyées aux pays intéressés sous forme de rapports, de notes succinctes ou de compilations.

Exemples d'écoutes commerciales

En 1994, la NSA avait intercepté des appels téléphoniques entre Thomson-CSF et le Brésil pour le projet SIVAM, un système de surveillance de la Forêt Amazonienne de 1,3 milliard d'US\$. Thomson était soupçonné d'avoir « acheté les membres stratégiques du gouvernement brésilien ». Conclusion, le contrat fut remporté par Raytheon Corporation qui annonça peu de temps après : « le Département du Commerce américain a travaillé durement pour soutenir l'industrie US dans ce projet ».

Au passage, la société Raytheon assure la maintenance et l'ingénierie de la station d'interception du réseau Echelon à Sugar Grove.

En 1995, par l'intermédiaire d'un satellite de communications commercial, la NSA a réussi à récupérer tous les fax et conversations téléphoniques entre le consortium Européen AIRBUS, la compagnie d'aviation Saoudi National Airlines et le gouvernement saoudien. L'agence avait trouvé que les commerciaux d'Airbus offraient des dessous de table aux officiels Saoudiens. L'information fut transmise à Boeing et Mc Donnell Douglas Corp, qui firent une offre plus avantageuse pour finalement remporter ce contrat de 6 Milliards d'US\$.

Moyens matériels et humains

Antennes, satellites, ordinateurs et réseaux Les antennes

La récolte systématique de communications transitant par satellite commença pour la NSA en 1971.

Deux stations terrestres furent construites dans ce but :

— la première à Morenstown, Cornouailles, en Grande-Bretagne, avec deux paraboles de 30m de diamètre. La première parabole interceptait les communications provenant de l'Intelsat de l'Océan Atlantique, la deuxième celle de l'Intelsat de l'Océan Indien.

— la deuxième station fut construite à Yakima, près de Washington, pour intercepter les communications transitant par le satellite Intelsat de l'océan Pacifique.

La situation resta inchangée jusqu'à la fin des années 70. C'est alors qu'un troisième site, toujours aux États-Unis, fut installé à Sugar Grove, en « West Virginia ». La responsabilité du site fut confiée à l'US Naval Security Group.

Par la suite, le réseau d'écoute Echelon se développa en parallèle du nombre croissant de télécommunications entre 1985 et 1995. Des stations furent implantées au Canada, en Australie ainsi qu'en Nouvelle-Zélande. Celles qui existaient déjà, furent agrandies et modernisées.

Comme montré plus haut, une quinzaine de stations d'écoute principales réparties dans le monde seraient en activité actuellement. Il existe sûrement d'autres stations, mais

elles seraient plus discrètes, plus petites et plus spécifiques à la région voire au pays où elles sont installées. Aujourd'hui, on estime, que le réseau Echelon utilise 120 antennes réparties dans les pays du pacte UKUSA, à des fins d'écoutes et de renseignements. Les catégories d'antennes (sachant que plusieurs types d'antennes peuvent se trouver sur une même station d'écoute):

- 40 sont pointées vers des satellites commerciaux ;
- 30 sont dirigées vers les satellites d'écoute (type Mercury, Keyhole...);
- 50 étaient pointées vers l'ex-Pacte de Varsovie, mais un certain nombre a sans doute été réorienté vers d'autres objectifs, tels que les satellites commerciaux.

Les satellites

On distingue trois classes de satellites :

- Satellite géostationnaire : c'est un satellite de type Mercury placé juste à côté d'un satellite relayant des communications transcontinentales de type Intelsat. De par la taille de sa parabole (de 80 à 100m), les signaux initialement reçus par le satellite Intelsat le seront également par le Mercury. Ce dernier les retransmettra à la station d'écoute la plus proche afin d'en analyser les données.
- Satellite d'observation : c'est un satellite de type Keyhole utilisant une technologie radar, qui permet de voir de jour comme de nuit et sous les nuages avec une précision l'ordre de quelques centimètres.

Ces satellites évolueraient à des altitudes variant entre 200 et 1000 km. Le dernier modèle a pour nom de code KH-12 Improved Crystal.

Aucune spécification officielle n'existe sur ce produit. Selon les Services secrets français, une quinzaine seraient en orbite actuellement.

- Satellite d'écoute basse altitude : cette classe de satellites sert de système d'écoute d'appoint principalement pour les régions dans les latitudes proches du Pôle Nord. Les Mercury couvrant mal ces régions (à cause de leur orbite géostationnaire), des satellites plus connus sous le nom de TRUMPET évoluent à des orbites polaires elliptiques, leur permettant de rester longtemps dans les régions du Nord. L'Agence peut alors écouter tous les transmetteurs dans ces zones et par la même occasion intercepter les signaux envoyés par l'ex-URSS à ses satellites de communications évoluant dans les mêmes orbites.

Petite précision tenant de l'anecdote. Motorola a lancé en 1997 le réseau de communication planétaire connu sous le nom d'IRIDIUM. Ce réseau constitué de 66 satellites évoluant en orbite basse et quadrillant la terre, devait permettre de pouvoir appeler et d'être joignable de n'importe quel point du globe.

Ce qui posa un problème pour la NSA dans un premier temps, attendu que les communications transitent du téléphone cellulaire directement par plusieurs satellites sans passer par des stations relais terrestres (en revanche INTELSAT utilise le principe des relais terrestre). Mais Motorola étant un gros fournisseur de l'Agence, on peut être sûr que le réseau est largement écouté par celle-ci d'une manière ou d'une autre.

Ordinateurs et réseaux

L'Agence est l'organisme au monde le plus grand consommateur de matériel informatique. Elle travaille par ailleurs en étroite collaboration avec quelques grands fabricants américains tels que Motorola, Intel, IBM, ainsi que le fabricant de super ordinateurs : CRAY/SGI.

Elle possède même sa propre unité de fabrication de composants à Fort Meade, pour éviter les fuites, et produire des processeurs à la demande.

Fournir un bilan informatique de la NSA afin d'estimer sa puissance de calcul est impossible, mais en se fondant sur les informations fournies par CRAY, le listing des 500 ordinateurs les plus puissants du monde, et surtout en essayant de dimensionner les besoins par rapport au volume d'écoute, il devient possible d'émettre quelques hypothèses. En regardant sur le site de Cray (www.cray.com), on peut se faire une idée des performances des super ordinateurs, le haut de gamme étant le CRAY SV1. Aujourd'hui c'est le super ordinateur commercial le plus puissant du monde (en 2002). Il est configurable sur mesure en fonction des performances et des attentes du client.

D'autres supers-calculateurs doivent exister, mais de puissance peut être plus réduite mais, surtout, dédiés à certaines tâches, notamment l'analyse vocale des écoutes téléphoniques. À ce propos, des puces spécialisées dans la reconnaissance vocale existent déjà sur le marché.

Nous arrivons donc à une vingtaine de supers-ordinateurs, des capacités de transmission optique/satellite de plusieurs dizaines voire centaine de Gbits/sec et des capacités de stockage pouvant sûrement atteindre des dizaines de milliers de Go. Il sera difficile d'en dire plus par manque d'informations pour l'instant.

Pour terminer sur le chapitre des ordinateurs et réseaux, la NSA serait dotée d'un réseau ultra sécurisé appelé INTELINK (Source : Top Secret Intranet Ed. Charles Goldfare Series - aut. Frederick Martin). Selon l'auteur, un ancien de l'agence, ce réseau, mis en place depuis 1994, serait relié aux bases de données secrètes de la NSA, de la CIA ainsi que des services spéciaux de l'armée américaine. La manière dont transitent les données

n'est pas connue, mais on peut penser que cela s'effectue par satellite et par des lignes spécialisées isolées des réseaux publics.

Il serait consultable depuis n'importe où dans le monde par environ 50.000 officiers de renseignement soigneusement triés sur le volet. Cela inclut bien entendu les principaux décideurs politiques, les ambassades américaines et les espions disséminés un peu partout dans le monde.

Ce réseau donnerait alors accès aux dernières écoutes, photos satellites ou aux rapports d'agents sur le terrain. INTELINK comprendrait ainsi plusieurs centaines de milliers de pages.

Les différents types d'écoutes

Les types d'écoutes possibles se décomposent en 4 grands axes :

- Satellites
- Câbles sous-marins
- Internet
- Radio (Micro-ondes, HF...)

Satellites

Comme cela a déjà été expliqué précédemment, les satellites de la NSA se positionnent de manière à être proches des satellites de communications civils afin de « copier » les signaux pour les retransmettre vers une station terrestre d'écoute qui se chargera de décrypter et d'analyser les messages.

Câbles sous-marins

Aujourd'hui une grande partie des communications transcontinentales passent par des câbles posés au fond des océans. Ces câbles sont maintenant pour la plupart en fibre optique, suite au besoin de plus en plus croissant de vouloir communiquer. Les débits par câble sont de l'ordre d'une dizaine de Gbits/sec ce qui permet d'acheminer des dizaines de milliers de communications téléphoniques simultanément.

On peut penser qu'il est impossible d'intercepter des signaux lumineux d'une fibre optique en raison du fait que la lumière ne produit pas d'émissions électromagnétiques, et qu'intercepter le signal lumineux sur une fibre reviendrait à rompre la communication.

Selon certains spécialistes, il n'en est rien. Le signal lumineux dans une fibre se dégradant au fur et à mesure du chemin parcouru à cause du support (qui bien qu'étant un matériau translucide présente une certaine opacité), a besoin d'être amplifié environ tous les 100 Km par ce que l'on appelle des répéteurs. À ce point précis, le signal optique est converti en un signal électrique numérique pour être amplifié puis reconverti en signal optique. Il devient alors possible de poser une bretelle à cet endroit-là pour transmettre les données vers un satellite relais en basse altitude qui les redirigera vers une station d'écoute, voire de doubler le signal sur un câble parallèle pour le réacheminer vers la station d'écoute la plus proche.

La pose d'une « bretelle » à 5.000 m de fond est bien entendu coûteuse en terme d'infrastructure, mais néanmoins tout à fait envisageable.

L'autre solution que la NSA a pu adopter est la pose de matériel d'écoute au point de sortie du câble sur terre ferme. En effet au nom du patriotisme et du pacte UKUSA, La NSA peut très bien imposer ses conditions à certains opérateurs télécoms anglo-saxons.

Internet

On peut penser que c'est là le bât blesse pour la NSA. Internet étant un réseau mondial constitué de milliers de serveurs où des quantités de données gigantesques circulent chaque jour.

Il n'en est rien. Durant les années 80, la NSA et les pays partenaires du pacte UKUSA, pilotait déjà un réseau de communications international plus grand que le Web en utilisant la même technologie.

