Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI
Office fédéral de la santé publique OFSP
Unité de direction Protection des consommateurs

Janvier 2007

Réseaux sans fil. Risques potentiels

Rapport répondant au postulat 04.3594 Allemann du 8 octobre 2004

Groupe de travail :
Office fédéral de la santé publique (OFSP)
Stefanie Gruber, Martin Meier, Mirjana Moser, Salome Ryf

Office fédéral de la communication (OFCOM)
Rolf Burgherr, Mark Fitzpatrick, Markus Riederer

Office fédéral de l'environnement (OFEV)
Andreas Siegenthaler

Swissmedic, Institut suisse des produits thérapeutiques
Daniel Reusser

Direction :
Office fédéral de la santé publique, division Radioprotection
Mirjana Moser

Informations complémentaires :
La présente publication est également disponible en allemand et en italien.
Le rapport est publié sous www.bag.admin.ch/wlan-bericht.

Condensé

Le présent rapport a été élaboré en exécution du postulat 04.3594 déposé par Evi Allemann et intitulé « Réseaux sans fil. Risques potentiels ». Il répond aux questions soulevées par ledit postulat et donne des informations en matière de rayonnement, de risques pour la santé, de sécurité des données et de nécessité de réglementation. Il analyse les technologies les plus répandues, comme Bluetooth, WLAN ou le nouveau WiMAX. Il présente les technologies actuelles, esquisse des scénarios d'avenir et donne des recommandations pour une utilisation correcte de ces nouvelles technologies.

La charge de rayonnement due aux réseaux actuels est relativement faible; elle se situe bien en dessous des valeurs limites en vigueur. Il est toutefois indiqué d'être prévoyant en la matière, du fait de l'évolution fulgurante des technologies vers des appareils de plus en plus performants, d'une utilisation proche du corps plus fréquente ainsi que de l'utilisation simultanée de plusieurs appareils dans un espace restreint. En outre, des incertitudes relatives aux conséquences sur la santé subsistent, notamment en ce qui concerne les effets à long terme.

La compatibilité électromagnétique constitue une problématique particulière aux réseaux sans fil. La plupart de ceux-ci émettent, comme beaucoup d'autres dispositifs, dans la bande de fréquence sans licence et il peut en résulter des brouillages réciproques. Une prudence particulière est recommandée dans le domaine médical où des dysfonctionnements d'implants électroniques pourraient poser des problèmes sanitaires.

Les réseaux sans fil recèlent également certains risques en matière de sécurité des données et de l'information. Ces risques sont supérieurs à ceux liés aux réseaux câblés, et, en outre, il est plus difficile pour le non spécialiste d'appliquer les mesures de sécurité de base. C'est pourquoi il importe d'informer la population de manière appropriée à ce sujet.

A ce jour, aucune nécessité de réglementation ne s'impose, ni en ce qui concerne le nombre croissant de stations publiques (hotspots), ni en ce qui concerne le rayonnement ou les conséquences sur la santé. L'évolution et la diffusion ultérieures de ces technologies ainsi que la recherche constante en matière de risques sanitaires devraient toutefois être suivies avec attention par les autorités compétentes.

Tant en ce qui concerne le rayonnement qu'en matière de sécurité des données liée aux réseaux sans fil, il existe un besoin de sensibilisation. Le rapport propose des recommandations en vue de réduire la charge due au rayonnement et d'améliorer encore la sécurité des données. Le rapport et les recommandations, ainsi que les fiches d'information qui se basent sur ces dernières sont publiés sur le site Internet de l'OFSP. Il s'agit en particulier d'informer les organisations de consommateurs et le corps médical.

