MANUEL

DE

CONTRE-MESURES

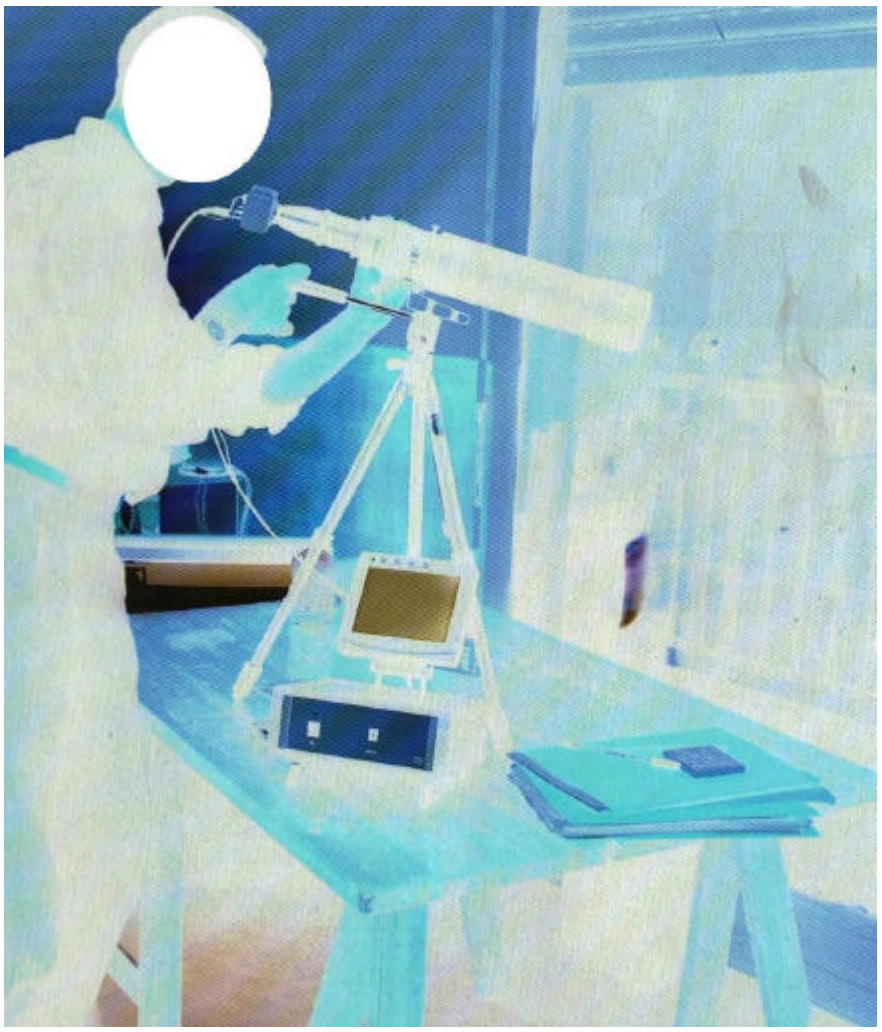
ELECTRONIQUES

Edition numéro 1

Octobre 2003

By RadioZ

CRCF Member



Comment combattre l'épidémie des écoutes clandestines, les interceptions illégales, les surveillances électroniques, la fuite d'information…

Qui veut vous espionner ? Concurrents ? Services de renseignements étrangers ?
Par quelles informations pourraient être intéressés vos agresseurs ? Commerciales ? Nouveaux brevets ?
Comment pourraient ils vous atteindre ? Ecoutes illégales ? Interceptions ?
Quand êtes vous le plus vulnérable ? Au bureau ? Au domicile ? En voiture ? En déplacement : à l'hôtel ?
Comment peut-on vous attaquer ?
Etes vous vulnérable ?

Autant de questions auxquelles vous serez à même de répondre à l'issue de ce dossier spécial et unique : surveillances électroniques, les nouvelles menaces…

Les risques évoluent sans cesse, le terrorisme et le grand banditisme gagnent tous les continents, la violence augmente, les technologies offensives évoluent également facilitant ainsi un nouveau fléau : le vol d'informations. De cette nouvelle menace est née une nouvelle activité : les contre-mesures électroniques plus communément appelées ***TSCM pour Technical Surveillance Counter Measures*** : debugging afin de lutter efficacement contre ce pillage de patrimoine intellectuel. L'interconnexion des systèmes d'information s'amplifie de jour en jour afin de faciliter la compétitivité des entreprises, des administrations et des grandes institutions. De ce fait, l'information regroupée devient plus vulnérable si l'on ne prend pas quelques précautions. L'explosion des moyens de communication (téléphones portables, modem, Internet, e-mails...) a également contribué à accroître les risques d'interception et de fuite d'informations.
Malheureusement, les responsables de sécurité n'ont pas tous le temps (ni les budgets) de se former ni de s'adapter à ces nouvelles technologies. Tous prétendent avoir tout prévu, mais leur manque de connaissances approfondies risque d'être à l'origine de gigantesques failles sécuritaires involontaires...
En effet, les technologies évoluent très vite et nécessitent une remise en cause, une remise en question perpétuelle. Parallèlement à cette formation nécessaire, une évolution matérielle est également indispensable. Le souci majeur est que cette formation requiert des entreprises, des administrations, des budgets colossaux et du temps... Sont-elles prêtes à faire ces investissements et en ont-elles les moyens... ?

VALEUR DE L'INFORMATION

De nombreux responsables ou dirigeants minimisent l'importance de l'information et les risques liés au vol de celle-ci. L'information est la valeur la plus importante d'une entreprise ou d'une organisation. Malheureusement, sa protection est rarement assurée de la même façon que la sécurité de l'entreprise face à l'effraction ou la protection du dirigeant face aux risques de kidnapping ou d'assassinat. Qu'elle soit d'ordre financière, commerciale, politique, projet de développement, l'information est la véritable richesse d'une entreprise ou de ceux qui la détiennent.

L'information peut être obtenue par des voies légales ou des voies non légales.
L'obtention d'informations par voie légale se fait via les sources ouvertes (les informations communiquées par la presse écrite ou orale, la télévision, la radio, les sites Internet, la presse spécialisée, les plaquettes commerciales, les interviews... sont autant de mines d'informations légales , d'où l'importance d'un responsable ou d'un service de vérification, de censure chargé de s'assurer que le cumul d'informations communiquées ne permettent pas de trahir des secrets ou de définir une nouvelle politique...). La seconde méthode, totalement illégale celle-ci, est l'obtention d'informations à l'insu de son détenteur et propriétaire : technique totalement prohibée et réglementée en France.Le coût des pertes financières dues à ces interceptions, écoutes et vols d'informations est incalculable... La menace est réelle et très sérieuse. Chaque personne, chaque organisation ou chaque entreprise est potentiellement une cible. Il existe de nos jours une réelle industrie de matériels de surveillance électronique, d'écoute ou d'interception. Cette nouvelle industrie génère une véritable économie évaluée rien que pour les États -Unis à plus de 2 milliards de dollars par an.

Cependant une méthodologie sécuritaire adaptée permettent, à peu de frais, de lutter efficacement et de minimiser ce type de risque ; le tout couplé à de fréquentes vérifications TSCM... De nos jours, les progrès technologiques permettent d'écouter, d'intercepter des conversations, des fax, des e-mails, des conversations satellites, des transferts de données ou de fichiers informatiques... Il n'existe pas de réelles statistiques sur l'augmentation de ces nouvelles menaces. Cependant, on assiste à une véritable explosion de ce marché et un accroissement incalculable de nouveaux consultants, de sociétés privées de sécurité, de sociétés d'investigation qui profitent de cette nouvelle industrie. Les vulnérabilités découlant de cette avancée technologique et de l'évolution de l'espionnage sous toutes ses formes sont ce que l'on nomme Les Nouvelles Menaces...

Nous assistons depuis ces dernières années à un accroissement démesuré voire à une explosion non seulement des techniques offensives, mais également de l'espionnage technologique, comme si la seule solution de développer de nouveaux produits, de nouveaux marchés pour une grande compagnie, était de voler l'idée à son concurrent... De plus, la sophistication des moyens d'écoutes, d'interceptions et d'espionnage, leur miniaturisation ainsi que leur baisse de coût ont mis ces produits à la portée de tous... L'une des plus importantes causes des pertes ou des vols d'informations provient des ordinateurs portables. Les utilisateurs voient en cet outil compact, facile à transporter seulement le côté pratique, mais ne sont malheureusement pas sensibilisés sur les conséquences de la disparition de celui-ci. Dans la plupart des cas, ils détiennent une importante partie commerciale, une partie communication, et dans le pire des cas, des projets d'évolution de l'entreprise (fusion, rachat...), des développements en cours, et peut être même les résultats d'années de recherche d'un nouveau produit : le patrimoine de l'entreprise, sa véritable richesse. Ils peuvent aussi contenir également des informations d'ordre militaire...

Pourtant, les ordinateurs portables «traînent» sur des bureaux sans surveillance alors que des personnes extérieures à l'entreprise interviennent dans les locaux (ouvriers, services de maintenance, réparateurs, réapprovisionnement des distributeurs de toutes sortes : boissons, café...). Or objectivement, avez-vous toujours effectué un contrôle strict des éléments extérieurs venus dans vos locaux : appel pour vérifier le rendez-vous, la transmission du nom du ou des intervenants et la vérification sur place de l'identité des personnes ? Sans avoir aucun préjugé sur les techniciens, réparateurs... l'usurpation de leur identité est la solution la plus simple pour évoluer dans un site sans attirer l'attention et circuler librement. Ces ordinateurs restent ouverts et allumés sans surveillance lors de la pause café ou du déjeuner ; ils sont laissés dans les coffres de voiture... ou pire encore dans les chambres d'hôtels lors de négociations en déplacement ou à l'étranger...

AUTO-DIAGNOSTIC DES RISQUES ENCOURUS PAR VOTRE ENTREPRISE PAR RAPPORT À SES ACTIVITÉS ET SON ENVIRONNEMENT

Quelques situations générant une augmentation du risque :

-Votre société détient-elle des informations qui pourraient intéresser la concurrence ?
-Savez-vous si votre société est une cible ?
-Prenez-vous des mesures suffisantes pour assurer la protection de l'information ?
- Adoptez-vous une politique de contre-espionnage
- Cette politique est-elle gérée par un responsable ou par un département spécifique
- Etes-vous tenu informé (le l'évolution des menaces ou des menaces elles-mêmes
- Avez-vous répertorié dans votre entreprise qui détient, négocie des informations sensibles ou confidentielles ?
- Savez-vous exactement qui dans l'entreprise à accès à ces informations confidentielles ?
- Votre personnel est-il sensibilisé face aux risques d'approches extérieures pour l'obtention d'informations confidentielles sur l'entreprise ou ses activités
- Votre personnel connaît-il la marche à suivre en cas d'approches ?
- Votre personnel vous rapporte-t-il d'éventuelles suspicions de vol d'information ?
- Des procédures sont-elles mises en place face à ces risques ?
- Votre personnel chargé de la sécurité de l'entreprise est-il sensibilisé et formé à ces risques ?
- Votre personnel reçoit-il régulièrement des informations sur les nouvelles menaces
- Votre société possède-t-elle sa propre équipe de contre-mesures électroniques ou fait-elle appel régulièrement à une société extérieure ?
- Votre société a-t-elle instauré une politique de vérification de l'ancienneté des personnels avant embauche, y compris celui des services de sécurité ?
- Détenez-vous des informations sensibles ou confidentielles : des secrets de fabrication
-Votre société travaille-t-elle avec l'armée, le gouvernement ?
-Votre société évolue-t-elle sur des marchés mondiaux ?
-La réussite financière de votre entreprise dépend-t-elle d'un secret de fabrication ?
- Et si oui, votre société survivrait-elle en cas de vol de ce secret, de cette information capitale, ou d'un brevet encore non protégé... ?
- Votre entreprise travaille-t-elle sur un développement capital pour les prochaines années ?
- Votre société va-t-elle subir une modification : fusion, rachat, cession... ?