Selon le partenaire britannique, GCHQ (Government Communications Headquarters) : « tous les systèmes étaient reliés ensemble dans le plus grand LAN d'Europe (LAN : Local Area Network – réseau local), qui étaient connectés également aux autres sites dans le monde formant le plus grand WAN du monde (WAN : Wide Area Network - réseau local mais au niveau mondial). Le protocole de communication utilisé est le protocole IP (comme celui du Web) ». Ce réseau global, développé sous le nom de : Projet EMBROIDERY, inclut le super serveur de communications de la NSA, PATHWAY. Il permet de fournir un réseau rapide, efficace, sécurisé pour le système Echelon ainsi que les autres systèmes.

Il est fort probable d'ailleurs, que ce réseau s'appelle maintenant : « Intelink »

Deuxième point, Internet est originaire des États-Unis suite à l'extension d'ARPANET, l'ébauche du premier réseau reliant les sites militaires américains dans les années 60 pour parer à une éventuelle attaque nucléaire de l'ex-URSS. Le développement du net s'est réalisé aux États-Unis, ainsi que la majorité des ressources qui vont avec (Routeurs, serveurs, backbones...). En clair, cela signifie qu'aujourd'hui les ressources physiques se trouvant majoritairement aux USA, de nombreuses connexions provenant de l'étranger passeront là-bas.

Les messages transitent sur le Web sous forme de « packets » appelés aussi « Datagrams ». Ces datagrams afin d'atteindre la bonne destination, contiennent l'adresse IP (ex : 123.123.123.123) de l'émetteur et du destinataire. Ces adresses étant uniques pour chaque serveur connecté sur le Web, il devient facile de réaliser un tri selon l'origine et la destination. Ce processus, s'effectue bien entendu en permanence par les routeurs et les échangeurs afin d'acheminer correctement les messages ; il facilite ainsi grandement la tâche de l'Agence ou de celles qui écoutent, pour le tri.

Les trajets empruntés par ces « packets », dépendent du point d'origine et de destination, du serveur par lesquels ils transitent, ainsi que de nombreux autres facteurs incluant

l'heure de la journée. En effet, les routeurs aux États-Unis sont calmes quand ceux de l'Europe atteignent des pointes d'activité dues au décalage horaire. Il devient alors possible et probable que certains mails devant parcourir une petite distance (par exemple : un mail de la France vers l'Allemagne), doivent d'abord transiter par un échangeur américain ou britannique, ce qui rend l'écoute des mails d'autant plus accessibles par la NSA.

Des sites où sont hébergés les news groups tel qu'Usenet produisent environ 15 Go de données par jour. Ces données sont accessibles à n'importe qui souhaitant les consulter. La NSA peut donc récupérer tout à fait officiellement ces informations pour un tri futur. D'ailleurs, en Grande-Bretagne, l'agence de la Défense de la Recherche & de l'Évaluation maintient une base de données de 1 Tera Octet comprenant 90 jours de messages Usenet.

La plupart des sites Internet accessibles au public sont parcourus par des « bots » (programme parcourant la page cherchant des mots clés) provenant de moteurs de recherches tels que Altavista, Hotbot, Google..., afin de les indexer. La NSA utilise également les mêmes méthodes pour récupérer les informations intéressantes.

Par exemple, un site basé à New York, connu sous le nom de <http://www.jya.com> propose de nombreuses informations touchant à la crypto, ou aux différentes méthodes d'écoute. Ce site étant réactualisé très régulièrement, la consultation des logs sur le site montre clairement qu'un « Bot » du Centre de Sécurité Informatique de la NSA, parcourt tous les matins le site afin de chercher de nouveaux fichiers et de les récupérer.

Il est admis que le trafic Internet au niveau international contenant des informations pouvant intéresser les agences d'écoutes (mails, transfert de fichiers, réseaux privés virtuels), ne représentent que quelques pour cent de la majorité du trafic sur les points d'échanges américains.

Selon un ancien employé de la NSA, cette dernière avait depuis 1995, installé des logiciels de type sniffers (renifleurs) pour analyser le trafic sur les neuf échangeurs américains (Internet Exchange Point- IXP). Deux de ces points, FIX east, Fix West appartiennent au gouvernement. Ils sont implantés très proches des autres échangeurs appartenant à des sociétés commerciales : MAE East & MAE West (MCI Worldcom). Les trois autres sites sont des échangeurs initialement développés par la National Science Foundation pour fournir au Web américain le backbone d'origine du Web.

Tableau des échangeurs américains surveillés par la NSA :

(A titre informatif, en France, il y a 3 échangeurs : 2 à Paris - GIX : Global Internet eXchange- et 1 à Grenoble)

Dernier point, il revient souvent que des grandes sociétés de télécommunications américaines, des éditeurs de logiciels (Microsoft, Lotus, Netscape...) collaborent avec la NSA pour développer des backdoors permettant de capturer des informations intéressantes sur les postes sur lesquels ces logiciels sont installés. Ils sont par ailleurs priés de modifier leurs produits destinés à l'exportation afin de faciliter la récupération d'informations.

Bien que la NSA n'ait jamais confirmé ni démenti ces rumeurs, en 1997 un jugement en Grande-Bretagne suite à une affaire de piratage démontra que l'agence surveillait le Web. Des témoins de l'US Air Force travaillant conjointement avec la NSA, admirent utiliser des sniffers de packets et des logiciels spécialisés pour « tracer » les tentatives de piratage d'ordinateurs militaires US. Le dossier s'écroula quand ces témoins refusèrent de fournir les preuves du système qu'ils avaient utilisé.

Radio (Micro-ondes, HF, etc.)

Les Hautes Fréquences Radio

Une des caractéristiques des ondes radio HF est le fait qu'elles se répercutent contre l'ionosphère et à la surface de la Terre et se propagent donc rapidement d'un bout à l'autre du globe sans nécessiter des infrastructures de réception importantes. Elles ont donc été privilégiées jusqu'au milieu des années 60 pour toutes les communications diplomatiques et militaires.

Les micro-ondes radio

Cette technologie a été introduite dans les années 50, pour augmenter la capacité de transmissions entre cités pour le téléphone, le télégraphe et plus tard pour la télévision.

Elles nécessitent à cause de la courbure de la terre des relais tous les 30 à 50 kilomètres sous la forme d'antennes de 1 à 3 m de diamètre au sommet de tours ou de building.

Le personnel humain

On sait seulement qu'environ 100.000 personnes travaillent directement ou indirectement pour la NSA. Par ailleurs, la NSA est probablement le plus grand recruteur de mathématiciens au monde.

Après la chute du mur de Berlin et de l'URSS, il semblerait que de nombreux savants russes se soient fait recruter par les États-Unis. L'État Russe étant incapable de payer ces savants, beaucoup d'entre eux se seraient exilés aux USA, en fournissant en contrepartie de la matière grise d'une valeur inestimable pour la NSA.

Aujourd'hui, la sécurité d'un pays repose en grande partie sur sa capacité à protéger ses données sensibles, par des moyens de cryptage. Les États-Unis l'ont bien compris, et travaillent pour cela sans relâche avec les mathématiciens de l'agence pour sécuriser ces informations, ces réseaux. Mais par la même occasion, l'agence joue le rôle de casseur de code, afin de mieux percer les secrets des pays

Conclusion

J'espère à travers cette présentation avoir pu vous montrer, ou plutôt vous donner un aperçu du fonctionnement de cette agence tentaculaire.

La majorité des gens se disent probablement qu'ils ne sont pas vraiment concernés par ce genre de chose parce qu'ils n'ont rien à se reprocher de toute façon. Et surtout parce qu'une personne prise individuellement ne peut de toute façon rien y faire.

Eh bien moi je soutiens le contraire, nous sommes tous concernés. Les États-Unis qui se veulent être un pays ami de l'Europe joue le double jeu. Comme précisé en introduction, c'est le pays le plus puissant du monde aussi bien en terme stratégique qu'économique. Et le renseignement n'y est pas pour rien.

Le renseignement stratégique (militaire) à mon sens est bien entendu nécessaire et indispensable afin de préserver la sécurité d'un pays, mais sur le terrain économique c'est une autre histoire.

Il ne faut pas se leurrer, les 500 plus grandes entreprises françaises font sûrement partie des écoutes de la NSA, tout comme certains décideurs politiques du pays. D'ailleurs, ce n'est pas pour rien que l'ambassade des États-Unis à Paris se trouve si proche de l'Élysée. Les enjeux économiques suite à la globalisation des échanges sont tellement élevés qu'il devient difficile de résister à la tentation d'utiliser ce système à son propre avantage.

On dit que 90 % des informations sont disponibles au grand public si on sait chercher, 5 % le sont à un public restreint, les 5 % restantes étant secrètes. L'art du système Echelon c'est simplement de pouvoir récupérer 99 % des informations afin de les rendre cohérentes et de les utiliser à l'avantage des États-Unis.

Le 2e point, c'est la vie privée Prenons un exemple paranoïaque mais sûrement pas si surréaliste que ça. Cette page parle de la NSA.

L'agence va finir par s'en rendre compte, et vérifiera sûrement qui se connecte sur cette page, et surtout saura qui en est l'auteur.

Peut être qu'une enquête rapide sera menée sur moi afin de mieux me cerner. Toute ma famille vivant à l'étranger, peut être que mes conversations téléphoniques seront enregistrées, mes mails interceptés.

Inquiétant non ? Alors il est temps de réfléchir afin de leur compliquer la tâche. C'est bien connu, on ne peut vaincre son ennemi qu'en apprenant à le connaître.

Perspectives

Aujourd'hui, la France n'a pas les moyens financiers pour créer ce genre de système. L'Europe pourrait le faire mais cela ne risque pas d'arriver tant qu'une véritable union ne sera pas mise en place. Mais il y a des démarches encourageantes :

— Il a été décidé il y a peu de temps au niveau européen, de créer un système GPS concurrent à celui des Américains, qui le voient d'un mauvais œil d'ailleurs. Concrètement, qu'est ce que cela signifie ? Que nous aurons enfin accès à un système de positionnement précis de qualité militaire. En effet, pour avoir une précision de l'ordre du mètre, avec le GPS, il faut demander l'autorisation au Département de la Défense Américaine, sinon la précision accessible au public est de l'ordre d'une cinquantaine de mètres, ce qui est largement insuffisant pour l'armée. On imagine mal en effet l'armée Française effectuer ce genre de demande aux américains !

— La France, via le SCSSI123 (organisme sous la tutelle du Premier Ministre) autorise le cryptage à 128 bits depuis la mi-mars 1999. C'est mieux que les 40 bits précédemment autorisés. Mais c'est loin des possibilités de cryptage pouvant aller jusqu'à 4096 bits. De toute manière, il ne faut pas se faire d'illusions : si l'État autorise ce genre de cryptage, c'est parce qu'il a les moyens matériels de casser la clé dans un laps de temps suffisamment rapide. Mais cela donne au moins le mérite de compliquer un peu plus les écoutes de nos « amis » de la NSA.

En tout cas, il apparaît clairement que la situation n'évoluera pas beaucoup dans les années à venir côté européen. Mais côté Américains, leur but est clair : rentrer de plein pieds dans le XXIe siècle en maîtrisant les hautes technologies afin de mieux dominer aussi bien stratégiquement qu'économiquement la planète.