1. Introduction

La communication sans fil constitue incontestablement le segment de marché le plus prometteur dans le domaine de l'information. En matière de réseaux sans fil on attend un boom analogue à celui qu'a connu la communication par téléphonie mobile, ce que laisse présager le nombre croissant d'utilisateurs tirant profit des avantages des accès mobiles et nettement améliorés au monde numérique : les réseaux sans fil permettent en effet de se passer de câbles pour relier les ordinateurs et les périphériques entre eux, et les ordinateurs à Internet, les liaisons correspondantes étant établies par radio.

Cette évolution soulève toutefois des questions en matière de sécurité des nouvelles technologies. Dans le domaine technique, il s'agit de la transmission sécurisée de données non falsifiées ainsi que de l'immunité d'autres appareils électriques aux perturbations rayonnées. Par ailleurs subsistent des questions concernant les effets potentiels exercés sur la santé par le rayonnement électromagnétique des réseaux sans fil aux caractéristiques partiellement nouvelles.

Suivant la proposition du Conseil fédéral du 12 janvier 2005, le Conseil national a adopté le postulat Allemann (04.3594 ; « Réseaux sans fil. Risques potentiels ») le 18 mars 2005.
Par le postulat, le Conseil fédéral est chargé d'élaborer *un rapport sur les risques potentiels des réseaux sans fil (réseaux locaux sans fil appelés « WLAN », Bluetooth, etc.). Le rapport portera aussi bien sur les réseaux sans fil et points d'accès des bureaux et des ménages que sur les stations Internet publiques (appelées « hotspots »). Il devra notamment mettre en évidence :*

- *le rayonnement des réseaux sans fil ;*
- *les conséquences pour la santé publique (notamment les risques encourus par les jeunes enfants) et les mesures envisageables ;*
- *les effets sur l'environnement ;*
- *la question de la sécurité des données ;*
- *la nécessité d'une réglementation relative à la multiplication des points d'accès privés et publics (cf. www.swisshotspots.ch).*

Les résultats seront portés à la connaissance des groupes cibles de manière appropriée.

Le présent rapport renseigne sur les questions soulevées par le postulat Allemann[1]. Il traite les technologies actuellement les plus répandues, comme Bluetooth, WLAN ou le nouveau WiMAX. Le rapport envisage en outre des scénarios en ce qui concerne les évolutions possibles et émet des recommandations pour une utilisation correcte de ces technologies.

Le rapport est publié sur la page Internet de l'OFSP, où figurent également des fiches d'information portant sur des thèmes spécifiques. Un article du Bulletin de l'OFSP informe le corps médical à ce sujet, les consommateurs quant à eux le sont dans le cadre de la collaboration avec le Bureau fédéral de la consommation.

[1] En complément au présent rapport, on recommande la lecture du rapport « Rayonnements non ionisants et protection de la santé en Suisse » élaboré en réponse au postulat Sommaruga « Rayons non ionisants. Valeurs limites » (00.3565). Il traite en détail les expositions, les effets sur la santé et la situation juridique en matière de rayonnement non ionisant. www.bag.admin.ch/nis-bericht

2. Réseaux sans fil : mode de fonctionnement et charge due au rayonnement

Définition

Dans un réseau sans fil, les appareils sont reliés par radio et non par câble, soit par un rayonnement électromagnétique à haute fréquence. Bien que la téléphonie mobile fonctionne également de cette manière, les réseaux sans fil englobent plutôt les liaisons radio à courte distance comme celles utilisées dans les réseaux formés d'ordinateurs et de leurs périphériques ou d'ordinateurs liés à Internet.

Mode de fonctionnement

Dans un réseau sans fil, les données et les informations sont transmises au moyen d'ondes électromagnétiques[2] (*champs électromagnétiques*, CEM). Pour ce faire, tous les appareils du réseau sont équipés d'une antenne d'émission/réception. Les données ou les informations à transmettre d'un émetteur à un récepteur sont tout d'abord transformées en un signal superposé à une onde porteuse, qui est ensuite émise. La superposition des données à l'onde porteuse entraîne une modification de celle-ci – on dit qu'elle est modulée. Il existe divers types de modulation et, par conséquent, divers types de rayonnement pour un signal radio. Un autre appareil est en mesure de capter le signal, de le comprendre et de le transformer en données ou informations d'origine. Les ondes porteuses sont des CEM à haute fréquence.