Ou plus simplement :
- Etes-vous en procédure de divorce ?
- La moindre fuite d'information pourrait-elle être fatale pour votre entreprise ?
-Avez-vous repéré la présence de personnes étrangères au service dans des lieux où elles n'auraient pas dû se trouver sans y être autorisées ?
-Avez-vous entendu dernièrement des sons étranges sur vos lignes téléphoniques ?
- Des interférences sont-elles brusquement apparues sur la radio, le réseau électrique (circuit lumière) ou sur la télévision.

Si vous avez répondu OUI à plus d'une question,
vous êtes une cible potentielle... de ces nouvelles menaces d'espionnage...

LES ÉCOUTES "LÉGALES" ET "ILLÉGALES"

On distingue deux types d'écoutes :

ÉCOUTES SAUVAGES

- Les écoutes non officielles, les interceptions de communications téléphoniques non pratiquées par une autorité publique officiellement mandatée, les écoutes effectuées en dehors de toute norme juridique ou au mépris total des règles existantes. Elles sont susceptibles de constituer une infraction prévue et réprimée par le Code Pénal ; notamment celles énoncées par l'art. 1er de la loi du 10 juillet 1991 concernant le secret des correspondances émises par voie des télécommunications (Selon l'art. L32 du Code des Postes et Télécommunications, on entend par télécommunication toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de renseignements de toute manière par fil, optique, radioélectricité ou autres systèmes électromagnétiques) et réprimées par l'art. 15 du Code Pénal découlant du fait d'intercepter, de détourner ou de divulguer des correspondances émises par voie de télécommunication ou découlant de l'installation d'appareils conçus pour effectuer de telles interceptions.

- Tout enregistrement ou transmission de paroles prononcées par une personne à titre privé ou confidentiel sans son consentement ; toute captation directe qu'elle soit effectuée dans un lieu privé ou public constitue une infraction à partir du moment où elle est effectuée à l'insu de la dite personne et est pénalement réprimée par l'art. 226-1 du Code Pénal.

ÉCOUTES OFFICIELLES

Deux seuls types d'écoutes officielles sont autorisées par la loi :
Les interceptions officielles effectuées dans le cadre d'une CR (Commission Rogatoire) lors d'une enquête judiciaire ordonnée par un Juge d'Instruction pour les besoins d'une enquête criminelle ou correctionnelle (seulement si la peine encourue est supérieure à deux ans), celles autorisées par le Premier Ministre, suite à une demande du Ministre de l'Intérieur, de la Défense, ou du Ministère chargé des Douanes. L'ensemble de ces différentes écoutes est sévèrement réglementé par la loi du 10 juillet 1991, mais ne prend pas en compte les écoutes du type microphoniques.

Une autre forme d'écoute légale s'implante de plus en plus actuellement : les écoutes sur le lieu de travail. De plus en plus d'entreprises doivent garder une trace des conversations téléphoniques : le secteur bancaire, les établissements financiers principalement pour les transactions boursières ; plus précisément les ordres passés par téléphone, dans le milieu de le vente par correspondance, les sociétés de télésurveillance, de taxi, de jeux télévisés, les services de secours d'urgence ou de dépannage afin de s'assurer de la bonne prise en compte et du traitement d'une demande ; le milieu carcéral pour certaines catégories de personnes privées du droit de correspondre librement : certains détenus.

Le but de ces enregistrements est de garder une trace, un élément de preuve afin de se prémunir contre tout litige, toute action en justice. Mais ils servent également pour la vérification et l'amélioration des relations, des rapports entre les membres de l'entreprise et la clientèle : la qualité de l'accueil et les discours tenus sont ainsi vérifiables et éventuellement améliorés. Ils sont aussi une preuve de confidentialité des informations internes à l'entreprise. D'autres motifs tels que la volonté de limiter les usages abusifs du téléphone à des fins personnelles sont également admis.
L'acquisition de matériels permettant ces enregistrements ainsi que les durées de stockage des conversations sont excessivement réglementées. Ces durées oscillent entre deux jours et deux mois afin de limiter les risques d'abus. Toute durée supérieure doit être sérieusement motivée pour être acceptée. En effet, depuis quelques années, les informations transmises de façon orale sont de plus en plus importantes et nombreuses et se sont substituées à l'écrit. Cette évolution est à l'origine du développement de ces pratiques d'enregistrement de conversations téléphoniques.

Mais attention, ces enregistrements de communications ou la sonorisation de certains locaux sont très strictement réglementés, et ne sont acceptés que dans le cas de l'intérêt de l'entreprise, et à condition expresse que tout le personnel de l'entreprise en soit averti et dans certains cas après consultation du CE (Comité d'Entreprise).

Afin de veiller au bon déroulement de ces écoutes, au strict respect de la législation, une commission a été créée : la C.N.C.I.S. : Commission Nationale de Contrôle des Interceptions de Sécurité. La mission première de la C.N.C.I.S. est la vérification de la légalité des autorisations d'interceptions : le contrôle des institutions de l'État. Cette vérification se traduit par un contrôle systématique et exhaustif de l'ensemble des demandes. Chaque année, cette commission rédige un rapport d'activité communiquant un bilan chiffré et commenté des interceptions réalisées et rappelant les différentes facettes des contrôles exercés par cette Commission. Une partie est également réservée à l'étude des différentes jurisprudences européennes et françaises.
Elle oeuvre pour garantir la protection des libertés individuelles.

CERTAINS SECTEURS D'ACTIVITÉ À RISQUE SONT PLUS PARTICULIEREMENT VISÉS

- Les ambassades et bureaux de représentations étrangers.
- Les cabinets d'avocats internationaux.
- Les bureaux d'étude.
- Certains organismes d'audit, de consultants.
- Le milieu de l'armement, du nucléaire, de la recherche.
- Les puissants groupes internationaux.
- Les groupes pétroliers.
- Les sociétés spécialisées dans les transactions financières, cession, rachat.
- Le milieu boursier et ses conseillers.
- Les acteurs économiques puissants.
- Les opérateurs télécom et bien d'autres encore...

LES RISQUES INTÉRIEURS

Les interceptions locales nécessitant des intrusions dans les locaux à surveiller :

- les micros émetteurs RF (Radio Fréquence), analogiques, numériques, à sauts de fréquence, à étalement de spectre, Burst.
- les micros courant porteur utilisant les circuits électriques 220 Volts ;
- les micros IR (infrarouge) et US (ultrasons) ;
- les interceptions, les écoutes téléphoniques;
- la déviation de lignes ou d'interphones ;
- les micros filaires utilisant le câblage téléphonique ;
- les micros filaires utilisant un câblage spécifique (sonorisation musicale des locaux, interphones...) ;
- les micros fibres optiques ;
- les micros transpondeurs ;
- les systèmes à induction ;
- les systèmes d'enregistrement numériques ou analogiques cachés ou connectés aux lignes téléphoniques;
- surveillance vidéo RF ;
- interception de fax, modems, claviers sans fils ;
- duplications clandestines de disques durs d'ordinateur ;
- piégeage de véhicules ;
- reprogrammation des PABX.

Les véritables dangers encourus par les entreprises ne viennent pas des écoutes officielles mais des interceptions clandestines illégales.
Différents matériels, techniques et modes opératoires offensifs sont existants pour obtenir des informations. Les risques peuvent venir de l'intérieur ou de l'extérieur.

LES RISQUES INTÉRIEURS

Les moyens d'interception locale suivants nécessitent obligatoirement pour leurs mises en place une intrusion dans les locaux à surveiller.

I) Les micros émetteurs RF (Radio Fréquence), analogiques, numériques, à sauts de fréquences, à étalement de spectre, burst... sont plus communément appelés micro émetteurs.

Autonomes, compacts, ils peuvent être à déclenchement VOX (présence de bruit ou de parole), horaire, déclenchement RF à distance (par une émission à courte distance par le piégeur), déclenchement optique (présence de lumière artificielle ou du jour)...

Leur fréquence de transmission peut être :

-ELF (Extremely Low Frequency),
-VLF (Very Low Frequency : très basses fréquences 3 KHz - 30 KHz),
-LF (Low Frequency, basses fréquences : 30 KHz-300 KHz),
-MF (Medium Frequency moyennes fréquences 300 KHz - 3000 KHz),
-HF (High frequency, hautes fréquences : 3 MHz - 30 MHz),
-VHF (Very High Frequency : très hautes fréquences : 30 MHz - 300 MHz),
-UHF (Ultra High Frequency, Ultra Hautes fréquences : 300 MHz - 3 000 MHz),
-SHF (Super Hight Frequency, supra hautes fréquences : 3 GHz - 30 GHz),
-EHF (Extremely High Frequency : 30 GHz - 300 GHz).

Leur technologie de transmission peut être :

-à fréquence simple, fixe pré-programmée,
-piloté par Quartz, PLL (Phase Locked Loop),
-VCO (Voltage Controlated Oscilator),
-AM (Modulation d'amplitude),
-FM (Modulation de Fréquence),
-WFM , NFM (wide & Narrow FM bande : Bande FM large et étroite),
-SSB (Single Side Band) USB LSB,
-sous porteuse à étalement de spectre (émission sur une fréquence étalée) rendant très difficile leur détection,
-Burst (technologie de compression afin de minimiser la durée de transmission informations en salves de très courtes durées),
-mono ou stéréo,
-numérique ou analogique,
-crypté afin que seul le destinataire puisse écouter et décoder la transmission,
de technologie Gsm...

Moins ils sont puissants, plus ils sont difficiles à détecter... certes leur distance d'émission s'en trouve réduite, mais seuls des matériels des plus performants peuvent les détecter. Ils peuvent se présenter sous différentes formes : petit boîtier simple ou camouflé : intégré dans des objets usuels courants : briquet, pendule, montre, horloge, capuchon de stylo, porte documents...

Avantage : Discrétion, facilité de dissimulation, temps de mise en place très court...

Inconvénients : leur autonomie est directement liée à la place disponible de la partie alimentation, elle-même liée à la puissance. En effet, plus le micro est puissant, plus son autonomie en sera réduite.

Ces micros peuvent être classés en deux catégories différentes ceux conçus pour être placés et laissés dans les locaux à surveiller (cachés dans des cendriers, des calculatrices, des pendules de bureaux, des horloges, dans un cadre, les murs, les mobiliers, un faux-plafond, une gaine technique...), et les micros compacts camouflés dans divers objets, introduits momentanément par le porteur durant un rendez-vous, une réunion. Ces micros à faible autonomie, donc très compacts peuvent être camouflés dans une montre, une mallette, un stylo; un livre...

2) Les micros courant porteur.

Des micros CP (courant porteur) utilisant les circuits électriques 220 volts non seulement comme alimentation, mais surtout comme vecteur de communication et moyen de transport du signal.

Ils peuvent être intégrés dans n'importe quel objet usuel raccordé au secteur : lampe, horloge, prise murale ou multiple, ou directement installés dans une prise électrique.

Cette technologie présente plusieurs avantages : la fourniture permanente de l'énergie d'alimentation du système évitant ainsi un retour sur les lieux pour changer les batteries ou piles, d'où une utilisation illimitée jusqu'à leur démontage ou découverte ; la discrétion et la simplicité de mise en place : pas besoins de démontage, ni d'aménagements spécifiques si l'on utilise la procédure de substitution d'un élément décoratif de la pièce (une lampe de bureau, une horloge...), difficilement détectable si l'on ne détient pas les matériels adéquats de détections, la possibilité de récupérer l'information de n'importe quel local intérieur sur une phase commune même au-delà des limites du bâtiment espionné ainsi qu'un coût modique.