La chronologie du Réseau ECHELON

1941 : Après l'attaque japonaise de Pearl Harbor, le centre d'écoute de Bletchley Park est développé en Grande-Bretagne par les Anglais et les Américains pour intercepter et décoder les communications militaires des Allemands et des Japonais. C'est le projet ULTRA.

17 mai 1943 : L'accord Brusa est signé entre le Royaume-Uni et les USA : il s'agit d'une coopération en matière de renseignement électronique. Les cryptanalystes chargés par le gouvernement britannique de casser le code de chiffrement de la machine allemande Enigma, regroupés à Bletchley Park autour du mathématicien Alan Turing, étaient parvenus à de spectaculaires succès, et avaient accepté de faire part de leurs découvertes aux Américains.

2 septembre 1945 : Traité de Sécurité entre les États-Unis et le Japon.

5 mars 1946 : La Grande-Bretagne crée le Commonwealth Sigint Organisation, avec le Canada, l'Australie et la Nouvelle-Zélande. Le Pacte UKUSA est en gestation.

1947 : Création de la première station d'écoute à Hong Kong. Dirigée par les Britanniques, elle a permis de préparer les bombardements américains sur Hanoï et d'obtenir des précisions sur les rapports de force du Politburo Vietnamien lors des pourparlers de paix.

1947/48 : Le pacte UKUSA est prorogé. Ce pacte secret conclu, pendant la Seconde Guerre mondiale, entre la Grande-Bretagne et les États-Unis, organise la collaboration des services de renseignement des deux pays dans le domaine de l'espionnage des télécommunications. Le Canada (7 juin **1948**, dans le cadre du pacte CANUSA avec les USA),

l'Australie et la Nouvelle-Zélande se joignent à ce pacte de coopération et d'échange des informations recueillies. Cibles principales : l'URSS et les pays communistes.

24 octobre 1952 : Aux États-Unis, création de la NSA (National Security Agency) par une directive de huit pages (National Security Council Intelligence Directive N°9) du président Truman en remplacement de l'AFSA (Armed Forces Security Agency). La NSA est chargée, au sein des services de renseignement, des opérations SIGINT (signal intelligence), c'est à dire de l'espionnage électromagnétique (surveillance des liaisons radios, des émissions radar, des télécommunications, etc.) et de la conception des systèmes de codage et de cryptage destinés à assurer la confidentialité des communications du gouvernement, des diplomates et des militaires américains.

1957 : Reconnaissance officielle de la NSA par le gouvernement américain.

25 août 1960 (ou 1961) : Naissance du NRO (National Reconnaissance Office), agence fabriquant des satellites-espions, suite à une controverse entre la Maison Blanche, la CIA et le DoD pour déterminer qui aurait la responsabilité des reconnaissances par satellite du pays. Son existence sera niée jusqu'en 1992.

1966 : La NSA prend le contrôle de la base de Menwith Hill (nord de l'Angleterre) qui était jusque-là dirigée par l'armée américaine. Elle en fera la plus grande station d'interception du monde.

8 Juin 1967 : Le navire USS Liberty est coulé par l'aviation israélienne qui l'avait confondu avec un bateau égyptien : le bilan fait état de 34 morts, 170 blessés.

Le 2 juillet 2003, l'agence de sécurité nationale (NSA) a libéré l'information additionnelle relative à l'attaque du 8 juin 1967 sur le « U.S.S. Liberty ». Ce document inclut ti enregistrements audio, et transcriptions (en anglais), trois rapports de suivi, et un rapport Cryptologic d'histoire des États-Unis intitulé « Attaque sur un collecteur de SIGINT, l'USS Liberty » Les enregistrements sont en hébreu et contiennent des décomptes de temps, en anglais, qui ont été ajoutés par l'opérateur d'interception. Les rapports de suivi sont des résumés des trois transcriptions, avec omission des paroles hors action, et un rapport compilé qui récapitule l'activité et contient le texte des transcriptions. Le rapport Cryptologic d'histoire des États-Unis est une version moins développée du même document à l'origine, libéré en 1999.

Comment l'information a été obtenue : Une heure après avoir appris que le « Liberty » avait été torpillé, le directeur de la NSA, le LTG Marshall S. Carter, USA, envoie un message à tous les emplacements d'interception demandant une recherche spéciale de toutes les communications qui pourraient refléter l'attaque ou la réaction. Aucune communication n'était disponible. Cependant, une des plateformes aéroportées, le U.S. Navy EC-121, avait rassemblé des conversations entre deux pilotes israéliens d'hélicoptères et la tour de contrôle du terrain d'aviation de Hazor suivant l'attaque sur le « Liberty ».

août 1968 : Lancement du premier satellite COMINT américain sous le nom de code CANYON, puis d'un second. Ils étaient contrôlés depuis la station de Bad Abling, en Allemagne, et visaient l'URSS.

Ils furent placés à proximité d'orbites géostationnaires afin de couvrir en permanence les cibles sélectionnées. Cinq autres satellites de cette classe furent lancés jusqu'en 1977.

1970 : Création de la station de Yakima dans le Nord-Ouest des États-Unis, en même temps que la première génération de satellites INTELSAT. La station est dotée d'une grande antenne orientée vers le Pacifique.

Octobre 1971 : Le sous-marin USS Halibut, croisant dans la mer d'Okhost, au large de la côte Est de l'URSS, enregistre les communications passant dans un câble militaire reliant les quartiers généraux de l'armée à Vladivostok à la péninsule du Kamchatka. Il était équipé d'une capsule de plongée à très basse profondeur fixée à la poupe du bâtiment et décrite par la Navy comme « un canot de sauvetage à basse profondeur ». En 1972, il lâcha une nacelle d'enregistrement à haute capacité à côté du câble qui fonctionna jusqu'en 1982, quand un employé de la NSA informa les Soviétiques de l'opération IVY BELLS.

1972 : Le GCHQ commence à « exploiter » une nouvelle station secrète à Morwenstow, non loin de Bude en Cornouailles, Angleterre. Cette station, dotée de trente antennes satellitaires, permettait d'intercepter les communications satellites au-dessus de l'Atlantique et de l'océan Indien.

1972 : Création au sein de la NSA, par mémorandum présidentiel, du Central Security Service chargé de coordonner les activités de cryptologie, de gérer les procédures d'écoute et de sécurité électronique du DoD. Il assure également la liaison avec les autres organes de renseignement et de sécurité.

1974 : Construction à Menwith Hill de la première grande antenne satellitaire.

8 août 1975 : Le Directeur de la NSA, Lew Allen, reconnaît, devant la Chambre des Représentants, que « la NSA intercepte systématiquement toutes les communications internationales, qu'elles soient vocales ou par câbles », il s'agit de l'opération SHAMROCK.

Juin 1978 : Lancement du premier satellite CHALET, suivi par un second en octobre 1979. Après que le nom du premier satellite fut apparu dans la presse américaine, ils furent rebaptisés VORTEX, avant d'être rebaptisés MERCURY en 1987, à la suite d'une nouvelle fuite.

1978 : Le Congrès adopte une loi (Foreign Intelligence Surveillance Act) définissant les procédures d'écoute de la NSA.

Été 1979 : Le sous-marin USS Parche, fait le voyage de San Francisco à la mer de Barents en passant au-dessous du Pôle Nord et installe un nouveau système d'enregistrement des informations par câbles près de Mourmansk. Il est toujours en activité et reçoit de hautes récompenses, chaque année de 1994 à 1997.

1980 : Entrée en service de la station de Sugar Grove dans l'Est des États-Unis (cette station existait déjà pour écouter les communications russes) afin de s'adapter à la deuxième génération de satellites INTELSAT. Une autre station est installée à Hong-Kong.

1981 : La NSA et le GCHQ construisent le premier réseau global à grande échelle (Wan). Jusqu'au milieu des années 90, ce réseau international, qui permettait de relier les stations SIGINT et les centres de traitement, était plus important qu'Internet. Le réseau est constitué de câbles transocéaniques et de liaisons spatiales. La plus grande partie des capacités des satellites de communications militaires américains et britanniques, Milstar et Skynet, est consacrée à transmettre des données pour les services de renseignement.

1985/87 : Projet de création d'un réseau mondial de surveillance des télécommunications révélé par le journaliste britannique Duncan Campbell. Le principe du projet F 415 est de relier entre elles, grâce à de puissants ordinateurs, les différentes bases d'interception des pays du pacte UKUSA qui sont disséminées à travers le monde.

Février 1983 : M. Thatcher fait surveiller par Echelon les conversations de deux de ses ministres (selon les informations de Mike Frost, ancien du CSE canadien).

1986 : Deux soldats américains étaient tués dans l'explosion d'une discothèque à Berlin-Ouest. L'attentat n'a pas été revendiqué. Pourtant, l'État commanditaire, la Libye, a été immédiatement identifié par les États-Unis : la NSA avait intercepté et décrypté les communications entre les ambassades de Tripoli à Berlin-Est et Rome. Quelques minutes après l'explosion, un membre des services secrets de Kadhafi disait : « L'opération a bien eu lieu. Elle n'a pas laissé de traces. » Quelques jours après, Reagan autorisait le bombardement de la capitale libyenne.

1988 : Lors d'une visite en Australie, Bob Tizard, ministre de la Défense néo-zélandais, révèle que deux nouvelles bases en construction ne sont pas destinées aux communications militaires, mais à intercepter les satellites de communications civiles lancés par les pays du Tiers Monde tels que l'Inde et l'Indonésie.

12 août 1988 : Duncan Campbell rédige le véritable premier article sur Echelon, publié dans l'hebdomadaire britannique « News Statesman ». Depuis lors, il ne cessera de réunir des éléments sur ce réseau.

1989 : La chute du mur de Berlin entraîne la redéfinition des priorités stratégiques des États-Unis. La conquête des marchés mondiaux est désormais l'objectif majeur.

1990 : La NSA intercepte les communications entre le fabricant japonais de satellites NEC et l'Indonésie pour la fourniture d'un contrat de 200 millions de dollars. Le président Bush intervient auprès de Djakarta. Le contrat sera partagé entre NEC et l'américain ATT.

1990 : Inauguration des nouveaux locaux de l'ambassade de Chine en Australie. Lors de la construction du bâtiment, des agents américains ont installé de multiples micros et des systèmes de surveillance des communications dans tous les murs. Les informations recueillies sont transmises directement par satellite au quartier général de la NSA dans le Maryland aux États-Unis.

Juillet 1990 : Les satellites Keyhole ont vu le déploiement des troupes irakiennes à la frontière du Koweït. Le 27, six jours avant l'invasion, les capteurs infrarouges ont repéré les camions militaires transportant de l'eau, du gasoil et des munitions.