La diffusion des CEM autour d'un émetteur dépend de l'antenne utilisée. Une antenne peut rayonner de manière uniforme dans toutes les directions (comme une ampoule électrique) ou uniquement dans une direction précise (comme un projecteur). Le gain d'antenne de cette dernière est plus important que celui d'une antenne isotrope rayonnant de manière uniforme. L'énergie émise par l'antenne pendant un certain temps correspond à la puissance d'émission (en watts, W). Généralement, c'est la puissance d'émission PIRE qui est utilisée[3], afin de décrire la puissance avec laquelle une antenne isotrope devrait émettre pour produire partout un rayonnement de même intensité, comme l'autre type d'antenne mentionné dans la direction de son rayonnement principal. ERP[4] décrit la puissance d'émission pour une antenne dipôle fictive.

Normes

Afin que les différents appareils d'un réseau sans fil puissent communiquer entre eux, diverses normes de télécommunication définissent les conditions de la transmission de données (fréquence de l'onde porteuse, modulation, intensité du signal, etc.).

Les normes les plus importantes concernant les réseaux sans fil sont les normes de télécommunication émises par l'institut américain *Institute of Electrical and Electronics Engineers* (*IEEE*).

Dans les chapitres suivants sont évoquées les trois familles de normes typiques pour les réseaux sans fil. Selon l'étendue du réseau on distingue :

- les réseaux de type WPAN (Wireless Personal Area Networks), de faible portée, pour des utilisations au poste de travail par exemple (normes IEEE 802.15, nom commercial Bluetooth) ;
- les réseaux de type WLAN (Wireless Local Area Networks), de portée un peu plus importante, pour des utilisations à l'intérieur des maisons par exemple (normes IEEE 802.11, également connu sous le terme WiFi) ;

[2] On utilise les notions d'ondes, de micro-ondes, de rayonnement électromagnétique, de rayonnement à haute fréquence. D'un point de vue physique, toutes ces notions sont des champs électromagnétiques (CEM) d'une certaine fréquence – cf. abréviations et définitions dans l'annexe, p. 31.

[3] Puissance isotrope rayonnée équivalente

[4] Puissance équivalente émise par un émetteur

- les réseaux de type WMAN (Wireless Metropolitan Area Networks) pour des réseaux régionaux comme ceux d'une ville (norme 802.16, nom commercial WiMAX[5]).

Le Tableau 1 présente un aperçu de ces normes avec certaines de leurs caractéristiques et la situation en Suisse.

Tableau 1 *Normes relatives aux réseaux sans fil*

	Norme IEEE[6]	**Puissance d'émission maximale (PIRE)**	**Fréquence (MHz)**	**Régime de la concession**	**Portée (m)**	**Régulation de la puissance**	**Débit de données max. brut (MBit/s)**
WPAN (Bluetooth)	802.15 Classe de puissance 1	100 mW	2400 – 2483,5	non	100	oui, dynamique	0,4 - 3
	802.15 Classe de puissance 2	2,5 mW	2400 – 2483,5	non	20	optionnelle	0,4 - 3
	802.15 Classe de puissance 3	1 mW	2400 – 2483,5	non	10	optionnelle	0,4 - 3
WLAN (WiFi)	802.11a	200 mW	5150 – 5250	non	50	non	54
	802.11b	100 mW	2400 – 2483,5	non	jusqu'à 200	non	11
	802.11g	100 mW	2400 – 2483,5	non	50	oui, statique	54
	802.11h	200 mW 1 W	5150 – 5350 5470 - 5725	non	50	oui, dynamique	54
WMAN (WiMAX)	802.16 Stations de base participantes	200 W/MHz 16/100 W/MHz 4W	3410 – 3600 5725 - 5875	oui oui à l'étude	30 000	oui	1 - 54

D'autres normes, comme HiperLAN, émises par l'Institut européen des normes de télécommunication (*European Telecommunications Normes Institute*, *ETSI*), ne sont pas répandues sur le marché, c'est pourquoi elles ne sont pas prises en compte dans le présent rapport.