Inconvénient : si plusieurs circuits électriques existent, circuit usuel, circuit spécifique installations informatiques, un repérage long et fastidieux préalable sera indispensable, et l'assurance qu'aucun filtre secteur ne soit présent. De même, le signal ne passera pas un transformateur.

3) Les micros I.R. (infrarouges) et U.S. (ultrasons).

Le micro I.R. transforme le signal audio de l'ambiance de la pièce piégée en un rayon infrarouge émis par une diode LED (Light Emitting Diode) invisible à l'oeil nu afin de transmettre les informations. Ces informations sont ensuite récupérées puis retransformées par le récepteur.

Cette transmission ne peut se faire qu'en ligne droite et ne doit pas être gênée par un obstacle sous peine de rupture de liaison. L'avantage de cette technologie est de ne pas rayonner d'émissions RF (très facilement détectables). Les dispositifs d'émission et de réception infrarouges ont comme inconvénient majeur de ne fonctionner qu'en portée optique, si un obstacle coupe la trajectoire du faisceau, il stoppe immédiatement la transmission. Cette technologie ne peut pas traverser les murs. Ils sont généralement positionnés près des fenêtres. N'émettant aucun rayonnement RF, ils ont par contre l'avantage d'être indétectables par des professionnels ne disposant pas de détecteur I.R. Très discrets, ces micros I.R. sont peu employés en raison des différentes contraintes de portée optique.

4) Les micros U.S. (ultrasons).

De la même façon que le système I.R., le micro U.S. transforme le signal audio de l'ambiance de la pièce piégée en un signal ultrason inaudible pour l'oreille humaine afin de transmettre les informations. Ces informations sont également récupérées puis retransformées par le récepteur.

5) Les interceptions et écoutes téléphoniques.

Il s'agit par différentes techniques de piégeage : de positionner des systèmes d'enregistrements numériques ou analogiques ou micros RF sur les lignes, d'effectuer des dérivations afin de capter des signaux électriques qui acheminent des sons sur le réseau téléphonique de l'entreprise, de détourner des lignes par piratage informatique de PABX (autocommutateur), de mise en place de BYPASS pour la récupération du signal analogique et renvoi de celui-ci, soit par émetteur RF (détectable par l'analyse spectrale), soit par l'utilisation d'une paire libre du câble téléphonique. Les lieux privilégiés pour la mise en place d'une dérivation sont l'autocom, les sous-répartiteurs d'étages (à ces endroits, le repérage des lignes y est le plus aisé) ; les armoires de centralisation des différents immeubles ou bâtiments sur les lieux publics peuvent également être utilisées.

Il existe un autre moyen d'espionnage permettant la capture des sons de la pièce par l'utilisation de la pastille micro du téléphone rapatriant ainsi soit les conversations téléphoniques, soit l'ambiance de la pièce lorsque le combiné est raccroché. La solution la plus rapide, 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 modifié à l'avance en y incorporant un sucre émetteur avec les inconvénients de facilité de détection et autonomie courte.

6) Les micros filaires utilisant le câblage téléphonique.

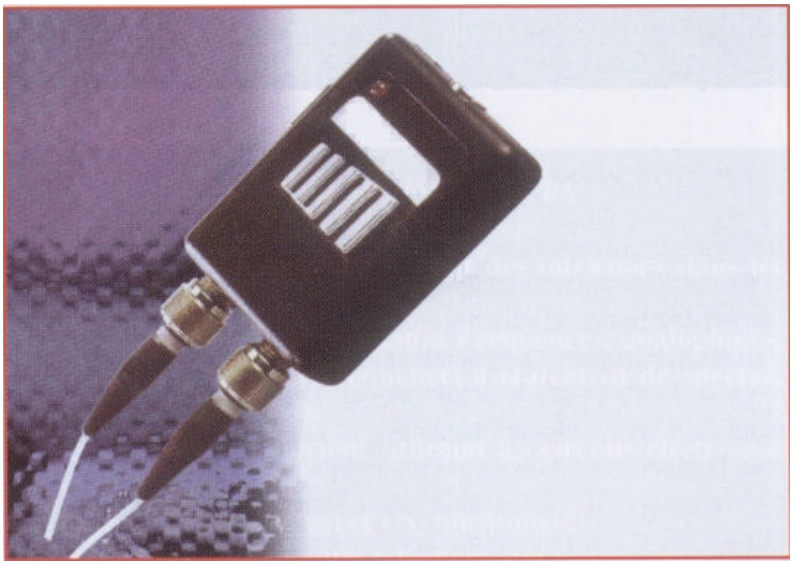
Dans de nombreux bâtiments, lors de réfection de systèmes téléphoniques, un nouveau câblage est installé, sans se donner la peine de retirer l'ancien... Il est alors également envisageable d'utiliser une paire libre d'un câblage (ou l'ancien câblage) téléphonique de l'entreprise. Étant donné que celui-ci traverse toute l'entreprise de part en part, toutes les pièces sont vulnérables, et le signal peut être récupéré facilement dans différents lieux, pièces, gaines techniques... mais également au-delà des limites de l'entreprise. D'où l'importance de bien vérifier que seuls les câbles nécessaires soient présents. Ils ne sont décelables que part l'utilisation d'ampli BF ou fouille physique approfondie des locaux.

7) Les micros filaires utilisant un câblage spécifique (sonorisation musicale des locaux, interphones...), leur propre câblage ou celui d'un d'interphone.

Très difficiles à détecter lorsque ce type de micro filaire possède son propre câblage et a été posé par des spécialistes de l'offensif, il nécessite énormément d'attention pour le mettre en évidence et un temps de pose important pour un travail discret et soigné. Il peut être mis en place lors de travaux de réfection de locaux.
Les interphones reliant les appartements, les entreprises, des locaux professionnels ou locaux éloignés peuvent être également modifiés en vue d'écoutes continues ou non par des personnes autres que les utilisateurs courants. Cette technologie permet d'utiliser des câblages déjà existants.

8) Les micros fibre optique.

Technologie de pointe permettant de convertir un signal audio en signal optique ne générant ainsi plus de perturbation. Ces produits de très petite taille, excessivement sensibles sont très difficiles à détecter et nécessitent une fouille physique très approfondie des locaux à vérifier. Le déport de l'électronique par rapport au micro peut atteindre 20 mètres.



9) Les micros type transpondeur.

Cette merveille technologique, à très faible consommation, est relativement difficile à détecter. Ce système de surveillance utilise une technologie radar relayant par le biais d'une antenne d'activation pour envoyer un signal capté par le transpondeur (camouflé dans un mur, un cadre, du mobilier...) et une antenne de réception des informations. Dans un encombrement minime, son autonomie de base lui confère une durée d'utilisation supérieure à 12 mois. Des batteries optionnelles peuvent accroître son autonomie au delà de 10 années...
Ce système est particulièrement utilisé dans le cas de surveillances longues durées, ou si l'activation doit être effectuée dans un avenir lointain par rapport à sa mise en place.

10) Les systèmes à induction.

L'utilisation d'une sonde de type Hall (effet de champs) permet l'interception des données transitant à l'intérieur d'un câble sans connexion physique. Les micros ou capteurs à induction placés à proximité immédiate d'un câble téléphonique analogique, d'un câble coaxial vidéo peuvent capter les informations qui transitent. Inconvénient de cette technologie : indétectable avec le TDR (analyseur de défauts de ligne) puisqu'il n'y a pas d'épissure dans le câble, pas de jonction ni dérivation.

11) Les systèmes d'enregistrement numériques ou analogiques cachés, ou connectés aux lignes téléphoniques.

Systèmes d'enregistrement analogiques du type magnétophone compact, dictaphone, ou numériques type DAT, pearlcorder numérique de plus en plus petits existent et possèdent des durées d'enregistrement phénoménales, décuplées par des systèmes Vox contrôle (déclenchement à la voix ou au bruit). Leurs inconvénients sont multiples : besoin de venir le mettre en place, de revenir le récupérer ou changer le support d'enregistrement. N'émettant aucun signal RF, ils ne sont détectables qu'avec un détecteur de jonctions non linéaires ou par le bais d'une inspection physique poussée. Ils peuvent soit enregistrer l'ambiance d'une pièce, soit être connectés au réseau téléphonique.

12) Surveillance vidéo RR

La démocratisation des caméras vidéo pinhole (tête d'épingle), sur le marché couplées à la banalisation d'émetteurs vidéo sur 2,4 GHz, sur 5,8 GHz (et même 7,2 GHz) possédant également la fonction intégrée de transmission de signaux audio, génère une nouvelle menace à prendre très au sérieux. En effet, lors de salons, nous avons pu observer des systèmes clandestins de transmission audio/vidéo intégrés dans des cadres, dans des pieds de statues de très petites tailles rendant les lampes de bureaux ou les horloges piégées bien obsolètes...

13) Interception de fax, modems, claviers sans fils.

Le fax est le moyen le plus rapide d'acheminer des documents entre différents sites : propositions commerciales, contrats, rapports... Ce moyen de communication a explosé depuis ces dix dernières années. Revers de la médaille, les systèmes d'interceptions de fax ont également énormément évolués. Il est en effet possible d'intercepter et d'archiver simultanément plus d'une cinquantaine de lignes fax pour des systèmes compacts et jusqu'à plus de 150 pour des plates-formes plus conséquentes. L'explosion des moyens de communication sans fil contribue également à augmenter fortement les fuites d'informations sensibles. Les améliorations des conditions de travail liées aux évolutions technologiques permettent aujourd'hui de téléphoner sans liaisons filaires, de connecter son PC portable par modem sans fils au réseau de l'entreprise... autant de nouveaux risques de vulnérabilité face aux interceptions distantes...

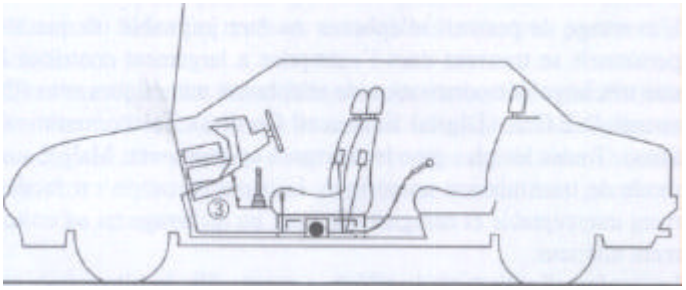
Depuis quelques mois, les nouveaux claviers informatiques sans fils font leur apparition. Certaines techniques de transmission sont de faible portée, mais d'autres rayonnent à plusieurs dizaines de mètres. Imaginez la simplicité de capture d'information...

14) Duplications clandestines de disques durs d'ordinateurs.

Nous assistons depuis peu à un nouveau phénomène de vol d'informations, après les vols de disques durs au sein même des entreprises et ce durant les heures ouvrables, une nouvelle technique est apparue : la duplication clandestine rapide de disques durs. Totalement invisible, cette technique était initialement employée par les services d'enquêtes pour recopier le contenu des disques sur commission rogatoire en vue de recherche de dossiers. Ces matériels redoutables, portatifs, autonomes et très simples d'utilisation permettent à un non spécialiste de dupliquer l'intégralité d'un disque en très peu de temps...

15) Piégeage de véhicules.