19 août 1991 : Lors du putsch de Moscou, la NSA obtient des photos de Gorbatchev emprisonné dans sa maison ainsi que des enregistrements de toutes les discussions téléphoniques entre les chefs rebelles. Avant tout le monde, Bush sait donc que le coup d'État ne réussira probablement pas.

3 septembre 1991 : Un document, aujourd'hui déclassifié, précise la mission du centre de surveillance électronique de l'US Navy, à Sugar Grove (Virginie Occidentale), en liaison avec le 544ème groupement de renseignement.

1991 : L'émission britannique World in Action effectue un reportage sur le fonctionnement d'un ordinateur Dictionary situé dans la station londonienne du GCHQ sur Palmer Street, Westminster (station UKC1000). L'émission cita des employés du GCHQ, qui souhaitaient rester anonymes : « Ici au troisième, [le GCHQ] a engagé un groupe de spécialistes de la sécurité de British Telecom... Ça n'a rien à voir avec la sécurité nationale. C'est parce qu'il est illégal d'intercepter tous les fax. Et pourtant ils prennent tout ce qui passe : ambassades, contrats, vœux d'anniversaire, tout y passe. Et ils mettent tout dans le Dictionary. »

1991 : Plus de 12 tonnes de cocaïne sont saisies grâce aux informations fournies par la NSA qui intercepte, à partir du Venezuela, toutes les communications des membres du cartel de Cali.

8 avril 1992 : dans son discours d'adieu à l'état-major de la NSA, le vice-amiral William Studeman, alors directeur de la NSA, décrit comment les « demandes pour un accès global accru [aux communications] se multiplient. La partie commerciale de cet accès global est une des jambes, qui, espérons-le, sera solide, sur laquelle la NSA devra s'appuyer au siècle prochain ».

1992 : L'arrestation pour espionnage d'un attaché commercial de Crypto AG par le gouvernement iranien devait entacher la réputation d'indépendance de la firme helvétique, soupçonnée d'avoir fourni depuis des décennies les clés de cryptage à la NSA.

1992-93 : La NSA espionne les communications des officiels mexicains qui négocient l'ALENA (Accord de Libre-échange Nord-américain) avec les États-Unis et le Canada.

1993 : Au cours du sommet de l'APEC (forum de coopération Asie-Pacifique), la NSA et le FBI installent des équipements capables d'écouter les communications des 15 dirigeants des pays de la zone Asie-Pacifique conviés à Seattle, aux États-Unis, par Bill Clinton. Certaines informations collectées semblent avoir été transmises à des chefs d'entreprises qui ont financé la campagne électorale du président américain.

1994 : Début du démantèlement de la station de Hong Kong : les antennes sont transférées en Australie.

1994 : Lors du bras de fer entre les États-Unis et l'Union européenne dans les négociations du GATT, le réseau Echelon est utilisé par Washington pour connaître la position de chacun des 15 pays de l'UE et la stratégie de la Commission européenne. Des consignes seront données aux fonctionnaires de Bruxelles leur demandant de ne pas utiliser le

courrier électronique, dont l'usage commence à se généraliser, pour transmettre des informations sensibles.

1994 : Interception des négociations entre le fabricant français de radars Thomson-CSF et les autorités brésiliennes. La NSA aurait donné le montant des « dessous de table » au Président Bill Clinton, qui serait par la suite intervenu auprès du gouvernement brésilien. C'est finalement la firme américaine Raytheon qui décrochera le contrat pour assurer la couverture radar de l'Amazonie.

1994 : Le directeur de la NSA, John Mac Connell, déclare : « Il n'y a pas un seul événement de politique étrangère qui n'intéresse le gouvernement américain et auquel ne soit pas directement mêlée. »

1994 : La NSA intercepte les coups de téléphone et les fax entre Airbus et les autorités saoudiennes. Le contrat de 6 milliards de dollars sera décroché par Boeing.

20 juillet 1994 : Bill Clinton renonce au projet de la NSA (remontant à la présidence de G. Bush) de doter chaque ordinateur ou chaque téléphone produit aux USA d'une clipper chip (ou puce pirate) permettant de surveiller les communications.

16 septembre 1994 : Les motifs stratégiques d'Echelon sont exposés dans un mémorandum confidentiel de la Maison-Blanche : « la fin de la Guerre froide a dramatiquement changé les priorités et les menaces vis-à-vis de notre sécurité nationale. Outre les questions politiques et militaires traditionnelles, les thèmes économiques suscitent une préoccupation et un intérêt croissant ».

1995 : L'envoyé de Bill Clinton au Japon, Mickey Kantor, bénéficie de l'aide de la NSA lors de discussions très serrées avec Tokyo sur les quotas d'importation de voitures.

15 juin 1995 : Un document, aujourd'hui déclassifié, donne des indications sur « l'activation d'unités Echelon » de l'armée de l'air sur plusieurs bases dans le monde.

Juillet 1995 : Les satellites Keyhole auraient vu les massacres de Srebrenica.

3 décembre 1995 : Le Baltimore Sun révèle que « à partir d'un satellite de communications commerciales, la NSA s'empara de tous les fax et appels téléphoniques entre le consortium européen Airbus, la compagnie aérienne nationale de l'Arabie Saoudite et le gouvernement saoudien. L'agence découvrit que les agents d'Airbus offraient des pots-de-vin à un officiel saoudien. Elle transmet l'information aux officiels Américains qui appuyaient l'enchère de Boeing Co. et McDonnell Douglas Corp., lesquels triomphèrent l'année dernière (1994) dans la compétition à six milliards de dollars ».

1996 : Une chaîne néo-zélandaise est parvenue à obtenir des images de l'intérieur du centre des opérations de la station de Waihopai. Les images furent obtenues clandestinement en filmant de nuit à travers des fenêtres partiellement obstruées par des rideaux. Le reporter parvint tout de même à faire des gros plans des manuels des techniciens du centre de contrôle. Il s'agissait de manuels techniques d'Intelsat, prouvant que la station espionnait des satellites civils. Le film montrait également que la station était pratiquement vide, gérée presque exclusivement par des ordinateurs.

1996 : Le néo-zélandais Nicky Hager met en évidence l'existence et le fonctionnement du plus grand réseau d'espionnage des communications jamais conçu. Il dévoile ce réseau baptisé « Echelon » dans un livre intitulé « Secret power ».

1996 : Signature d'un accord entre Lotus et le gouvernement américain pour l'exportation des systèmes de cryptage de 65 bits : en échange de la licence d'exportation, Lotus garantit aux autorités américaines l'accès à 24 de ces bits appelés « champs de réduction de charge de travail ».

Juin 1997 : Un exercice secret, appelé Eligible Receiver, voit 50 à 75 agents de la NSA attaquer et pénétrer les ordinateurs du DoD à partir de programmes téléchargés sur Internet (63% des attaques n'ont pas été détectées). Le commandement de la Zone Pacifique aurait pu être rendu inopérant.

Septembre 1997 : Lors du jugement de deux activistes britanniques arrêtées et jugées pour avoir essayé de pénétrer dans la base de Menwith Hill, R. Morris, chef de la planification d'urgence chez British Telecom, rend publics des documents prouvant le branchement de la station sur trois tronçons de fibre optique qui permettent chacun de véhiculer plus de 100 000 communications domestiques.

1997 : La NSA reçoit le « National Intelligence Meritorious Unit Citation » décerné par le DCI pour services rendus pendant la Guerre froide et durant 50 ans.

Novembre 1997 : les pouvoirs publics suédois ont appris que le système cryptographique du logiciel Lotus Notes d'IBM, utilisé notamment par les parlementaires et l'administration, mais aussi l'industrie, avait été affaibli pour faciliter le décryptage des courriers électroniques par la NSA, qui disposait d'une partie de la clé de cryptage. Lotus s'est défendu mollement de ces accusations, assurant seulement avoir reçu des garanties que le gouvernement américain n'en ferait pas « mauvais usage ».

Décembre 1997 : Le Parlement européen publie, sur l'initiative du député britannique Glynn Ford, le rapport Évaluation des techniques de contrôle politique 114 qui dénonce le système d'interception des transmissions hertziennes mis en place par les États-Unis dès 1948 pour recueillir le maximum d'informations sur l'Union soviétique et ses alliés.

1998 : La NSA aurait infiltré des agents au sein de la mission de désarmement de l'ONU en Irak. Leur mission : installer de petits systèmes d'interception pour capter les communications de Saddam Hussein et de l'état-major irakien.

1998 : Le NRO annonce un plan de restructuration des différentes classes SIGINT dans une architecture commune dénommée IOSA pour accroître les performances des satellites et le traitement du signal.

Février 1998 : Le général Michael Hayden est nommé à la tête de la NSA qu'il modernise, notamment par la création des premières cellules opérationnelles chargées d'intervenir dans le cyberspace.

11 mai 1998 : Le Sunday Times a relaté que par le passé les radômes de Menwith Hill (station NSA83) dans le Nord du Yorkshire au Royaume-Uni, avaient eu pour tâche d'intercepter l'ensemble du trafic ILC — essentiellement des communications commerciales ordinaires. Le personnel est passé de 400 personnes dans les années quatre-vingt à plus de 1400 aujourd'hui auxquelles s'ajoutent 370 personnes venues du ministère de la Défense. Le Sunday Times fait part également d'allégations selon lesquelles les conversations entre la société allemande Volkswagen et General Motors ont été interceptées et que les Français se sont plaints que Thomson-CSF, l'entreprise électronique française, avait perdu un contrat d'un montant de 1,4 million de dollars destiné à la fourniture d'un système radar au Brésil parce que les Américains avaient intercepté des détails des négociations et les avaient transmis à la compagnie américaine Raytheon qui avait par la suite remporté le contrat. Selon une autre plainte, Airbus industrie aurait perdu un contrat d'une valeur d'un milliard de dollars au profit de Boeing et McDonnell Douglas car des informations avaient été interceptées par l'espionnage américain.

20 août 1998 : Treize jours après un double attentat contre les ambassades américaines au Kenya et en Tanzanie, les États-Unis bombardent des camps d'extrémistes musulmans visant, sans l'atteindre, le milliardaire Oussama ben Laden. Les satellites du NRO guidèrent les missiles grâce aux signaux du téléphone satellitaire de ce dernier.

3 septembre 1998 : La NSA a mis en place il y a deux ans un astucieux programme de mise à la retraite anticipée d'une partie de ses personnels, qui lui permet à la fois d'élargir son influence dans l'industrie privée en y plaçant ses cadres qui souhaitent partir, et de recruter les jeunes talents dont elle a besoin. Intitulé « Soft Landing » (atterrissage en douceur), ce programme aurait déjà permis à la NSA d'économiser 25 millions \$.

Septembre 1998 : Une étude commandée par le Parlement européen souligne les dangers que fait peser l'activité de ce réseau sur les pays de l'Union européenne et sur leurs entreprises. Steve Wright, membre d'OMEGA, une association britannique pour les droits des citoyens (Manchester) constate, dans un rapport adressé au Parlement européen, que tous les courriers électroniques, les conversations téléphoniques et les fax sont enregistrés par routine par la NSA qui fait suivre toutes ces données à Fort Meade.