Détermination de la charge de rayonnement

La dose est une mesure de la charge due au rayonnement, qui est en relation directe avec les effets exercés sur la santé. La dose significative pour les CEM à haute fréquence est l'énergie de rayonnement absorbée par le corps par unité de temps et par unité de poids. Celle-ci constitue le taux d'absorption spécifique (TAS, exprimé en Watt par kilogramme, W/kg), qui est toujours exprimé sur 10 g de tissus et une durée de 6 minutes. La valeur du TAS constitue la valeur limite de base des recommandations sur les valeurs limites de la CIPRNI (Commission internationale de la protection contre le rayonnement non ionisant, en anglais ICNIRP; recommandation sur les valeurs limites, cf. paragraphe 3.2).

[5] La norme européenne correspondante est la norme Hiperman de l'Institut européen des normes de télécommunications (ETSI)

[6] IEEE 802.11 (WLAN) http://standards.ieee.org/getieee802/802.11.html
IEEE 802.15 (Bluetooth) http://standards.ieee.org/getieee802/802.15.html
IEEE 802.16 (WiMAX) http://standards.ieee.org/getieee802/802.16.html

La valeur TAS étant difficile à déterminer directement, on préfère procéder à une détermination indirecte via une grandeur relative aux immissions comme le champ électrique (exprimé en Volt par mètre, V/m) ou la densité de puissance (exprimée en Watt par mètre carré, W/m^2). Ces grandeurs constituent les valeurs limites de référence des recommandations sur les valeurs limites de la CIPRNI. Elles ne s'utilisent que si la source de rayonnement est éloignée du corps et que si le corps tout entier est exposé de manière uniforme. Pour les utilisations proches du corps, la valeur TAS doit être déterminée directement.

Par exposition, on entend le rayonnement auquel une personne est soumise durant un certain temps.

Les immissions et les valeurs TAS dépendent de très nombreux facteurs comme la puissance d'émission, la distance par rapport à l'émetteur, la fréquence, la modulation, etc. Certains d'entre eux sont précisés dans le tableau 1 et dans la description des technologies.

Dans le présent rapport, on met généralement en évidence les pires scénarios (p. ex. puissance émettrice maximale, débit de données maximal, etc.) et on les compare aux valeurs limites. La charge de rayonnement réellement émise est normalement inférieure aux valeurs correspondant au pire scénario.

Les mesures précises du rayonnement émis par les réseaux sans fil sont très coûteuses et exigent de très bons instruments et de grandes connaissances. Des débits de données variables, l'étalement du signal sur plusieurs fréquences, etc. constituent autant d'obstacles à franchir lors de la mesure, qui peuvent facilement conduire à des erreurs systématiques.

2.1 Réseaux de type WPAN (Wireless Personal Area Networks), Bluetooth

Applications et normes

Bluetooth (IEEE 802.15.1) est la première norme WPAN pour les transmissions vocales et de données sur de courtes distances. Les émetteurs Bluetooth étant très petits et peu coûteux, et utilisant peu de courant, de très nombreux appareils en sont déjà équipés. On peut ainsi relier, par exemple, un téléphone mobile et un dispositif mains libres (figure 1) ou un ordinateur portable et un bureau (*desktop*) entre eux ou un ordinateur avec les périphériques comme le clavier, la souris, le joystick, les haut-parleurs, l'imprimante, la caméra, etc. De nouvelles applications sont développées en permanence. A l'échelle mondiale, environ 10 millions d'émetteurs Bluetooth étaient écoulés par semaine à fin 2005, et le marché est en constante augmentation.[7]