Pour les dirigeants, les hauts responsables, le véhicule de direction est le prolongement du bureau. Des négociations, des rendez-vous s'y déroulent. Pour ces raisons, la vérification périodique de ceux-ci est indispensable afin de lutter contre toute présence de système d'écoute ou de localisation. Un exemple flagrant remonte à quelques années lorsque la presse spécialisée a révélé que le véhicule utilisé par le principal représentant (Gerry Adams) du Sinn Fein Irlandais était doublement piégé, et ce depuis longtemps... : un système d'écoute doublé d'un système de localisation permettant ainsi de connaître non seulement la position exacte mais également l'ensemble des conversations, négociations, projets... Conclusion : toujours considérer son véhicule comme non sûr sauf s'il fait l'objet régulièrement d'opérations de contre-mesures électroniques et que son stationnement est toujours sécurisé (soit sous surveillance vidéo au parking de l'entreprise, soit sous l'eeil du chauffeur, soit dans un box fermé à clé et lui-même sécurisé au domicile).



16) Reprogrammation et intrusion par le PABX.

Le PABX, terme technique (également appelé PBX ou autocomutateur) est le standard téléphonique. C'est ni plus ni moi qu'un ordinateur spécifique dédié à la gestion du système téléphonique de l'entreprise permettant le raccordement de l'ensemble c postes téléphoniques de l'entreprise ainsi que certains autres terminaux spécialisés : terminaux informatiques, équipements d'audio ou de visioconférence, applications informatiques liées à la téléphonie, équipements pour téléphones mobiles, systèmes gestionnaires des coûts de télécommunications, équipements de diffusion de messages ou de musique au réseau de télécommunication public numérique.

Il donne également accès à des services téléphoniques avancé les PABX intègrent des fonctions de CTI (couplage téléphonie informatique), des fonctions de mobilité (postes mobiles numériques sans fils du type DECT)... Tous les PABX (autocommutateurs) possèdent une ligne de télémaintenance (via modem) pour les vérifications, paramétrages distants, vérifications de bon fonctionnement, corrections de programmes, dépannages afin de minimiser les déplacements sur sites. Le revers de la médaille, est que, cette liaison avec l'extérieur peut être également utilisée de façon offensive pour effectuer diverses malversations en intervenant par le biais d'une programmation distante pour...

- la création de postes fantômes,
- l'activation de la fonction conférence à l'insu de l'utilisateur du poste : le poste décroche automatiquement et se positionne en mode main libre en autonome,
- la réorientation de la communication entre deux interlocuteurs ou plus, vers une autre ligne afin de réaliser une écoute ou un enregistrement pirate...

La difficulté de détections de ces modifications est qu'il n'y a aucune intervention physique comme le câblage d'une bretelle sur une ligne.
Afin de minimiser les risques d'interventions non désirées sur le PABX, et par conséquent les intrusions clandestines au sein de l'établissement, il est fortement recommandé de noter toutes les interventions effectuées dans un registre, de vérifier l'identité et prendre en note le nom de chaque technicien intervenant sur le système, de vérifier sa carte professionnelle, et enfin de téléphoner à l'entreprise pour une vérification approfondie et une confirmation de l'identité des techniciens. D'où la nécessité pour une équipe de contre-mesures électroniques d'avoir dans son staff technique et d'utiliser les compétences d'un informaticien afin d'effectuer un contrôle rigoureux des programmations des PABX face aux risques ci-dessus énoncés.

Pour conclure, il est indispensable de privilégier plusieurs axes :

Toutes les technologies ci-dessus étudiées ou presque toutes nécessitent une pénétration dans les lieux à piéger... Par conséquent, une politique de sécurité adaptée à ces nouvelles menaces permet d'en limiter les risques. Un strict contrôle d'accès périmétrique, une vérification performante des accès des personnes à l'entreprise ou aux lieux sensibles, une interdiction totale d'accès aux installations sensibles sont le premier niveau limitant l'introduction et la pose de systèmes clandestins d'écoutes ou d'interceptions.

LES RISQUES EXTÉRIEURS

Les interceptions distantes ne nécessitant pas intrusions dans les locaux :

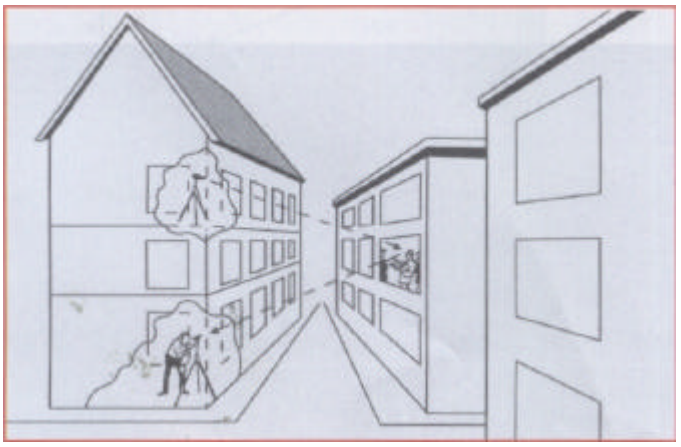
- les écoutes par technologies laser;
- les écoutes à distance par canon à son, micro parabolique ;
- les interceptions de téléphones portables GSM ;
- les interceptions de téléphones numériques sans fils D.E.C.T.
- les interceptions de pager;
- les écoutes audio de l'extérieur du briment ;
- les interceptions de claviers d'ordinateurs sans fils, de modem sans fils ;
- l'interception de communications téléphoniques satellites (Mini M, INMARSAT...)
- les observations longues distances à l'aide de télescopes, jumelles, surveillance vidéo longue distance ;
- les captures d'EMI (interception de perturbations électromagnétiques) ;
- l'interception de communications téléphoniques distantes.

LES RISQUES EXTÉRIEURS

Les interceptions distantes ne nécessitent pas d'intrusion dans les locaux.

1) Les écoutes par technologies micro laser.

Son emploi permet de capter les vibrations d'objets ou des vitres proches d'une source sonore. Le micro laser est l'une des technologies les plus complexes à mettre en oeuvre et à utiliser. Il nécessite de très bonnes connaissances techniques. En effet, un faisceau laser quitte l'émetteur, va frapper la vitre de la fenêtre cible qui vibre en fonction des bruits ou paroles générées dans le bcal, se reflète dans celle-ci, et est récupéré par la cellule du récepteur. Le récepteur transforme les vibrations récupérées du local surveillé en signaux sonores. La complexité réside dans le positionnement du dispositif, les calculs d'angle de réflexion. Ce système est d'une redoutable efficacité et est utilisable à très longue distance. La prolifération actuelle de bâtiments vitrés découlant de la modernisation architecturale risque d'accroître l'utilisation de ce type de système d'écoute.



2) Le micro parabolique.

Il est constitué d'un microphone très haute sensibilité situé au centre d'une parabole. Sa grande directivité lui permet de se focaliser sur une scène bien précise à l'aide d'un viseur (sur certains modèles) et d'éliminer une partie des bruits parasites avoisinants. Il est couplé à un amplificateur équipé de différents filtres afin de nettoyer le son des impuretés et des interférences sonores. La portée de ces systèmes est assez courte et dépend non seulement de la taille du réflecteur parabolique (minimum 60 cm de diamètre) mais surtout du milieu sonore dans lequel on utilise le micro. Le manque total de discrétion de ce système en rend son utilisation peu discrète donc rare. Des canons à sons équipés de micros très directifs fonctionnent sur le même principe d'écoute à distance.

3) Interception de téléphones portables GSM.

Différents systèmes d'écoutes et de localisation de téléphones Gsm existent. Ils se présentent soit sous la forme d'une BTS fantôme (relais de substitution) positionné entre l'utilisateur du portable et le véritable relais de l'opérateur, soit sous forme de systèmes d'interceptions passifs.
Une seconde utilisation et fonction redoutable sur les téléphones Gsm est la possibilité de paramétrer le décroché automatique (sans sonnerie) par le biais d'accessoires tels que des kits piétons. Il est alors tout à fait envisageable d'utiliser ce téléphone comme un matériel espion, qui, lorsqu'il est appelé, décroche automatiquement et retransmet l'ambiance sonore de la pièce où il a été positionné. Imaginez un tel système dans votre faux plafond de la salle de réunion, bureaux de direction... ou dans votre voiture.

4) Interception de téléphones numériques sans fils D.E.C.T.

L'avantage de pouvoir téléphoner ou être joignable où que les personnels se trouvent dans l'entreprise a largement contribué à une très large démocratisation de téléphones numériques sans fils norme D.E.C.T. (Digital Enhanced Cordless Telecommunications). Toutes les plus grandes marques en proposent. Malgré son mode de transmission numérique, la communication est facilement interceptable et enregistrable pour un archivage ou un traitement ultérieur.
Le confort d'utilisation de téléphones sans fils doit-il se faire au détriment de la sécurité de votre entreprise ... ? Pour ces raisons, si l'utilisation de téléphones D.E.C.T. est réellement indispensable et est devenue un outil indispensable au bon fonctionnement de l'entreprise... alors, si tel est le cas, tournez vous obligatoirement vers des modèles chiffrés afin de garantir une confidentialité totale pour l'entreprise, l'ambassade, le laboratoire de recherche, ou simplement le service communication... Il en est de même pour les systèmes domestiques ayant intégré bon nombre de foyers...

5) Interception de Pager.

Chaque système d'interception de pagers (radio messagerie) permet l'interception, le décodage, l'analyse, le traitement et l'archivage simultané de plus de 100 numéros en temps réel. Leurs capacités de ciblage sur ces 100 numéros de pager, la recherche par mots clés dans les messages (plus de 1500 mots clé traités en temps réel), les filtres d'exclusion dans certains messages sont autant de moyens d'obtenir des informations cruciales : code d'accès, numéros de téléphone, dates, heures et lieux de rendez-vous...

6) Ecoutes audio de l'extérieur du bâtiment ou de la pièce.

Lorsqu'il est totalement exclu de pénétrer dans le bâtiment ou les locaux «cibles», des solutions existent. L'utilisation de stéthoscopes électroniques, d'accéléromètres amplifiant les bruits, les voix à travers les vitres, les portes, les murs épais de plus d'une vingtaine de centimètres permettent une écoute de très bonne qualité. Très utilisés dans les hôtels, ils sont soit à écoute directe : l'utilisateur positionne le matériel et écoute les informations capturées sur place, soit déportés : connectés à un moyen de transmission (émetteur RF ou autre), le signal est déporté sur un lieu d'écoute et de traitement de l'information.

7) Les interceptions de claviers d'ordinateurs sans fils, de modem sans fils.

Deux solutions existent : soit le micro émetteur placé derrière le clavier saisissant au fil de l'eau toutes les frappes, soit les claviers sans liaison filaire.

Les marques les plus prestigieuses proposent aujourd'hui des claviers d'ordinateur sans fils. Les premiers accessoires à bénéficier de ce type de technologie avant-gardiste étaient les souris et Trackball. Selon les types de liaisons utilisées, leur portée varie totalement.

Que l'une ou l'autre des techniques soit employée, le résultat reste le même... l'accès à vos informations les plus confidentielles est dorénavant très simple... vos codes d'accès aux fichiers sécurisés par mot de passe, vos clés de cryptage... sont à la portée du moindre agresseur.

8) Interception de communications téléphoniques satellites (Mini M, INMARSAT...).

De tous les temps, les gouvernements ont toujours voulu connaître le contenu des communications téléphoniques satellites pour des raisons de sécurité nationale (terrorisme, grand banditisme, trafic de drogue, atteinte à la sûreté de l'État...). Le problème est que cette technologie s'est «banalisée», démocratisée et l'on trouve aujourd'hui pour des budgets abordables et nettement moins onéreux que des chaînes d'interceptions gouvernementales, des possibilités d'interception et d'écoute de ces communications particulières.