24 février 1999 : Le New York Times publie un article décrivant en termes généraux le système Echelon comme une coopération entre l'Australie, le Canada, la Nouvelle-Zélande, le Royaume-Uni et les États-Unis visant à écouter l'ensemble des échanges téléphoniques et électroniques du monde.

Février 1999 : La Maison-Blanche lance un programme de recherche afin que l'industrie informatique développe des ordinateurs ayant la possibilité de vitesse de traitement de 30 téraflows en 2001 et de 100 téraflows en 2004. L'objectif est de répondre au défi que pose la cryptographie.

Printemps 1999 : Les Commissions du Renseignement du Congrès — créées dans les années 70 en partie à cause des activités illégales de la NSA sur le sol américain — se sont néanmoins émus d'accusations selon lesquelles des Américains auraient été placés sur écoute.

11 mars 1999 : Martin Brandy, Directeur du DSD Australien (Defense Signals Directorate), brise le silence et révèle que son service « coopère effectivement avec des organisations équivalentes d'espionnage des signaux outre-mer sous l'égide de l'alliance UKUSA ». Cette déclaration fut diffusée le 11 avril 1999 dans le « Programme du Dimanche » sur Channel 9 TV.

Été 1999 : Un expert en sécurité informatique, Andrew Fernandes, annonce qu'il a découvert deux « clés secrètes » dans un logiciel de Microsoft, dont l'une était dénommée... « NSA Key ». Microsoft assure que cette appellation signifie simplement que cette clé est conforme aux standards imposés par la NSA, mais se défend de « partager les informations » que donne cette clé avec des tiers, même avec la NSA.

20 novembre 1999 : Le professeur Christopher Simpson, de l'American University de New York a révélé quelques-uns des mots clés grâce auxquels le système Echelon effectue ses écoutes : AK-47, Cocaïne, Stinger (du nom du missile anti-aérien portable), TWA 800 (l'identification du vol du Boeing qui a explosé au-dessus de l'Atlantique), Militia, Davidian (le surnom de la secte Waco en 1993) ou « Vince Foster » (un ami de Bill Clinton travaillant à la Maison Blanche qui s'est donné la mort en 1993).

6 décembre 1999 : Le New Yorker révèle que l'USS Jimmy Carter (SSN-23), de type Seawolf, va être réaménagé en vue de missions de services secrets de type subaquatiques (écoutes de câbles) à partir de 2004.

1er janvier 2000 : Le passage à l'an 2000 a provoqué une panne des systèmes terrestres de traitement de l'information des satellites-espions.

5-12 janvier 2000 : L'ordinateur central du système Echelon était hors service pendant toute la semaine : le coût de la remise en marche du système s'élèverait à la modique somme de 1,5 million de dollars.

24 janvier 2000 : La NSA admet que l'ensemble de son réseau informatique de traitement et d'analyse a connu une panne totale pendant trois jours : le système a littéralement été noyé sous l'information.

Février 2000 : Des documents « top-secret » déclassifiés de la NSA confirment l'existence du programme Echelon.

22-23 février 2000 : Examen par le Parlement européen du rapport sur le fonctionnement d'un réseau Echelon.

23 février 2000 : Exposé de Duncan Campbell devant les eurodéputés des activités de la NSA et du système Echelon.

Mars 2000 : La DGSE est mise en cause par la presse spécialisée pour collaborer avec la NSA qui lui aurait transmis une partie de son savoir-faire dans les années 70.

28 mars 2000 : Le Figaro relate les confidences d'un expert des services de renseignement américains : « Pour l'adversaire, il est chaque jour plus aisé de cacher son jeu dans le brouhaha. Et pour nous, il devient chaque jour plus difficile de déchiffrer les partitions qui nous intéressent. C'est un vrai problème pour la NSA ».

10 mars 2000 : Selon le journal Le Monde, Georges Tenet, directeur de la CIA, aurait déclaré devant le Congrès américain que les États-Unis n'utilisaient pas leurs services de renseignement pour promouvoir leurs activités économiques.

Mars 2000 : La presse allemande affirme que la station de Bad Aibling se consacre à l'espionnage d'entreprises allemandes et suisses.

24 mai 2000 : Le parquet de Paris a ouvert une enquête préliminaire sur le réseau Echelon, soupçonné d'avoir servi à l'espionnage industriel.

Juin 2000 : La diffusion de comptes rendus d'interceptions de la NSA classés « secrets » et relatifs aux conversations de Hilary Clinton et de Jimmy Carter suscite un vif intérêt chez les membres de la commission pour les affaires de renseignements de la Chambre des Représentants.

Juin 2000 : L'Irlande s'intègre au Pacte UKUSA.

13 octobre 2000 : Ilka Schröder, députée allemande des Grünen au Parlement européen, a décidé de déposer une plainte contre X auprès du plus haut magistrat de la république fédérale, pour « exploitation et tolérance du système d'espionnage Echelon » dans son pays. « Cette plainte vise tout particulièrement les États-Unis et la Grande-Bretagne, ainsi que le gouvernement allemand ». Elle a également porté plainte auprès du procureur de Berlin, son lieu de résidence.

16 octobre 2000 : le général Michael Hayden, lors d'un congrès sur la guerre de l'information qui s'est tenu à Baltimore a réitéré sa volonté que la NSA représente la figure de proue du Pentagone pour toute la défense du Cyberspace.

21 janvier 2001 : Le ministre néerlandais de la Défense nationale présente une note circonstanciée intitulée « L'écoute à grande échelle des systèmes de télécommunication » dans laquelle il estime l'existence du réseau Echelon plausible.

22 janvier 2001 : Dans l'exposé qu'il fait devant la Commission temporaire sur Echelon, Duncan Campbell estime que les USA font appel à leurs services de renseignement pour aider les entreprises américaines à obtenir des marchés. Les informations seraient transmises via la CIA, avec l'aide de l'Advocacy Center et de l'Office of Executive Support au Department of Commerce.

23 janvier 2001 : Le Jane's Defence Weekly révèle l'existence d'une base Echelon à Taïwan qui se trouverait dans les montagnes de Yangmingshan, au Nord de Taïpei.

25 janvier 2001 : Un cadre de la NSA a affirmé au Monde du Renseignement que l'Agence disposait d'un des premiers ordinateurs quantiques fonctionnant dans un cadre opérationnel. Cela lui donne une confortable avance dans la durée de déchiffrement de la plupart des algorithmes utilisés. Il y aurait ainsi cinq ordinateurs quantiques de 40 bits dont les performances surpassent largement les supercalculateurs de type ASCI Red Tops et Cray T3E.

Début 2001 : La Suède découvre que les logiciels Lotus utilisés par les services gouvernementaux et par de nombreuses entreprises disposent de clés activant des back doors contrôlées par la NSA.

Février 2001 : Un second câble de liaison Internet casse entre la Chine et les USA. Les internautes chinois risquent de ne plus pouvoir surfer pendant plusieurs jours en raison de « travaux » sur un câble sous-marin défectueux, un câble qui donne accès aux serveurs basés aux États-Unis. C'est la seconde fois qu'un câble sous-marin est « défectueux » dans cette région. Il y a quelques mois déjà un autre câble, donnant une liaison entre l'Europe et l'Australie avait souffert du côté de Taïwan. Un sous-marin poserait-il une dérivation ?

Février 2001 : « NSA Career Fair 2001 » : séance de recrutement organisée par la NSA, à l'intérieur du R&E Building de Fort Meade. 600 postes sont à pourvoir dans sept domaines : la recherche fondamentale en informatique, l'ingénierie informatique, la cryptanalyse (et notamment la cryptographie quantique), les mathématiques, l'analyse des signaux radio électriques, les langues étrangères et l'analyse du renseignement.

5 février 2001 : Le fabricant de logiciels VMware vient de s'associer à la NSA pour créer un ordinateur inviolable : le projet, baptisé Net Top, vise à transformer chaque ordinateur en autant de PC virtuels tournant sur un ordinateur sous Linux. Ces murs virtuels, mais quasi inviolables permettraient de retrouver la configuration actuelle d'ordinateurs séparés physiquement sur différents réseaux correspondant à des classifications différentes.

Mars 2001 : Les États-Unis devraient déployer, à partir de 2005, un réseau de satellites-espions aux performances encore inégalées dans le monde. A ce titre, le groupe américain de défense Boeing vient de recevoir un contrat portant, à terme, sur un total de 25 milliards de dollars. À l'heure actuelle, le NRO exploite, en permanence, six satellites-espions : trois de la classe KeyHole pour l'observation optique et infrarouge par beau temps ou temps couvert, et trois autres de la classe Lacrosse pour la reconnaissance radar, par mauvais temps et de nuit. Ces satellites pèsent quinze tonnes en moyenne. Tel qu'il a été révélé par des indiscretions de sources ayant requis l'anonymat, le projet consiste à passer, dès 2005, à l'exploitation de vingt-quatre satellites-espions en orbite haute, pesant le tiers des satellites actuellement en service et capables de collecter, selon les cas, entre huit et vingt fois plus d'images avec une précision de quinze centimètres. Le NRO a donc fait le choix d'une constellation de satellites-espions moins lourds que les précédents et maintenus ou renouvelés en orbite, de façon à disposer d'une couverture relativement permanente de la Terre.

Mars 2001 : La Lettre de l'Expansion révèle que la NSA s'est lancée dans ce qui semble bien être le plus important plan de mise à niveau de l'histoire dans le domaine des technologies de l'information.

Le projet intitulé « Groundbreaker », évalué à 5 milliards de dollars, s'étalera sur dix ans. Trois équipes s'affrontent pour remporter le contrat. La première, conduite par Computer Science Corporation, comprend General Dynamics et Verizon Communications. La deuxième est menée par AT&T. Enfin, la troisième est composée notamment de Raytheon et WorldComm. Verdict en juillet. Dès le 07/06/2000, le Washington Post annonçait qu'afin de maintenir son avance technologique la NSA envisageait de privatiser une partie non classifiée (1200 à 1500 employés seraient transférés vers le secteur privé) de ses activités technologiques (économie d'1 milliard de \$ sur les dix prochaines années).

Mars 2001 : Der Spiegel a publié un article qui explique pourquoi le ministère des Affaires étrangères et le ministère de la Défense allemand se sont débarrassés du système d'exploitation Windows. En effet, selon le journal, le système de Microsoft laisserait un « backdoor » qui permettrait à la National Security Agency (NSA) américaine de pénétrer et d'espionner les ordinateurs sur lesquels le système est installé.

De plus, le chef de la diplomatie allemande a également décidé de suspendre tous les projets de vidéoconférence, après que les autorités ont découvert que les données transitaient par Denver, Colorado.

L'administration allemande a donc fait appel à deux firmes locales, Deutsche Telekom et Siemens, pour trouver, dans les plus brefs délais, des solutions de remplacement.