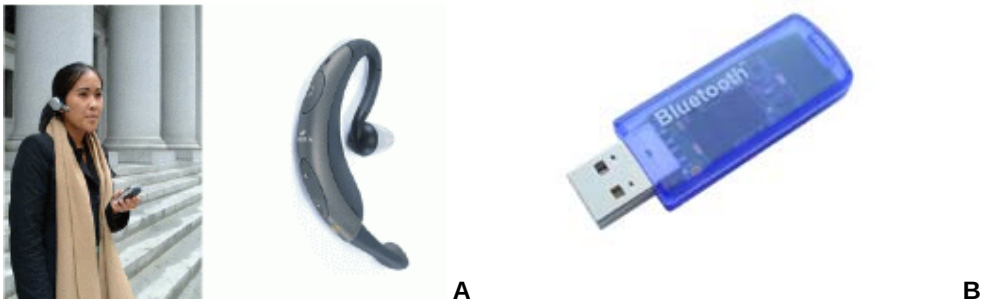


***Figure 1 A** La communication sans fil entre un téléphone mobile et un dispositif mains libres constitue un exemple d'application de Bluetooth[9]. **B** Clé USB avec émetteur Bluetooth*

[7] http://www.imsresearch.com

Mode de fonctionnement

Bluetooth émet dans la bande libre ISM[8], à une fréquence d'environ 2,45 GHz. La bande de fréquence est subdivisée en plusieurs canaux. Pour minimaliser les interférences avec d'autres réseaux Bluetooth ou d'autres applications radio fonctionnant à la même fréquence, le signal n'est pas émis sur un seul canal mais partiellement sur plusieurs (spectre étalé). A cet effet, on change en général de canal toutes les 625 µs au maximum (fast frequency hopping). Dans des intervalles de temps égaux, les utilisateurs du réseau émettent à tour de rôle leurs données, un utilisateur pouvant utiliser jusqu'à cinq intervalles de temps à la fois. Cela conduit à une caractéristique irrégulière, pulsée, du rayonnement, la fréquence de base de ce dernier étant généralement de 1600 Hz (1600 impulsions par seconde).

Lorsque deux appareils Bluetooth sont à portée l'un de l'autre, une liaison s'établit en général automatiquement. Dans un réseau simple, jusqu'à huit appareils peuvent être reliés activement entre eux. Dans ces conditions, un des appareils prend la direction (maître, master en anglais) et organise le trafic dans le réseau. Dans des réseaux structurés, cet appareil émet également en l'absence de transmissions de données afin que les autres appareils puissent se synchroniser par rapport à lui. A cet effet, le maître émet régulièrement un bref signal. Les autres appareils (esclaves, slaves en anglais) peuvent se déclencher afin d'économiser l'énergie et n'écouter le trafic du réseau que de temps en temps.

Pour diverses applications il existe trois classes de puissances différentes (cf. tableau 1). La classe de puissance 3, correspondant à la puissance la plus faible, est la plus répandue.

La puissance émettrice effective est généralement inférieure à la puissance maximale. Pour diverses raisons, il est avantageux de n'émettre qu'à une puissance telle que les récepteurs puissent encore juste capter le signal. Cela permet d'économiser la batterie et les autres installations ne sont pas perturbées. Un appareil peut mesurer la puissance reçue et demander à l'émetteur d'augmenter ou de diminuer, si possible, la puissance d'émission (régulation de la puissance). Par conséquent, la puissance d'émission, et donc aussi la charge due au rayonnement, ne sont pas constantes. La régulation de la puissance est obligatoire pour la classe de puissance 1 et, optionnelle, pour les classes 2 et 3.