Étant donné leur coût encore élevé, ce mode de transmission n'est réservé qu'à des hauts responsables, des décideurs. Par conséquent, la valeur de ces informations sensibles est cruciale pour une entreprise. D'où la nécessité d'employer des solutions de chiffrement fort (si la législation du pays d'utilisation le permet).

9) Les observations longues distances à l'aide de télescopes, jumelles, surveillance vidéo longue distance.

L'évolution architecturale n'a pas forcement que du bon. Certes, une tour en verre est relativement esthétique, mais au niveau de la confidentialité des informations... il reste des progrès à faire. A quoi bon investir un budget annuel conséquent afin de garantir un contrôle d'accès strict, d'utiliser des solutions de sécurité informatiques, d'investir dans des formations ou des sensibilisations pour l'ensemble du personnel, si parallèlement à ces efforts, un simple télescope permet de visualiser directement l'écran informatique de l'assistante de direction, ou même du PDG... Qu'ils soient manuels (modeste télescope), vidéo, ces moyens redoutables permettent de lire des documents posés sur un bureau, positionnés sur le support de saisie incliné à côté de l'ordinateur, ou simplement à une personne sachant lire sur les lèvres de retranscrire en direct une conversation, à des distances parfois bien supérieures à 500 mètres... alors qu'un simple store, ou un film sur les vitres garantirait un premier niveau de sécurité.

10) La capture de rayonnement électromagnétique EMI (interception de perturbations électromagnétiques).

Il y a déjà de longues années, lors d'un congrès de sécurité informatique, des ingénieurs étrangers annonçaient pouvoir capter les interférences électromagnétiques générées par les matériels informatiques, plus précisément les écrans (le tube). Tout appareil électrique génère un rayonnement qui lui est propre. Ce risque d'interception à distance des perturbations électromagnétiques est un phénomène qui inquiète beaucoup les responsables sécurité.

En effet, s'il est possible de capter cette signature, il n'est donc plus indispensable de pénétrer dans le bâtiment pour y placer un système d'écoute clandestin. Les écrans d'ordinateur ne sont pas les seuls à générer des perturbations : les fax, telex, imprimantes... Seule solution : la norme TEMPEST ou la cage de Faraday. La première solution réside dans l'utilisation de matériels blindés de façon à minimiser au maximum ces fuites et la seconde d'utiliser des salles possédant un blindage mural interdisant toute fuite de rayonnement radioélectrique vers l'extérieur (solution étudiée dans la partie «moyens de défense» du présent dossier).

11) Interception de communications téléphoniques distantes.

Si aucun accès n'est possible au PABX, ni par re-programmation de celui-ci, une connexion clandestine sur la ligne numérique en amont de la TNR (terminal numérique) reste toutefois possible. Cette solution très coûteuse nécessitant de très bonnes connaissances techniques implique également un endroit discret pour cacher le matériel afin qu'il ne soit pas repéré. Par conséquent, il y a statistiquement peu de chances que cette technologie volumineuse et coûteuse soit employée.

12) Stations gouvernementales d'interception et moyens de surveillance.

Un autre type d'interception d'une performance effrayante sont les stations d'interceptions gouvernementales et les satellites : le FAPSI russe, le système Sigint en Chine, l'ILC en Écosse, San Vito dei Normanni en Italie, Chicksands en Angleterre, Karamursel en Turquie, Kirknewton en Écosse, GCHQ/NSA de Menwith Hill en Angleterre, Vint Hill Farm en Virginie, Morwenstow en Cornouaille, Yakima à Washington, Kourou en Guyane, d'autres en Israël, au Pakistan, en Inde ; mais également par satellite : les premiers satellites des USA Comint CANYON, placés près des orbites géostationnaires, une nouvelle classe de satellites Comint, CHALET, puis VORTEX renommés MERCURY, RHYOLITE, AQUACADE, RHYOLITE, MAGNUM, ORION...

Ces moyens d'interceptions totalement automatisés écoutent toutes les fréquences, toutes les communications et déclenchent les enregistrements sur présence de «mots clés programmés», sans oublier le réseau ECHELON qui à fait couler beaucoup d'encre ses 10 dernières années et les avions de surveillances équipés de moyens d'écoute et de localisation sillonnant le ciel en permanence...

LES RISQUES MOMENTANÉS

Une dernière catégorie de risques subsiste, et non des moindres !

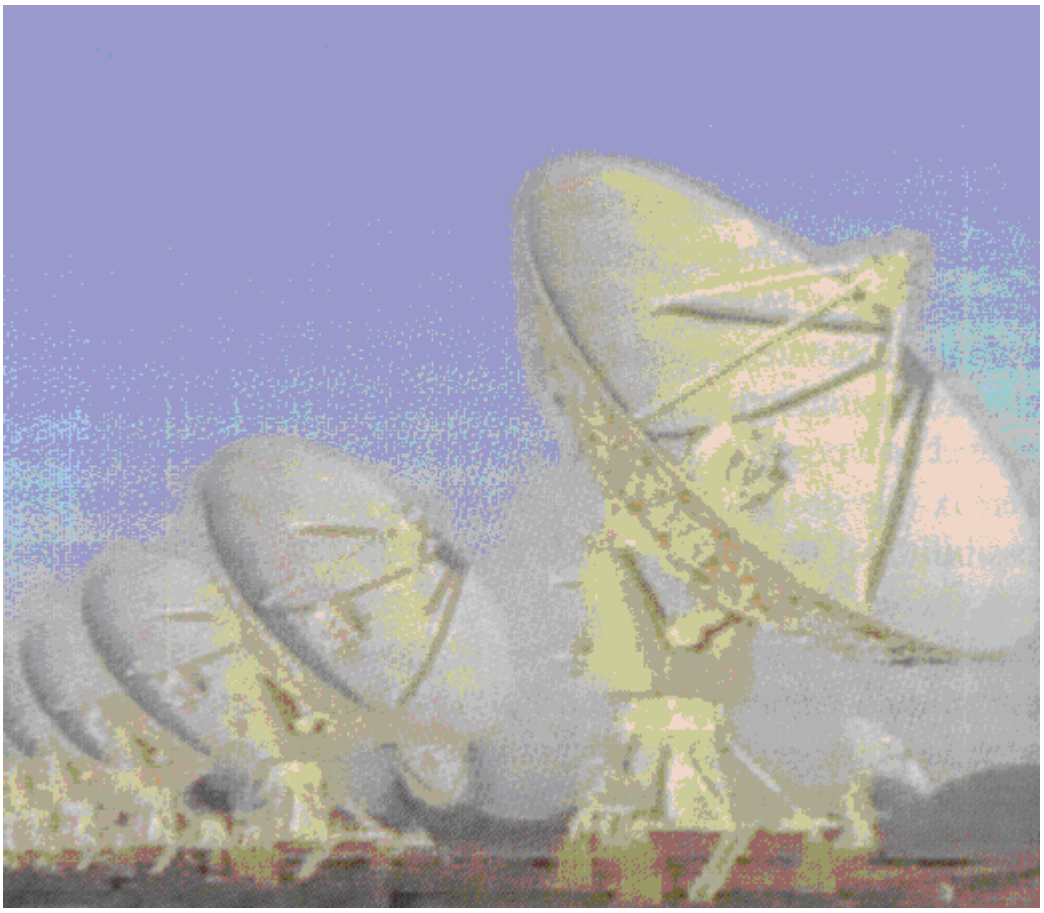
Les risques momentanés : les interceptions, les piégeages momentanés, les enregistrements durant un rendez-vous, une réunion :
- par port de micro RF
- par port de système d'enregistrement
- par port de moyens audio/vidéo camouflés dans un attaché-case.

Effectivement, le peu de statistiques et d'informations résultant des écoutes, interceptions, enregistrements clandestins, fuites d'informations, montrent que très souvent la fuite provient de l'intérieur de l'établissement, avec la collaboration ou non d'un membre du personnel, durant un événement important : réunion de direction, étude de nouveaux projets ou d'un changement politique de l'entreprise, rachat, fusion... Le moyen utilisé peut être un simple Gsm, plus sophistiqué, un Gsm d'apparence éteint à activation invisible distante ou un téléphone numérique sans fils resté par pure inadvertance ouvert et en mode d'émission, un enregistreur numérique compact, un micro RF, jusqu'aux possibilités les plus avancées : attaché-case équipé audio/vidéo camouflé... Donc, avec un minimum de vigilance, quelques précautions, ces risques potentiels peuvent être nettement réduits.
Détection et interdiction de moyens de communication Gsm ou traditionnels, vérification rapide des portes documents et sacs, l'utilisation de systèmes automatiques de détection de toute source d'émission RF signalant l'activation d'un Gsm, téléphone sans fils, micro... seraient un premier niveau.

Évoquons enfin pour anecdote le cas du piégeage de l'ambassade des États-Unis à Moscou par les Soviétiques.

Dans un aigle en bois (l'emblème américain) était disposé un microphone passif donc indétectable... Ce système, totalement passif camouflé dans la sculpture, était en fait composé d'un diaphragme métallique relié à une très courte antenne quart d'onde et ne nécessitait aucune source d'énergie d'alimentation : donc pouvant être utilisable indéfiniment...
L'activation d'un puissant champ radioélectrique extérieur à l'ambassade engendrait les vibrations créées par les sons perçus, de la même façon que vibre une peau de tambour, et transformait le système en véritable émetteur. Ce sont des modifications de l'organisme humain et plus particulièrement des cellules sanguines des personnels de l'ambassade dues aux bombardements intensifs d'hyperfréquences qui ont mis la puce à l'oreille et ont permis de démasquer cette technologie après une très longue utilisation.
Moralité de cette anecdote : méfiez-vous toujours des cadeaux d'entreprises décoratifs... ils peuvent, comme le cheval de Troie, renfermer des pièges mortels... Nous y reviendrons ultérieurement dans la partie conseils.

Décidément malchanceux, les américains ont découvert dans les murs de leur nouvelle ambassade, toujours à Moscou, un réseau de fibres optiques destiné à l'interception...



MOYENS DE DÉFENSE

DÉTECTEUR D'ÉMISSIONS GSM ET BROUILLEUR

Le premier niveau de sécurité pour une réunion sensible, s'il n'est pas envisageable de demander aux participants de laisser leur Gsm en dehors de la pièce ou si vous n'êtes pas certain que toutes les batteries n'aient été ôtées des téléphones : un détecteur d'activités Gsm. Ce détecteur discret, en veille sera déclenché soit par une liaison avec la BTS (échange d'informations permanent avec la borne de l'opérateur la plus proche), soit par un appel téléphonique qu'il soit émis ou reçu. Ce détecteur a été développé initialement pour détecter toute utilisation clandestine de Gsm dans les prisons et correspond tout à fait pour une sécurisation de rencontre confidentielle.

Certaines options permettent également la détection d'émissions de téléphones D.E.C.T., satellite (IRIDIUM : postes relativement compacts), d'émetteurs RF... et couvrent les bandes de 0 à 8 ou 10 GHz.

Le second niveau : le brouillage par saturation. La législation concernant les brouilleurs ou saturateurs Gsm est très complexe... En effet leur utilisation est interdite, mais est autorisée dans une propriété publique à partir du moment où vous ne débordez pas sur l'extérieur. Plusieurs puissances sont disponibles afin de s'adapter à la superficie à sécuriser : des modèles portatifs de la taille d'un téléphone Gsm, très discrets pour couvrir des distances de 1 à 2 mètres, pour sécuriser des distances équivalentes à la taille d'une petite salle de réunion, jusqu'à des modèles permettant un brouillage de quartier (uniquement pour les gouvernements).