8 mars 2001 : Des consultants intervenant dans des sociétés d'intelligence privée apportent des informations à la « Commission temporaire sur le système Echelon » du Parlement européen. Cette expertise sert principalement à démontrer l'agressivité du système en matière d'espionnage économique.

Mars 2001 : Libération révèle que la Commission européenne aurait permis à la NSA d'accéder à ses systèmes de cryptage des informations confidentielles. Ce serait le chef du bureau chargé du cryptage lui-même, le britannique Desmond Perkins qui aurait reconnu : « J'ai toujours eu de très bons contacts avec la NSA à Washington : elle vérifie régulièrement nos systèmes (de cryptage) pour voir s'ils sont bien verrouillés et s'ils sont correctement utilisés ». Ainsi, la NSA n'a même plus besoin de recourir à Echelon... puisqu'elle dispose de ses entrées à la Commission ! Le lendemain, démenti officiel : « L'entreprise Siemens, qui a fabriqué notre système de cryptage, nous a expliqué qu'il avait été testé par la NSA. C'était un argument de vente. Cela s'est passé il y a dix ans... ».

Avril 2001 : Une station d'Echelon vient d'être démilitarisée. Le site Physics Today présente la nouvelle acquisition de « Pisgah Astronomical Research Institute » : une ancienne station de la NASA construite dans les années 60 puis transformée dans les années 80 pour permettre l'interception des signaux des satellites géostationnaires de l'hémisphère Nord. Rosman Station est située au Sud-ouest d'Asheville, dans la forêt de la Caroline du Nord (à l'Ouest de l'État). La station eut pour vocation d'espionner les relations entre Cuba et le Pacte de Varsovie et d'intercepter les messages échangés entre Moscou et les sites des missiles SS-20 en Allemagne de l'Est. Puis, ce fut l'Amérique Latine et le trafic de drogue.

11 Avril 2001 : La NSA vient de signer un accord de 1,2 million US\$ avec NAI Labs pour développer le système sécurisé SeLinux. Le 2 janvier dernier, l'agence gouvernementale américaine NSA annonçait avoir mis au point un noyau pour Linux plus exigeant en matière de sécurité. Chose encore plus étrange, elle comptait – dans l'esprit de l'Open Source – mettre le code de Security-Enhanced Linux (SeLinux) à disposition du public. Cette véritable rupture avec la tradition de la NSA vient d'être renforcée cette semaine avec la signature d'un accord avec NAI Labs. Portant sur 1,2 million de dollars sur deux ans, il stipule que NAI Labs, compagnie privée de sécurité, continuera le développement du prototype SeLinux. NAI Labs est en fait une filiale de PGP Security, véritable Némésis privée de la NSA depuis plus de dix ans. Cet accord s'inscrit dans la continuité d'un précédent contrat passé entre les deux agences en juin dernier.

13 avril 2001 : Un sondage montrait récemment que la moitié des Américains étaient d'accord pour que le FBI ou d'autres agences gouvernementales espionnent leur courrier. L'ACLU a donc décidé d'utiliser les grands moyens pour que les citoyens américains comprennent à quel point leur vie privée est violée, en toute illégalité et en toute impunité, par ces systèmes qui peuvent intercepter à tout moment des courriers électroniques. Pour l'un des directeurs de l'association américaine, Barry Steinhart, le but premier d'Echelon est « la surveillance mondiale, pas seulement des autres services de renseignement, mais aussi des civils ». L'ACLU met l'accent sur le fait que Carnivore, mis en place par le FBI, viole le quatrième amendement de la Constitution américaine. L'Union propose sur son site des astuces pour écrire ou rencontrer son élu local et pour envoyer directement des fax aux députés et sénateurs. Dans la presse, la campagne (qui paraîtra dans le New York Times et le New Yorker) présentera un téléphone portable avec ce titre : « Désormais équipé d'un système à trois interlocuteurs : vous, la personne que vous appelez, et le gouvernement ».

24 avril 2001 : Dans son audition devant la Commission temporaire sur Echelon, Nicky Hager souligne que le système n'est pas tout puissant : « Tout ne peut être intercepté en raison de ressources par définition limitées ; il faut se contenter de ce que promettent des informations importantes ».

26 avril 2001 : Le quotidien La Meuse reproduit les inquiétudes du Comité R, chargé de contrôler les services de renseignement et de sécurité belges, qui vient de remettre un rapport au Parlement. Selon lui, l'absence de moyens et d'instructions interdit à la Sécurité de l'État de mener à bien sa mission de protection du patrimoine scientifique et économique belge. Le Comité R évoque également la mésaventure survenue à un centre universitaire de recherche victime d'une tentative d'intrusion dans son système informatique, doublée d'un cambriolage au cours duquel du matériel a été manipulé ou volé. Ces événements font suite à un important contrat portant sur la livraison de matériel de pointe (les autorités américaines avaient refusé qu'une firme US livre ce type de matériel pour motifs de non-prolifération).

Les soupçons se portent sur les Allemands ou les Américains.

11 mai 2001 : après les difficultés d'Alain Krivine, député européen et membre de la commission Echelon, pour obtenir un Visa d'entrée aux États-Unis, la délégation

européenne a quitté Washington jeudi 10 mai : la plupart des rencontres prévues avec les autorités américaines n'ont pas été honorées (entre autres celles avec la CIA, le Département d'État et la NSA). Cette politique de la porte close semble cohérente (!) si on considère le peu de pouvoir dont dispose en la matière un organisme comme le Parlement européen, pour ne pas parler de l'actuel comité (temporaire) sur le système d'interception Echelon.

Les députés ont tout de même pu rencontrer des membres de la Chambre des représentants, un ancien patron des renseignements américains, et des responsables du département américain de la justice. À cela s'ajoutent des ONG de défense de la vie privée comme l'ACLU ou l'Epic.

11 mai 2001 : Lors de sa rencontre avec la délégation de la Commission temporaire sur Echelon à Washington DC, Jeff Richelson, auteur américain et ancien membre NSA, a déclaré qu'Echelon désignait un réseau d'ordinateurs au moyen duquel seraient filtrées des données échangées entre les services de renseignement.

18 mai 2001 : Un virus nommé Echelon aurait pour but de saturer les grandes oreilles américaines. Ce ver arrive par email sous le nom de « Echelon.vbs ». Ce virus contient un texte caché conçu pour attirer les robots fouineurs du réseau d'espionnage Echelon.

31 mai 2001 : Le quotidien britannique The Register publie une liste réactualisée des mots qui déclenchent Echelon.

2 juin 2001 : Une fuite de la Commission temporaire sur le système d'interception Echelon nous permet de vous présenter son projet de rapport, rédigé le 18 mai 2001.

6 juin 2001 : Le quotidien bavarois Münchner Merkur a eu accès à un dossier secret du Pentagone dans lequel est programmée la fermeture de la station de Bad Aibling pour septembre 2002. Cette fermeture intervient dans le cadre d'une réduction des forces américaines en Europe où les bases terrestres seront remplacées par des satellites d'interception.

10 juin 2001 : Selon La Tribune, la NSA voit d'un mauvais œil l'évolution de la technologie. Depuis 1989 le Pentagone aurait réuni des chercheurs pour tenter de percer les connexions réalisées via la fibre optique. Finalement, la NSA aurait conçu une chambre sous-marine destinée à mettre sur écoute des câbles transatlantiques. Y aurait-il cause à effet des câbles sous-marins qui ont mystérieusement cassé en Australie et en Asie du Sud-est ?

16 juin 2001 : Les États-Unis vont fournir une aide « sur le plan technologique, de l'information et de la détection des communications » au gouvernement espagnol. Cela se traduira par un recours au réseau de satellites-espions américains Echelon, capables, disent-ils, de localiser tout mouvement des membres de l'ETA et d'intercepter leurs communications.

18 juin 2001 : Le serveur public de la NSA est hors service : il n'est plus possible de télécharger le guide sécurité Windows 2000 en raison d'un afflux massif de connexions.

21 juin 2001 : Dans la journée du 31 mai dernier, un agent du Government Communications Head-quarter (GCHQ) est décédé dans des conditions inhabituelles. Quittant son service peu avant 13 h pour rentrer chez lui en voiture, Donald Brian Davies (53 ans) a percuté une barrière de sécurité sur la route.

Les premiers examens pratiqués à l'hôpital de Cheltenham ont indiqué qu'il avait perdu la maîtrise de son auto après un malaise. Puis, dans les heures qui ont suivi, le fonctionnaire a succombé sans que les véritables causes de son décès ne soient identifiées par les médecins. La police a ouvert une enquête. Et la semaine dernière la famille a annulé les funérailles pour cause d'autopsie.

27 juin 2001 : Dans un témoignage exclusif publié le 27 juin 2001 par le quotidien Mainichi Shimbun, le journaliste néo-zélandais Nicky Hager affirme que les moyens d'interception de la NSA ont été « ouvertement » utilisés en secret pour des missions d'espionnage industriel contre le Japon, et au bénéfice des États-Unis.

2 juillet 2001 : Echelon a espionné le Pape et a aussi écouté une grande partie de l'activité diplomatique du Vatican, en particulier durant les années 1995 à 1998. Le Saint-Siège s'en est aperçu et a pris des « mesures telles qu'on peut dire aujourd'hui que le Vatican est le seul État à être entièrement crypté ». Aucun fax, mail, téléphone, émettant depuis les « pièces qui comptent » dans le palais ne peuvent être interceptés, envoyés et enfin lus et déchiffrés par les services des États-Unis d'Amérique. (Repubblica).

3 juillet 2001 : Duncan Campbell, dans un article du Gardian, revient sur le « Rapport Echelon » en discussion au Parlement Européen et met en garde les Européens contre la volonté des Américains de saper les projets (allemands) d'une Europe du renseignement. En effet, les USA créent progressivement des alliances bilatérales avec l'Espagne (lutte contre l'État), la Norvège, le Danemark, la Suisse et l'Italie (lutte contre le terrorisme).

3 juillet 2001 : Une cinquantaine de militants de Greenpeace occuperait depuis cinq heures du matin trois points stratégiques de la base de Menwith Hill afin de protester contre le projet de bouclier antimissile. Un autre groupe manifeste devant l'entrée de la base au son de la musique du film « Mission Impossible ».

3 juillet 2001 : Alors qu'un soldat américain du 353rd Special Operations Group de Kadena Air Base est accusé du viol d'une Japonaise de vingt ans, la presse nipponne dénonce l'espionnage économico-politique que mènerait la Nouvelle-Zélande à l'encontre du Japon dans le cadre du pacte UKUSA.

4 juillet 2001 : La station chypriote d'Ayios Nikolaos (appartenant aux Britanniques) est victime depuis plusieurs jours de manifestations d'une centaine d'écologistes protestant contre l'installation de nouvelles antennes qui, selon eux, mettent en danger la vie des riverains et des oiseaux en raison des radiations électromagnétiques. Un député et un écologiste se sont enchaînés à un des pylônes de la base.