Charge de rayonnement

Mesures d'immissions

A la demande de l'OFSP, des mesures ont été effectuées sur divers émetteurs Bluetooth. Deux clés USB différentes, équipées d'une antenne (classes de puissance 1 et 2)[9], et un PDA (personal digital assistant ou agenda électronique)[10] ont été examinés. Afin de simuler le pire scénario, les mesures ont été réalisées avec des débits de données maximaux et une puissance émettrice maximale.

[8] Industrial Scientific Medical-Band, bande de fréquence libre

[9] Kramer A et al. Development of Procedures for the Assessment of Human Exposure to EMF from Wireless Devices in Home and Office Environments. 2005

[10] Kühn S et al. Development of Procedures for the EMF Exposure Evaluation from Wireless Devices in Home and Office Environments. Supplement 1: Close-to-Body and Base Station Wireless Data Communication Devices. 2006

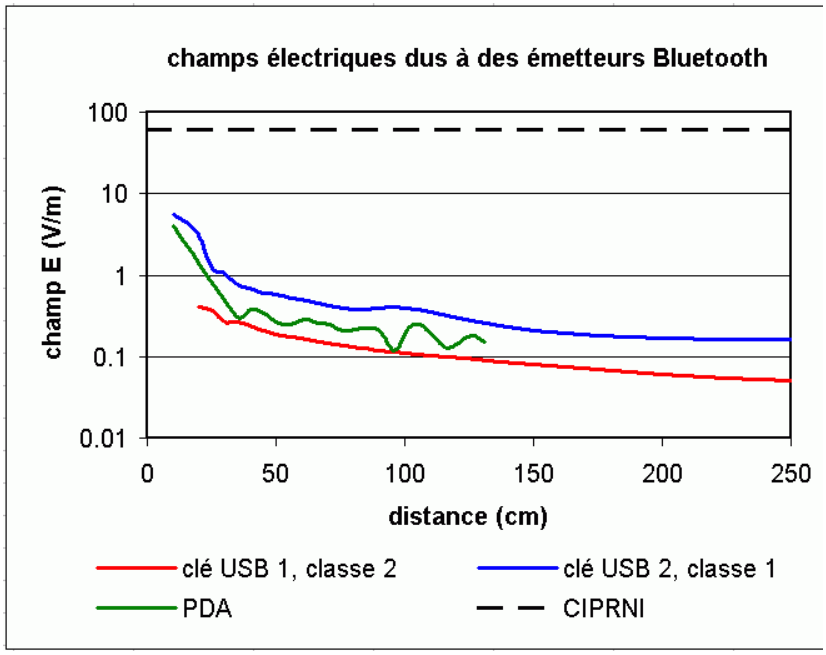


Figure 2 *Champ électrique (champ E) en fonction de la distance pour deux clés USB munies d'une antenne, de classes de puissance différentes, et un PDA. Pour le champ on a utilisé une échelle logarithmique, le champ diminuant très vite lorsque la distance augmente***.**

Les intensités de champ mesurées pour les émetteurs Bluetooth sont représentées sur la Figure 2 en fonction de la distance (cm). Dans les conditions du pire scénario, elles atteignent moins de 5 % (classe de puissance 1) et moins de 1 % (classe de puissance 2), des 61 V/m correspondant à la recommandation sur les valeurs limites de la CIPRNI.

Taux d'absorption spécifique TAS

Pour simuler la charge de rayonnement subie par le corps lorsque les appareils sont utilisés à proximité de celui-ci, les valeurs TAS ont été mesurées sur un fantôme. A cet effet, les émetteurs Bluetooth ont été fixés directement sur celui-ci. On a utilisé les mêmes clés USB et le même PDA que lors des mesures d'immissions (cf. figure 2). On a en outre mesuré les valeurs TAS relatives à deux dispositifs mains libres lors d'une liaison téléphonique avec un téléphone mobile situé à une distance de 1,5 m (les deux de la classe de puissance 3). Les résultats sont présentés dans le tableau 2.