Un assouplissement de la législation est en cours d'étude pour les salles de spectacles (théâtres). Paradoxalement, rien n'a été prévu pour le milieu industriel... Doit-on en conclure qu'il est plus important de supprimer des sonneries de téléphones portables durant une représentation que de protéger le patrimoine intellectuel français... véritable richesse de nos entreprises ?

GÉNÉRATEUR DE BRUIT BLANC

Afin de lutter efficacement contre les risques d'interceptions distantes liés à cet engouement pour les bureaux vitrés, il est indispensable de se prémunir contre ces menaces. Les générateurs BE de bruits blancs, bruits roses, et de micro vibrations permettent de contrer tout système d'écoute laser, canon à son, micro parabolique, stéthoscope électronique... : les micros vibrations et la génération des différents bruits les rendront inopérants dans leur mission de capture d'informations. Rappelons qu'un simple rideau suffit à contrer les observations vidéo ou à l'aide de jumelles ou télescope.

D'autres générateurs permettent une saturation des pastilles micro (electret) annihilant celles-ci et rendant donc impossible toute fuite d'informations RF, filaire, par courant porteur, par enregistrement numérique ou analogique ; mais ces technologies sont très réglementées. L'utilisation de brouilleurs RF est également possible. Ils couvrent de 0 à 4 GHz (voir plus) sans trou, mais interdisent toute réception : donc plus de transmission radio, plus de télévision... Ce mur virtuel infranchissable n'est utilisable que par des instances gouvernementales. Certains ont été inculpé, initialement pour lutter contre les risques terroristes attentatoires (embarqués à bord du véhicule pour parer les engins explosifs disposés sur un itinéraire de chef d'État). Les brouilleurs CP assurent la sécurisation des courants électriques afin d'en interdire l'utilisation. Dans certains cas, la mise en place de simples filtres secteur garantit une barrière suffisante. Quant aux brouilleurs EMI, ils protégeront contre les interceptions distantes et les captures de perturbations électromagnétiques générées par les matériels informatiques principalement.

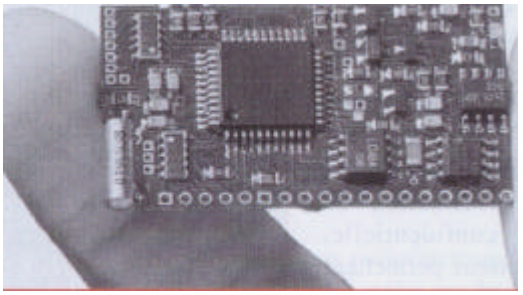
LA CAGE DE FARADAY : L'ULTIME REMPART

Cette technologie de blindage anti-compromission électromagnétique permet une protection contre l'espionnage électronique. Une isolation totale du monde électromagnétique extérieur et inversement ; en un mot : aucune onde ne peut plus ni entrer ni sortir... Soit sous forme de panneaux, soit sous forme de toile, cette technologie de blindage électromagnétique sera la seule parade contre cette pollution électromagnétique générée par les équipements électroniques, microprocesseurs.
Les aérations, clim, tuyauteries ou passage de câbles seront les points névralgiques nécessitant une attention toute particulière. Il va de soi, que moins il y aura d'ouvertures (portes, fenêtres) moins il y aura de risques. Une installation correctement effectuée garantira une étanchéité de 100% face aux interférences électromagnétiques.

Cette technologie de protection haut niveau est indispensable pour sécuriser efficacement contre toute fuite ou perturbation, des salles de réunions, de bureaux de direction, des services R & D (laboratoires de recherche et développement), des centres de communications, des salles de marchés, sites militaires...

CRYPTAGE : CHIFFREMENT DES COMMUNICATIONS TÉLÉPHONIQUES, RTC, RNIS (NUMÉRIQUES) SATELLITES...

Parallèlement au besoin de sécuriser l'information au sein de l'enceinte, il est également indispensable de protéger son stockage et ses transferts afin d'en assurer sa pérennité. A quoi bon faire poser la meilleure porte blindée pour sécuriser l'entrée principale si la porte de derrière reste ouverte... ?



Malgré une législation en France encore beaucoup trop restrictive concernant l'emploi de solutions de chiffrement sérieuses (chiffrement lourd), différentes possibilités matérielles ou logicielles permettent de garantir un premier niveau de sécurité. En effet, le risque est nettement moins important lorsque le PC portable d'un responsable est dérobé soit dans l'entreprise, soit s'il a été laissé par inadvertance dans la chambre d'hôtel ou dans le coffre de la voiture, si les fichiers sont cryptés.

Les solutions de chiffrement actuelles permettent aussi bien d'envoyer des dossiers sécurisés par e-mail, que de faxer des documents de façon sûre entre deux filiales ou d'utiliser un téléphone RTC, RNIS, portable ou satellite de manière totalement sécurisée.

D'autres solutions telles que l'utilisation de PC portables équipés des disques durs extractibles, d'un contrôle d'accès biométrique par analyse de l'empreinte digitale autorisant son démarrage ne sont plus des fictions mais bel et bien des technologies actuelles.

Enfin, à l'issue des opérations ponctuelles de contre-mesures électroniques, différents produits, simples d'utilisation permettent de garantir un haut niveau de sécurité. La pose de scellés de sécurité permet de contrôler l'intégrité de salles de réunion, d'armoires, d'objets sensibles pouvant être victimes d'un piégeage ou d'un simple échange standard. De même que l'utilisation d'enveloppes sécurisées permet de garantir un secret total sur des documents sensibles devant transiter.

MATÉRIELS DE DÉTECTION DE SYSTÈMES D'ÉCOUTE ET D'INTERCEPTION

1) LES DÉTECTEURS PORTATIFS DE MICRO RF

Les détecteurs à main, peu encombrants, autonomes, permettent une première détection de sources RF proches, mais sans démodulation. La présence d'émissions clandestines se traduit par l'illumination de led en fonction de la puissance du signal ou d'un affichage cristaux liquides de la fréquence détectée.

SIG-NET

Détecteur d'émissions numériques et analogiques, il couvre la gamme de 10 MHz à 3 GHz. Sa fonction alarme le déclenche automatiquement lors d'une transmission radio ou Gsm durant une réunion, dans un avion, un hôpital, une prison... Sa technologie avant-gardiste lui permet également de détecter les transmissions burst. Il combine une information visuelle et sonore.
Prix : environ 1 450 euros HT.

RF DETECT

Bien d'autres détecteurs manuels existent. Mais
une attention toute particulière doit être apportée au choix du détecteur. En effet, il ne faut pas confondre un fréquencemètre uniquement capable de vous indiquer la fréquence d'émission dans les cas d'un signal simple, mais par contre, totalement incapable de vous mettre en évidence un signal particulier type burst ou spectre étalé. Celui-ci couvre de 0 à 10 GHz, et détecter tout type d'émission. Ces petits matériels, compacts,
discrets sont idéaux pour vérifier des lieux de rendez-vous, en lieu public : restaurants...
Prix : environ 1 895 euros HT.

RF DETECT BOX

Détecteur d'émissions numériques et analogiques couvrant la gamme de 10 MHz à 10 GHz. Son automatisation totale lui permet d'inscrire la fréquence sur l'afficheur. Sa technologie récente autorise la détection de micros de dernières générations.

2) LES ANALYSEURS DE SPECTRE

Outil indispensable permettant de visualiser la représentation graphique du spectre autorisant ainsi une analyse des plus précises sur chaque pic de fréquence. Ils se présentent sous plusieurs formes : analyseurs complets, ou versions logicielles à utiliser via un PC portable derrière un récepteur large bande.

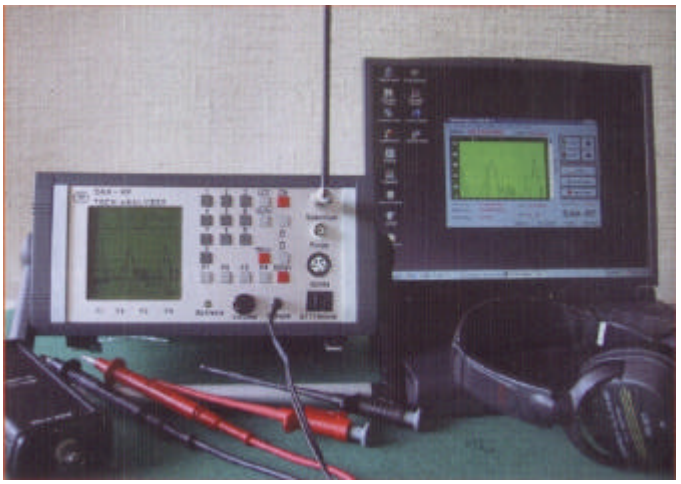
DÉTECTEURS D'HARMONIQUES SCANLOCK M2

L'analyseur de spectre M2 est un récepteur spécialement développé afin de détecter et localiser les micros émetteurs radios espions (RF) et Courant Porteur (CP) dans une gamme de fréquence de 0 à 5 GHz dans des lieux sensibles. Sa démodulation du signal reçu (donc soumis à l'art. 226 français) lui permet l'analyse et une levée de doute immédiate en cas de détection d'un signal : transmission inoffensive ou système clandestin d'interception. Il est équipé d'un nouveau logiciel d'analyse spectrale utilisable en 2 D (deux dimensions ou 3 D permet dans un temps très court une analyse totalement automatisée et la possibilité d'effectuer les enregistrements sur PC des relevés effectués et des comparaisons d'analyses entre deux prestations de contre mesures. Son point fort étant sa rapidité pour scanner sa large bande spectrale : moins de 15 secondes. Prix : de 8 200 à 16 500 euros HT selon les options

SAN-RF

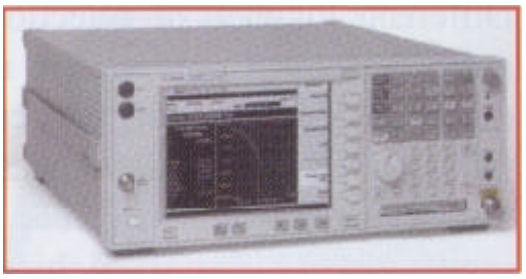
Le Système Analyse spectrale Numérique est un système de détection permettant de couvrir toute la gamme de mesures associées aux opérations TSCM. Son démodulateur intégré à bande large (donc soumis à l'art. 226 français) couvre de 100 KHz à 2,1 GHz en mode Oscillateur RF et de 5 KHz à 5,1 GHz en mode Oscillateur local (Oscillateur Fondamental) et en option jusqu'à 21 GHz.

Utilisable soit en autonome, soit piloté par un PC portable, son option modem interne lui permet une délocalisation des commandes autorisant ainsi la surveillance spectrale d'une réunion sensible à distance. Sa fonction FINDER scanne l'intégralité du spectre et se cale automatiquement sur la fréquence détectée la démodulant instantanément (signaux analogiques). Sa sonde EMI permet des relevés précis des distances de rayonnements dues aux perturbations informatiques ; il peut également être proposé avec des sondes détections US ET IR. Prix : environ 33 000 euros HT selon les options.



SÉRIE PSA E 440 À 443

Cette série d'analyseurs de spectre à dynamique élevée couvrent les bandes de 3 Hz à 26,5, 40 et 50 GHz.