5 juillet 2001 : Au cours d'une session du Parlement européen, mardi 3 juillet, les membres ont entériné 60 amendements avant de valider la résolution informant qu'Echelon n'était pas un outil d'espionnage industriel menaçant. Quelques membres du comité ont protesté, indiquant notamment que cette réunion n'avait que bien peu fait pression sur les États-Unis pour brider ses capacités d'espionnage.

Le rapport sera soumis au vote de l'ensemble des députés européens, lors de la prochaine session parlementaire à Strasbourg, au mois de septembre.

7 juillet 2001 : Le Wall Street Journal rapporte que la NSA a réussi l'exploit d'aller percer et capter des câbles à fibres optiques, qui transportent des millions de liaisons entre matériels informatiques et téléphones, au fond de l'océan, grâce à un sous-marin spécial. Mais, selon son directeur général, Michael Hayden, la difficulté est d'analyser des masses d'informations. « Avec les nouvelles technologies, il y a trop de choses, trop compliquées à interpréter », a-t-il confié au WSJ

10 juillet 2001 : Dans son supplément économique, Le Monde publie une série d'articles relatifs à l'espionnage industriel mené par les États-Unis — les grandes oreilles de l'Oncle Sam — au nom de la lutte contre la cybercriminalité.

16 juillet 2001 : Après une action coup de poing de Greenpeace dans la base Echelon de l'US Air Force de Vandenburg en Californie, 15 militants et deux journalistes ont été poursuivis pour « violation de zone sécurisée » (ils risquent 6 ans de prison et 255 000 \$ d'amendes). Ils auraient empêché un test de missile dans le cadre du programme « Star Wars ».

29 juillet au 10 août 2001 : Les plus hauts responsables du renseignement américain se sont réunis dans les locaux de l'Aspen Institute, sur le site du Wye River Plantation Conference Center, dans le Maryland. Le partage des informations entre services secrets et agences de police judiciaire s'est imposé comme un thème saillant. En outre, plusieurs intervenants ont souligné la nécessité d'élaborer de nouveaux produits, confondant sources ouvertes et données classifiées, qui assureraient une information en temps réel des décideurs politiques.

31 juillet 2001 : Le contrat relatif au projet Groundbreaker — plus de 2 milliards de dollars sur 10 ans — a été attribué à un consortium industriel dirigé par Computer Sciences Corporation (CSC), choisi pour son expérience en matière de reclassement des employés gouvernementaux.

09 août 2001 : Dans un article du magazine New Scientist, un astronome (Jonathan McDowell) dénonce comment l'enregistrement des satellites-espions américains sur les registres de l'ONU ne correspond pas aux orbites réellement empruntées par ces satellites.

21 août 2001 : L'agence américaine (CERT, Computer Emergency Response Team) et son homologue australienne (AusCERT) « vont s'allier pour accélérer le développement de méthodes, d'instruments, et de techniques en vue d'assurer la protection des réseaux interconnectés servant de support aux infrastructures d'information nationales et mondiales », ont-elles annoncé dans une déclaration commune.

Cet accord intervient alors que les deux agences ont coopéré de manière informelle depuis longtemps, notamment lors du passage à l'an 2000, pour prévenir le bogue informatique.

23 août 2001 : Un article du Washington Post reprend les événements du 24 janvier 2000, date à laquelle le système d'écoute Echelon a été frappé de surdité. On y apprend que c'est l'ensemble des stations qui a été affectées, que la NSA est confrontée à un difficile problème de sureffectif, qu'Echelon semble dépassé par l'augmentation du flux d'informations numériques parcourant la planète et que l'interception systématique doit faire place à une recherche ciblée. Reste que la NSA peut saisir au vol un peu plus de 6 To à l'heure soit près d'un cinquième de la capacité moyenne des communications téléphoniques mondiales.

28 août 2001 : Un sergent major de l'Air Force qui était détaché au NRO par TRW (société spécialisée dans l'électronique de défense), Brian P. Regan (ancien membre également de la Defense Intelligence Agency), a été arrêté par le FBI alors qu'il tentait de quitter les États-Unis pour Zurich : il est convaincu d'espionnage au bénéfice d'une puissance étrangère, en l'occurrence la Libye ou l'Irak. Il était spécialisé dans la cryptanalyse, l'analyse d'images satellites et la gestion du réseau Intelink. Durant la Guerre du Golfe, il avait été assigné à l'Irak Regional Intelligence Task Force du Joint Intelligence Center.

5 septembre 2001 : 367 votes pour, 159 votes contre, 34 abstentions, le Parlement Européen réuni à Strasbourg vient d'entériner sa reconnaissance du réseau d'écoute UKUSA connu sous le nom d'Echelon. Un vote qui n'aura strictement aucun effet tangible, mais qui admet officiellement les possibles interférences entre le monde des affaires et celui des services de renseignements.

6 septembre 2001 : TTU confirme que la NSA améliore sa présence en Europe (en Espagne et en Irlande) ce qui lui permettrait de développer une infrastructure SIGINT. De plus le FBI aurait également détaché une équipe à Dublin pour aider les autorités irlandaises à intercepter les communications GSM et utiliser le système Carnivore dans la capture des messages Internet circulant sur les téléphones portables.

12 septembre 2001 : Au lendemain des attentats, les analystes parlent d'un Pearl Harbor des services de renseignement US : manque de moyens ou inadéquations de ces derniers ? En tout état de cause, « Si les services de renseignements étaient parvenus à se rassembler, nous aurions pu déjouer les attaques » a estimé le sénateur Richard Shelby, vice-président de la commission des services de renseignements du Sénat. Un constat renouvelé par John Martin, ancien représentant du Département américain de la Justice. « C'est un échec de la sécurité et de l'ensemble des services de renseignements américains ».

13 septembre 2001 : Selon le Frankfurter Allgemeine Zeitung, la NSA, depuis déjà trois mois, collectait des informations sur des actions terroristes en préparation qui concernaient le détournement d'avions de ligne devant servir d'armes contre des cibles symboliques de la culture des États-Unis et d'Israël. L'accord ne se serait pas fait à temps sur les modalités à mettre en place pour combattre cette menace.

14 septembre 2001 : Alors que l'on se demande aux États-Unis si l'on ne va pas en revenir aux méthodes humaines de surveillance, des activistes prévoient pour le 21 octobre prochain une journée de lutte contre le système de surveillance mis en place par la NSA.

18 septembre 2001 : BAE a installé un laboratoire de R&D en guerre de l'information à Arlington, en Virginie, qui travaille avec la DARPA, la NSA et le Naval Research Laboratory. Un autre bureau spécialisé dans la gestion des programmes avait déjà ouvert en mai.

18 septembre 2001 : Selon la BBC, les satellites-espions américains se concentrent tous et de façon exclusive, sur les pays hôtes de Bin Laden. De plus des satellites commerciaux (Orbimage-4, doté d'une caméra destinée à analyser la composition des sols qui va être lancé le 21 septembre ; Quickbird, qui devrait être lancé le 18 octobre) vont également être affectés à cette tâche afin de pallier à l'absence des satellites militaires quand ces derniers ne seront pas au-dessus de l'Afghanistan. Rappelons enfin qu'en 1998, lors des frappes américaines contre des sites terroristes en Afghanistan, les écoutes de Menwith Hill avaient permis de localiser Bin Laden dans son camp de Zhawar Kili au sud est de la ville de Khost.

Cette interception avait permis de discriminer le téléphone satellitaire du banquier saoudien. Probablement prévenu par des informateurs au sein des services pakistanais l'ISI, Bin Laden avait précipitamment quitté son camp, échappant de peu aux Tomahawks américains.

21 septembre 2001 : Les deux satellites OrbView 4 (appartenant à la société d'imagerie Orbimage) et Quick Toms (propriété de la NASA) sont tombés dans l'Océan Indien une minute après le lancement, le deuxième étage de la fusée Taurus a pris feu. OrbView 4 était doté d'un instrument d'imagerie hyper spectral, baptisé « Warfighter », qui aurait notamment servi à localiser les terroristes cachés — dans le sous-sol ou dans des grottes — en Afghanistan.

27 septembre 2001 : Selon le Réseau Voltaire, le 11/09, le Secret Service, reçoit un appel des auteurs des frappes de New York et Washington. Pour créditer sa menace, la voix donne les codes secrets permettant d'authentifier les ordres présidentiels donnés depuis la Maison-Blanche ou Air Force One. Immédiatement, pour protéger Georges W. Bush, l'avion présidentiel à bord duquel il rentre à Washington est dérouté vers une destination inconnue, tandis que la Maison-Blanche et le Capitole sont évacués et les personnels politiques conduits dans abris antiaériens. Aucun membre du Conseil national de sécurité ne pense plus à des « attaques terroristes », tous pensent qu'un coup d'État militaire est en cours. Le calme ne reviendra qu'à 20 h 30.

2 octobre 2001 : Metamute, site qui traite de la culture numérique, lance un concours littéraire autour d'Echelon, dans le cadre de la troisième édition de la « Jam Echelon day ». Il offre un total de 1 000 euros aux meilleures œuvres de fiction sur le thème. Echelon serait en effet capable d'ignorer une simple liste de mots clés, mais pourrait, par contre, s'intéresser à un récit complet. Attention : le mot « Echelon » ne doit jamais apparaître dans l'œuvre. (Vnu Net)

3 octobre 2001 : La NSA a commencé à moderniser les équipements cryptographiques du gouvernement. Cette mutation devrait s'échelonner sur une quinzaine d'années. Selon l'agence, il faudra changer 400 000 téléphones, radios, cartes à puce et autres appareils de télécommunication utilisés dans tous les ministères. La principale raison invoquée est que de nombreux hackers ont réussi à décoder les algorithmes de cryptage qui permettent l'accès aux infrastructures vitales de l'agence. D'après les spécialistes cités par USA Today, la NSA a grossi artificiellement ses lacunes sécuritaires et chercherait tout simplement à obtenir une augmentation de ses budgets pour le quinquennat 2003-2008.

5 octobre 2001 : Selon BBC News, la fusée Titan IV qui a décollé la semaine dernière d'une base de l'US Airforce a mis en orbite un satellite-espion KH-12 pour Key Hole, (trou de serrure), (ou Krystal) capable de suivre des déplacements de véhicules, d'armes ou de petits groupes de personnes se déplaçant à pied. Cette opération est organisée par le NRO.

13 octobre 2001 : Près de 300 personnes ont manifesté devant la base de Menwith Hill, essentiellement pour protester contre le projet américain de Guerre des Étoiles et des interceptions qui n'ont pu empêcher l'attentat du WTC.

16 octobre 2001 : L'Agence Spatiale japonaise (NASDA) et la société australienne Xantic, filiale de Telstra, ont signé un accord pour la construction de deux stations de contrôle de satellite dans le Telstra International Telecommunications Centre de Perth. La première station assurera les communications avec deux satellites japonais à buts scientifiques et commerciaux. La seconde contribuera à la sécurité de quatre satellites de renseignement dans leur phase de lancement et de mise en orbite, puis elle sera démantelée.