SAN RX

Tout dernier-né des analyseurs de spectre, ce système d'analyse de signaux RF numériques et analogiques est un récepteur numérique ultra sensible à large bande couvrant le spectre de 150 KHz à 4 GHz (bientôt 10 GHz puis 21 GHZ) sans trous. Le contrôle et le pilotage du récepteur se font par PC portable. Il est également possible de télécommander le système à distance via un réseau LAN/WAN ou un modem. Une sortie IF (fréquence intermédiaire) à 10,7 ou 21,4 MHz permet la connexion d'un système de traitement des signaux en externe. Sa possibilité de démoduler la totalité des signaux analogiques audio et vidéo (donc soumis à l'art. 226 français) ainsi que la majorité des signaux numériques (décodeurs optionnels), le fait qu'il soit l'un des plus rapides du marché, mais surtout qu'il puisse être laissé sur place comme «boîte noire» assurant ainsi une veille et un enregistrement h24 de la globalité du spectre rapatrié à distance en font l'un des matériels les plus complets pour une équipe de contre-mesures. Il est livré avec une série d'antennes : omnidirectionnelle, actives larges bandes ou directives.

Prix : de 23 000 à 45 000 euros HT selon les options.

Une autre technique pour la mise en évidence de pièges (surtout numériques) à l'aide d'analyseurs de spectre est la détection d'une harmonique. Cette porteuse parasite générée par un VCO, PLL, diviseur ou multiplicateur de fréquence a une fréquence toujours supérieure au signal de base : sa fréquence fondamentale. Par conséquent, vous pourrez tout à fait détecter la première, seconde, troisième, quatrième ou cinquième harmonique.

Exemple Fréquence fondamentale	/Harmonique initial	/Second harmonique
330 MHz	660 MHz	990 MHz
435 MHz	870 MHz	1305 MHz

2) LES VALISES DE DÉTECTIONS AUTOMATISÉES

OSCOR

Sans aucun doute le système le plus connu et le plus utilisé à travers le monde, il permet une vérification RF 10 KHz à 3 GHz (21 GHz en option), les courants porteurs, les sources infrarouges, la démodulation de signaux vidéo, la localisation de la source émettrice. Fourni en valise, le système est également équipé d'un analyseur spectral large bande, d'un démodulateur (donc soumis à l'art. 226 français), de sa propre imprimante interne, d'une série d'antennes, d'une interface de liaison vers un PC permettant grâce a son modem un paramétrage à distance.
Prix : de 16 000 à 28 900 euros HT selon les options.

DETECT CASE

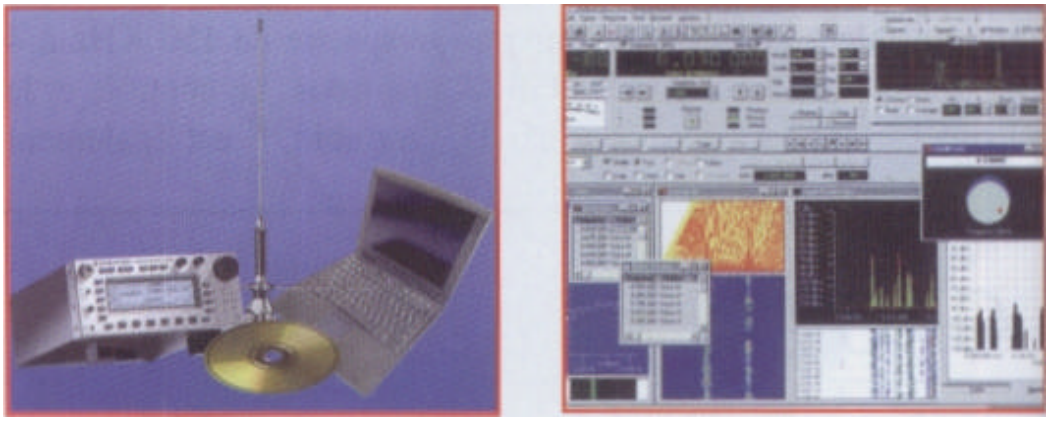
Système global de détection, discret, compact, cette valise permet la vérification spectrale totalement automatisée de 150 Khz à 10 GHz (21 en option), des courants porteurs, les sources IR et US, et comprend également un détecteur ELF pour la mise en évidence de pièges passifs. Elle peut être proposée en deux versions : sans démodulation, ou avec (donc soumis à l'art. 226 français). Prix : de 13 500 à 25000 euros HT selon les options.

3) RÉCEPTEURS LARGES BANDES (SCANNERS)

Les récepteurs larges bandes sont des outils très pratiques et totalement complémentaires aux analyseurs de spectre. Leur technologie leur permet un paramétrage préalable, une levée de doute immédiate sur les signaux analogiques détectés, une vérification du spectre de 150 KHz à 2060 GHz, la vérification des courants porteurs lorsqu'ils sont équipés de la sonde adaptée. Ils peuvent également être connectés à différents logiciels d'analyse spectrale.
Prix : de 1200 à 2 000 euros HT selon les modèles haut de gamme.

4) LES LOGICIELS D'ANALYSE SPECTRALE

Différents logiciels de détection et de reconnaissances de signaux radio existent. Couplés à un récepteur larges bandes, ils sont à même de déceler des signaux compromettants types burst, sauts de fréquences ou autres. Des fonctions de paramétrage initial, d'enregistrement, de comparaison de relevés, la création de relevés références, la création de fichiers log sont autant de possibilités offertes permettant une mise en évidence immédiate de systèmes d'interception.
Leurs prix oscillent entre 7 500 et 16 800 euros HT.



5) LES DÉTECTEURS DE JONCTIONS NON LINÉAIRES DJNL

Les détecteurs de jonctions non linéaires utilisent le principe du radar d'harmoniques pour détecter à distance tout appareil électronique caché, tout type de circuit électronique, même inerte. Leurs techniques d'analyse simultanée du second et du troisième harmonique retournées par la cible leur permettent par comparaison des signaux une discrimination précise entre des cibles électroniques (jonctions électroniques) et des cibles non-électroniques (jonctions métalliques). Ces détecteurs sont des éléments indispensables pour une équipe spécialisée afin de détecter et localiser lors d'opérations de contre-mesures des appareils électroniques clandestins cachés.
Leurs prix oscillent entre 16 800 et 20 650 euros HT.

Les deux détecteurs les plus connus et les plus utilisés au monde sont les suivants :

LA SÉRIE DES SUPER BROOM (ECM, ADVANCED) (photo ci dessous)

L'ORLON

6) LES DÉTECTEURS DE SYSTEMES PASSIFS ELF DETECT

Le détecteur de sources E.L.F. spécialement conçu pour la détection d'activité E.L.F. (émission très basses fréquences générées par tout circuit électronique en fonctionnement ou par tout circuit électronique ayant été alimenté par une alimentation continue (polarisée) ou alternative (non polarisée) dans un environnement proche est idéal pour la vérification TSCM ponctuelle de bureaux (opérations de contre-mesures électroniques), de salles de réunion...
Ce dispositif a été développé pour la détection de toute activité E.L.F. générée par des matériels hors fonctionnement tels que : magnétophone numérique ou analogique, stéthoscope électronique, ligne de surveillance filaire, caméra CCD, système électronique de déclenchement d'E.E.I. / LE.D. (Engins Explosifs Improvisés), haut-parleur de surveillance, certaines piles ou batteries, etc... dissimulés dans les faux plafonds, cloisons, murs, vitres, mobiliers et objets divers.

Son fonctionnement totalement passif lui permet également d'effectuer un contrôle du courrier, colis suspects, paquets, objets divers pouvant contenir des E.E.I., mais surtout de la vérification de lieux et de personnes : présence de Gsm (même éteint et démonté), présence de disquettes informatiques (contrôle d'accès de laboratoires de Recherches & Développement)...
Prix : environ 4 500 euros HT.

7) LES DÉTECTEURS DE DÉFAUTS DE RÉSEAUX ET LIGNES TÉLÉPHONIQUES (TDR : TIME DOMAIN REFLECTOMETERS)

Les TDR (aussi appelés détecteurs de défaut de lignes) sont également un lourd investissement pour une équipe TSCM. Leur utilisation nécessite une réelle expérience et une sérieuse formation aux techniques télécom. A l'heure actuelle, hormis certaines unités de contre-mesures électroniques privées, les seuls utilisateurs de ces matériels de tests sont les techniciens de France Télécom ou autres opérateurs téléphonie afin de déceler des défauts de ligne. Ces instruments de mesure sont capables de détecter des pièges filaires, des dérivations de lignes à des distances pouvant atteindre 15 à 30 km selon les modèles. Ces instruments de test révèlent la moindre irrégularité d'impédance, le moindre défaut ou irrégularité de câblage, la plus petite dérivation et sont même capables d'indiquer à quelle distance un câble téléphonique a été dénudé ; permettant ainsi de mettre en évidences des piégeages démontés utilisés dans le passé.

Ils intègrent les fonctions suivantes : multimètre numérique pour mesures de : tensions DC & AC, potentiel étranger, résistance de lignes et de résistance d'isolement, contrôle qualitatif des paires : courant de boucle, mesures de bruit, désadaptation, pertes d'insertion, et diaphonie, localisateurs de défauts : pont numérique (RFL) offrant différents modes de tests: 3-fils, 4-fils, et Kupfmuller (idem Fabe), mesure capacitive pour la localisation des circuits ouverts, et échomètre (TDR) pour la recherche des défauts sur les lignes avec ou sans pupins.
Tous les résultats des mesures sous forme de signatures sinusoïdales peuvent ensuite être enregistrés pour servir à double titre : étayer le rapport d'audit, mais également les superposer lors de prestations futures dans le cas d'un contrat annuel de contre mesures. Sans TDR, il est quasiment impossible de localiser avec exactitude tout défaut de ligne, tout piège inductif, ou autre forme de modification clandestine de ligne téléphonique permettant ainsi d'effectuer de façon précise et rapide une inspection physique visuelle localisée comme levée de doute.

Les toutes dernières générations proposent même un boîtier d'activation distant qui ouvre et ferme les lignes, crée des défauts... Elles permettent également le test de lignes numériques de type ADSL.

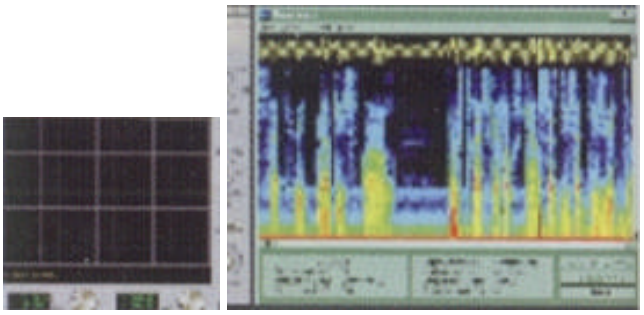
Une option révolutionnaire en cours de tests permettra la mise en évidence d'éventuelles présences de systèmes d'interceptions par induction (présence de sonde à effet d'Hall) captant les perturbations et rayonnements émis par le câble actuellement indécelable par un TDR traditionnel. Cet élément optionnel sera utilisable sur tous les TDR existants.
Leurs prix oscillent entre 3 000 et 7 500 euros HT.

8) LES SYSTEMES D'ANALYSES DE LIGNES TÉLÉPHONIQUES TESTEUR DE CABLES ET DE LIGNES FILAIRES TSCM 500 (AMPLI BF)

Les interceptions, les écoutes téléphoniques, les bretelles, les dérivations... sont devenues monnaie courante dans un monde où l'espionnage industriel est passé risque numéro 1 pour les gouvernements, les ambassades, les entreprises importantes, ou évoluant dans des milieux sensibles...
Les amplificateurs TSCM sont spécialement conçus pour effectuer des vérifications filaires audio (téléphone, câblage réseaux, câblage de sonorisations, etc...) afin de détecter la présence de source BF (Basse fréquence), de systèmes d'écoute, de Bypass. Ces testeurs très simples d'utilisation permettent la détection de micro à courant porteur filaire téléphonique, les tests de câblage téléphonique (numérique et/ou analogique), la détection de pastille micro filaire dynamique ou électret, le report de câblage à partir d'un haut-parleur de sonorisation, l'activation de systèmes d'écoute télécommandés par un générateur de son intégré, la détection de magnétophone avec un report de pastille électret, la vérification de bon fonctionnement, sans report, de tout système filaire BF... La possession d'une alimentation (automatique) interne permet l'activation distante de microphone de type électret ou dynamique.

Ces testeurs de câbles peuvent être également fournis avec différentes options : logiciel de traitement du signal (BU) oscilloscope, logiciel de traitement du signal analyseur de spectre, equalizer 10 bandes électronique, sonde de mesure sans contact à effet Hall faible rayonnement, accéléromètre pour mesure vibratoire dans le spectre BF. Leurs prix oscillent entre 3 500 et 11 000 euros HT.

Pour ces raisons, il est grandement conseillé à une équipe de contre-mesures électroniques de détenir et d'utiliser ces deux moyens successifs de contrôle afin de s'assurer de la totale intégrité non seulement des téléphones, mais également des lignes et câblages téléphoniques.



9) LES DÉTECTEURS CP (COURANT PORTEUR)

Certaines équipes n'ont pas forcément les budgets ni la nécessité de posséder un analyseur de spectre pour la vérification CP (courant porteur). Pour cette raison, des détecteurs automatisés, plus simples d'utilisation, permettent un contrôle rapide et efficace par affichage direct de la fréquence d'un système d'écoute sur courent porteur).

10) LES DÉTECTEURS LR. ET U.S.

L'évolution des technologies offensives a nécessité une équivalente évolution des matériels de détection. Ces derniers temps, nous avons pu observer une recrudescence de micros I.R. et U.S.

Le système ***US DETECT 500*** a été spécialement développé pour détecter une activité ultrasonique (émission U.S.) dans un environnement proche par détection et démodulation de proximité (donc soumis à l'art. 226 français). Il est idéal pour la vérification lors d'une opération de contre-mesures électroniques. Le balayage de la plage de fréquences ultrasoniques avec le potentiomètre du détecteur dans une pièce (sans avoir omis d'allumer tous les appareils fonctionnant sur secteur/sur pile) permettra la révélation et la démodulation des signaux ultrasoniques mais également la vérification des postes téléphoniques au(x) décroché(s). Prix : environ 2 000 euros HT.

Le système **IR *DETECT 500*** a également été spécialement développé pour détecter une activité infrarouge et/ou laser (émission dans le spectre lumineux visible ou invisible) dans un environnement proche par détection et démodulation de signaux lumineux de proximité (donc soumis à l'art. 226 français). Ce dispositif est conçu pour la détection de toute émission provenant de l'intérieur d'une pièce ou de l'extérieur d'un bâtiment de type écoute laser sur vitre. Prix : environ 5 200 euros HT.

Le point le plus important n'est pas d'avoir les meilleurs matériels existants, les toutes dernières technologies de détection si leurs utilisateurs ne maîtrisent pas 100 % de leurs capacités. Ce n'est pas parce que vous possédez un piano que vous savez vous en servir...

VULNÉRABILITÉS COURANTES DES ENTREPRISES

Une attention toute particulière est à porter sur l'utilisation des moyens de transmissions autres que les lignes téléphoniques traditionnelles et les téléphones Gsm. En effet, l'utilisation des émetteurs récepteurs portatifs traditionnels (postes radio) par les services d'entretien, mais surtout les services sécurité sont très facilement interceptables par un simple récepteur large bande ou scanner... L'utilisation de postes chiffrés est donc grandement conseillée. L'évolution de moyens mondiaux de communication comme le web (net) permet de commander et de se procurer très facilement des scanners, des récepteurs larges bandes dans des pays proches de la France (où la réglementation est moins restrictive) et de les recevoir discrètement par la poste. Ces écoutes sont totalement invisibles et indétectables. Cette vulnérabilité inquantifiable quant aux dégâts qu'elle peut générer est malheureusement méconnue ou trop peu prise en compte... Imaginez la valeur des informations qui transitent par le plus sensible service de l'entreprise : votre service sécurité... !

Une seconde attention toute particulière devra également être portée quant à l'utilisation des téléphones numériques sans fils pour entreprise : les téléphones D.E.C.T.
En effet, les technologies évoluent sans cesse, et l'on se trouve confronté à une arrivée sur le marché de systèmes d'interception multicanaux permettant l'écoute de ces téléphones numériques sans fils. Leur détention et utilisation sont bien entendu strictement réglementées, mais rappelons que seuls les honnêtes gens effectuent les démarches officielles en vue d'une acquisition légale de ces matériels particuliers, qu'en est-il de ceux qui les utiliseront à des fins purement offensives... ! Il est vrai que c'est un réel confort de pouvoir être joignable en n'importe quel lieu de l'entreprise, mais à quel prix ?

Pour ces raisons, si l'utilisation de téléphones D.E.C.T. est réellement indispensable au bon fonctionnement de l'entreprise, il faudra se tourner vers des modèles chiffrés afin de garantir une confidentialité totale pour l'entreprise, l'ambassade, le laboratoire de recherche, ou simplement le service communication...

Une autre vulnérabilité réside dans la société choisie pour assurer la communication et la promotion de l'entreprise. En effet, celle-ci sera au coeur d: vos petits secrets... alors uj conseil : choisissez-la bien ce une société sans scrupule peu se mettre à la disposition d l'un de vos concurrents et lu livrer des informations confidentielles...

Une source de fuite majeur réside également dans le traitement sécuritaire des stagiaires En effet, peu de contrôle d'ancienneté ou de moralités sont effectués, et pourtant: durant leur stage, ils ont accès à des lieux ou des informations stratégiques... possèdes des moyens d'accès physique ou informatiques qui ne sa pas toujours modifiés après leur départ... Une vérification de l'ancienneté est également conseillée pour les nouveaux salariés même si l'activité de l'entreprise n'est pas ultra sensible... elle évitera bien des déboires. Il est également conseillé d'intégrer au contrat d'embauche des clauses de confidentialité afin de se prémunir contre toute fuite volontaire ou involontaire de la part du nouveau salarié : la sensibilisation commence dès l'embauche...
On entend par fuite involontaire, un bavardage anodin de secrétaire, de collaborateur comme au bar le soir où l'on se retrouve entre amis, la pression retombe et l'on évoque avec colère les problèmes internes avec un chef de service, la réussite de la signature d'un nouveau contrat avec la société X, les menaces de licenciements causées par la fusion avec le Groupe Y alors que l'information est encore relativement confidentielle... ou même des brouillons, prises de notes ou mémo oubliés par inadvertance sur le bureau parce que l'on est pressé de prendre son train...
L'un des problèmes les plus importants et les plus risqués pour les grandes entreprises est la progression de l'externalisation du service de sécurité par la sous-traitance de sociétés extérieures. En effet, si celles-ci ne sont pas suffisamment sensibilisées ni formées à ces nouvelles menaces, le niveau de sécurité s'en trouvera gravement affecté...

De même, les services de gardiennage et de nettoyage peuvent se révéler être de potentielles sources de risque. Attention, ne déformons pas les propos énoncés... nous n'incriminons aucunement les entreprises sous-traitantes, mais n'évoquons que des faits basés sur des faits passés réels.

Le souci actuel réside dans le fait que de nombreuses formations ou sensibilisations quant aux vulnérabilités informatiques, aux risques d'intrusions dans les réseaux informatiques existent ; mais are niveau des vols d'informations liés aux écoutes clandestines, aux risques d'interceptions, de surveillance électronique : il n'existe quasiment rien...

Un risque, dont la majorité des professionnels sous-estime totalement les conséquences, est la maintenance du matériel informatique : lors d'une panne d'ordinateur (de bureau, portable, serveur, agenda électronique...), rien de plus normal que d'envoyer en réparation le matériel défectueux... mais avez-vous songé aux informations qu'il contient ? Informations commerciales, projets de développement, contacts militaires...

Enfin, nous assistons trop fréquemment lors de réunions $_t$ dans des grandes salles de conférences mises à disposition de grandes sociétés, de grands groupes pour des réunions avec les actionnaires, de séminaires de motivation, ou de mise en place d'une nouvelle

politique de communication, action commerciale à l'échelon national ou international à l'utilisation de micros de scène sans fil.
A quoi sert alors votre service de sécurité chargé du filtrage afin qu'aucun élément étranger à la réunion ne puisse pénétrer si vous permettez, par l'utilisation d'un micro de scène HF, de monitorer à distance l'intégralité des propos tenus, des questions posées... Soyez vigilants... vérifiez que si micro sans fil il y a, la technologie ne facilite pas la fuite d'informations capitales..

L'objectif de cette dernière rubrique n'est pas de vous rendre paranoïaque mais de générer une réflexion afin de minimiser les risques et ainsi d'accroître le niveau de sécurité.

LES DIFFÉRENTS ACCESSOIRES INDISPENSABLES AUX OPÉRATIONS DE CONTRE-MESURES ÉLECTRONIQUES

Divers accessoires sont totalement indispensables pour une bonne investigation technique. La partie recherche et fouille physique, malgré une utilisation majoritaire de matériels de contrôles électroniques est aussi importante voire plus. Par conséquent, différents petits matériels complémentaires permettent d'améliorer et simplifier différentes tâches.

- L'utilisation de jeux de miroirs fixés sur une perche télescopique équipée d'une lampe puissante permet une vérification des endroits inaccessibles, des faux plafonds... Rappelons que les faux plafonds sont les endroits les plus rapidement accessibles pour placer discrètement des pièges : magnétophones discrets, Gsm à activation distante...

- Une lampe rechargeable puissante est également très utile pour vérifier l'arrière des radiateurs, le dessous des meubles...

- L'utilisation de scellés de sécurité a plusieurs utilités : une fois la vérification physique (démontage et ouverture des téléphones) et électronique effectuée, l'apposition de scellés de sécurité transparents à marquages UV (ultraviolet) et séquentiel permet de garantir que le téléphone n'a pas subi de modification, d'échange standard, de piégeage..., la fermeture de différentes pièces sensibles (local BABX) ou armoires afin d'en vérifier l'intégrité. De plus, une vérification des numéros de série des scellés permet, à l'aide du rapport d'audit, une vérification par comparaison du responsable de la sécurité entre deux opérations de contre-mesures électroniques. Le marquage UV n'étant visible que sous présence d'une lumière UV, le scellé passe en majorité du temps pour un vulgaire bout de ruban adhésif...

- Un appareil photo numérique est également indispensable pour mémoriser différents points névralgiques, différentes vulnérabilités ou dans le but de vérifications ultérieures et enfin pour l'élaboration du rapport d'intervention. Certaines équipes, lors d'opérations de contre-mesures électroniques en profitent pour établir un diagnostic sur les vulnérabilités principales, les lacunes sécuritaires et les améliorations possibles conseillées.

Pour des équipes bénéficiant de davantage de budgets, des solutions d'inspection vidéo permettent de faciliter les fouilles et inspections des systèmes vidéo montés sur perches télescopiques équipées de micro caméras éclairées et d'écran de contrôle, facilitent également les vérifications de châssis de véhicules, des caméras également fixées à l'extrémité de perches télescopiques vidéo traditionnelle ou thermiques (changement de caméra et donc de technologie en quelques secondes) équipées de leur écran de contrôle, divers endoscopes afin d'éviter le démontages des garnitures lors de vérification de véhicules. Des caméras thermiques ou des systèmes d'inspection rayon sont également utilisés par des équipes gouvernementales

cHaOs RaDiO cLuB France

Manuel TSCM by RaDiOz

CRCF Member

http://perso.ksurf.net/CRCF/

http://fr.groups.yahoo.com/group/CRCF/