17 octobre 2001 : Selon D. Campbell, dans The Guardian, le gouvernement américain achète toutes les images de l'Afghanistan produites par Space Imaging, la plus performante société civile d'imagerie satellitaire américaine. Pour 1 912 500 dollars, la National Imagery and Mapping Agency (NIMA) s'est réservé l'exclusivité des droits sur toutes ces images. Actuellement des photos satellitaires de l'Afghanistan sont disponibles sur le marché commercial. Elles sont produites par deux satellites, Eros d'Image Sat et Spot. Le gouvernement israélien est cependant prêt à interdire à ImageSat de vendre ses images dès que les États-Unis le demanderaient.

18 octobre 2001 : Selon Intelligence Online, le déménagement de la base allemande Bad Aibling est reporté, à l'issue de discussions entre les ministères de la Défense allemand et américain, en raison des attentats du 11 septembre.

18 octobre 2001 : La NSA sort la 3e partie de sa version de Linux : le prototype SELINUX LSM vient d'être mis en ligne, doté de plusieurs corrections d'erreurs et des améliorations de sécurité.

Fin octobre 2001 : Selon Intelligence Online les multiples échanges entre la NSA et un fournisseur tel que World Com UUnet rendraient crédible une intervention des services de sécurité US dans les serveurs de l'opérateur, en cas de crise grave. (cf. les cônes de silence).

1er novembre 2001 : Selon TTU, l'Indian Space Research Organisation (ISRO) a procédé au lancement du Technology Experiment Satellite officiellement destiné à tester les technologies nécessaires aux futurs satellites-espions ainsi qu'aux IRS-2. Sa caméra panchromatique serait capable d'une résolution inférieure à 2,5 mètres — certaines sources n'hésitant pas à placer la barre à un mètre. Le programme aurait du reste été lancé en juillet 1999, peu après les événements de Kargil et le premier test du missile de portée intermédiaire pakistanais Ghauri-2, en avril 1999.

4 novembre 2001 : Le New York Times révèle qu'une station secrète de la CIA se trouvant sous le WTC a été détruite par les attentats du 11 septembre, provoquant d'importantes difficultés dans la gestion du Renseignement US.

9 novembre 2001 : La CIA pourrait bien devenir le nouveau VC à la mode dans la Silicon Valley : l'agence de renseignements américaine, sur la sellette depuis les attentats terroristes du 11 septembre, n'hésite pas à financer les start-ups susceptibles de l'aider dans la lutte antiterroriste via son fonds In-QTet.

10 novembre 2001 : Une commission créée à la demande du Président Bush à la suite 11 septembre propose de restructurer la Communauté du Renseignement Militaire Américain et d'en confier la tête à la CIA qui dirigerait la NSA, le NRO et la National Imagery and Mapping Agency (chargée d'interpréter les photos satellites et de créer les cartes militaires). Ainsi tout le Renseignement US, militaire et civil, électronique et humain, serait rassemblé en une seule institution ! Les conclusions définitives seront rendues le mois prochain.

14 novembre 2001 : la NSA vient de fermer le Musée National de la Cryptographie « pour une période non déterminée ».

22 novembre 2001 : Selon TTU, la mise en place du projet Groundbreaker au sein de la NSA est en passe de provoquer des mouvements sociaux. Une menace de licenciement de 400 techniciens a déjà provoqué des débrayages. À cela s'ajoute le flou qui entoure l'avenir de la NSA : elle pourrait être dissoute et passer sous le contrôle de la CIA.

24 novembre 2001 : Le Sénat américain a voté le Patriot Act qui vise à renforcer les moyens d'écoutes, de surveillance et de contrôle des communications du territoire national par l'emploi du système Carnivore (rebaptisé DCS 1000), complètement amélioré du système Echelon. C'est un pas de plus dans la tentative de maîtrise totale de l'information.

29 novembre 2001 : La firme Booz Allen & Hamilton a développé à la demande du FBI un nouveau virus de type keylogger, Magic Lantern, qui, agrégé au système Carnivore, réalise des intrusions et des écoutes électroniques. Il enregistre les frappes d'un clavier avant que, par exemple, les informations ne soient cryptées ou supprimées. Il comporte enfin une base de données réservée à l'enregistrement de mots clés à rechercher dans la machine cible. (Intelligence Online).

3 décembre 2001 : Microsoft apprécie peu la perspective de voir Windows NT, qui équipe les ordinateurs des parlementaires allemands au Bundestag, remplacé par un système d'exploitation à base de noyau Linux. C'est pourquoi l'éditeur a décidé de permettre à la présidence du Parlement, ainsi qu'à la Commission pour les technologies de l'information et de la communication, d'avoir accès au code source de Windows.

6 décembre 2001 : Le ministère américain du commerce (US Department of Commerce) vient d'approuver un standard de cryptage des données, l'Advanced Encryption Standard (AES), qui a pour vocation de protéger les données d'ordre personnel et financier utilisées par le gouvernement, ou dans le cadre d'échanges commerciaux. Il remplace les deux normes actuellement utilisées, le protocole Triple DES et le Data Encryption Standard (DES), adopté en 1977 par le National Institute of Standards and Technology (NIST), une antenne du ministère du Commerce américain. L'AES supporte des clés de codage à 128, 192 et 256 bits, alors que le DES ne supportait que les clés à 56 bits.

7 décembre 2001 : Lockheed Martin Corp. a annoncé que plus de la moitié de sa division télécommunications serait démantelée et largement liquidée. Lockheed Martin va également tenter de vendre ses parts dans plusieurs sociétés de communications, comme Intelsat (24 %), Inmarsat (14 %), New Skies Satellites N.V. (14%), Americom Asia-Pacific (50 %).

10 décembre 2001 : Quatre fabricants de logiciels antivirus (Symantec, McAfee, Trend Micro, Sophos) ont déclaré qu'ils n'ouvriraient pas la porte au virus/ver de surveillance électronique du FBI. Cette décision serait davantage liée aux activités de certains fabricants dans des marchés émergents (comme la Chine) qu'à des préoccupations d'ordre éthique pour les clients actuels (Les Chroniques de Cybérie).

12 décembre 2001 : Un porte-parole du FBI l'a reconnu : le développement de Magic Lantern est en cours. Ce logiciel, dont l'existence a été révélée pour la première fois par la chaîne Internet MSNBC en novembre, appartient à la catégorie des keyloggers. Installé sur un micro-ordinateur, le keylogger surveille et garde en mémoire les touches frappées au clavier par l'utilisateur. Lorsque quelqu'un crypte ses communications avec un logiciel trop difficile à casser, il est beaucoup plus simple de découvrir son mot de passe ou bien le contenu de ses messages en récupérant les données du keylogger.

13 décembre 2001 : Le FBI et les douanes américaines épaulés par l'Australie, le Royaume-Uni, la Finlande et la Norvège ont démantelé mardi 11 décembre un réseau mondial de pirates informatiques qui fournissait sur la toile des copies illégales de programmes.

14 décembre 2001 : Les services de renseignement américains, dont l'efficacité a été mise en doute par les attentats du 11 septembre, verront leur budget augmenter de 8 %

l'an prochain. L'augmentation des crédits à la CIA, à la NSA (National Security Agency) et aux autres services de renseignement, a été entérinée à l'unanimité par le Sénat jeudi soir. Le budget actuel est d'environ 30 milliards de dollars.

L'augmentation servira notamment à accroître les moyens « humains » de la CIA et à recruter de nouveaux spécialistes de langues ou dialectes, deux domaines dont les carences ont été mises en lumière par les attentats de New York et Washington. (Reuter)

17 décembre 2001 : Après le lancement réussi le 10 décembre de « Maroc-Tubsat », le Maroc est, après l'Égypte et l'Arabie Saoudite, le troisième pays du monde arabe musulman à disposer d'un satellite spatial, rapporte lundi la télévision marocaine 2M. Entièrement conçu par des chercheurs marocains,

« Maroc-Tubsat », dont les tests de fonctionnalité ont été réalisés en partenariat avec l'université de Berlin, a été lancé à bord de la fusée russe Zenit depuis la base de Baïkonour (Kazakhstan). Pesant environ 50 kilos, ce satellite assurera, selon l'agence officielle de presse marocaine MAP, « quatre missions : observation de la terre, messagerie, collecte de données et localisation ».

21 décembre 2001 : Les états arabes du Conseil de coopération du Golfe (CCG) envisagent d'acheter leur propre satellite-espion. Ce besoin a été mis en lumière lors de la guerre contre l'Afghanistan : les Émirats Arabes Unis, membres du Conseil, ont été incapables d'obtenir des images satellites de l'Afghanistan malgré leur contrat avec la société américaine Space Imaging Inc (le Pentagone avait obtenu l'exclusivité des photos de l'Afghanistan prises par le satellite Ikonos de Space Imaging).

Vers un projet européen

Tout le monde espionne tout le monde. Et le plus riche sera le mieux informé.

Ces projets demandent énormément d'argent pour être menés à bien. Le projet européen est en marche et fait beaucoup de bruits aux USA, qui y sont farouchement opposés. La Grande-Bretagne doit d'abord s'affranchir de ses alliances avec les États-Unis,

Nous n'en sommes qu'au début. En dehors des pays anglophones, il émerge un axe France-Allemagne au niveau de l'intelligence économique et l'espionnage. Les Américains essayent actuellement de partager Echelon avec le plus de pays européens possible tout en tenant à l'écart l'Allemagne et la France.

Le Danemark, la Suisse, la Finlande sont par exemple déjà du côté américain .

Pourtant, Echelon n'est pas un enfant du baby-boom paranoïde de la guerre froide, mais un instrument du bloc USA/Royaume-Uni destiné prioritairement à surveiller les autres pays du bloc de l'Ouest.

Une formidable façon pour les États-Unis de suivre les évolutions des bénéficiaires du Plan Marshall et d'acquérir en temps réel toute information plus ou moins confidentielle qui transiterait sur les ondes : fax, email, téléphone, tout y passe.

Les Français, dindons de la farce, tentent de rattraper le retard accumulé lors des années Balladur.

A l'initiative du Parlement européen, ce rapport dense, mais très clair, car retravaillé entièrement pour un public de non-techniciens, démystifie la paranoïa très Roswellienne du mythe Echelon (« on nous ment, on ne nous dit rien ») pour la remplacer par un factuel très parlant : les services secrets américains ont pu pendant des années connaître ce qu'ils souhaitaient des secrets d'États locaux. Exit donc toute confidentialité économique ou politique ; pas besoin de ligne rouge vers le bureau ovale.

Echelon, lui, écoutait tout. Avec la plainte internationale déposée par l'ancien juge d'instruction Thierry Jean-Pierre (député européen), ce rapport très documenté devrait jeter un pavé dans la mare trop tranquille des relations Europe/États-Unis....