Tableau 2 *Valeurs TAS liées à plusieurs émetteurs Bluetooth*

Dispositif	Classe de puissance	TAS (W/kg)
Clé USB 2	1	0,466
Clé USB 1	2	0,0092
PDA		0,01
Kit « mains libres » 1	3	0,00117
Kit « mains libres » 2	3	0,00319

Les valeurs TAS mesurées sont toutes inférieures à celles de la recommandation sur les valeurs limites de la CIPRNI (2 W/kg pour la tête et le corps, et 4 W/kg pour les extrémités).

2.2 Réseaux de type WLAN (Wireless Local Area Networks)

Applications et normes

Dans un réseau WLAN, on relie principalement des PC et des ordinateurs portables entre eux, ou des ordinateurs avec des périphériques (imprimantes, scanners, etc.) ou un point d'accès pour la liaison à Internet. A cet effet, les nouveaux ordinateurs portables sont équipés d'un chip WLAN ; il existe aussi des cartes WLAN à insérer dans les PC ou les ordinateurs portables (cf. figure 3). Certains agendas électroniques PDA disponibles sur le marché sont équipés de WLAN et peuvent aussi être utilisés comme téléphones mobiles.

Figure 3 *Points d'accès WLAN et cartes WLAN pour PC et ordinateurs portables* ***Fehler! Textmarke nicht definiert.***

Pour ce qui est des réseaux de type WLAN[11], les normes prédominantes sont les normes IEEE 802.11a, b, g et h (cf. Tableau 1), la plus répandue étant la norme IEEE 802.11g, qui a remplacé la norme IEEE 802.11b. Il existe également des appareils fonctionnant sous la norme IEEE 802.11a, mais leur exploitation n'est permise qu'à l'intérieur des bâtiments et à puissance réduite. En Europe, on a introduit à sa place la norme IEEE 802.11h, mais, pour le moment, les produits correspondants sont encore peu nombreux sur le marché.

Mode de fonctionnement

Les normes IEEE 802.11b et g émettent dans la bande libre ISM des 2,45 GHz. De nombreuses autres applications utilisant également ce domaine de fréquences, les interférences ne peuvent être exclues. Les normes IEEE 802.11a et h émettent dans la bande de fréquence située entre 5,15 GHz et 5,35 GHz, et pour la IEEE 802.11h, également entre 5,47 et 5,725 GHz. En Suisse (et en Europe), ce domaine est également utilisé pour d'autres services. C'est pourquoi l'utilisation d'appareils de la norme a n'est autorisée qu'à puissance réduite et qu'à l'intérieur des bâtiments. En Europe, la norme h a été adaptée de manière à ce que la fréquence puisse être immédiatement libérée lorsqu'une autre application en a besoin.

Les réseaux WLAN peuvent être exploités en mode infrastructure ou en mode ad hoc. Dans un réseau ad hoc, les PC ou les autres composants sont directement reliés entre eux. En mode infrastructure, la transmission des données s'effectue par le biais d'un nœud de réseau central (point d'accès). Par ce dernier, le réseau peut également être relié à un autre réseau (Internet, Ethernet). La plupart des réseaux WLAN fonctionnent en mode infrastructure.

Lorsqu'un appareil veut émettre, il écoute d'abord un instant si un autre appareil est déjà en train d'émettre. Si ce n'est pas le cas, il peut le faire. La durée d'émission n'est pas fixée et le point d'accès ne la contrôle pas. En général, le point d'accès émet un signal toutes les 100 ms pendant 0,5 ms (trame

[11] On confond souvent WLAN et WiFi. Le WiFi n'est toutefois qu'un certificat de certains fabricants devant garantir l'interopérabilité des divers produits WLAN.

balise, beacon en anglais) de manière à ce que les divers appareils puissent se synchroniser par rapport à lui. De ce fait, le beacon émet à une fréquence de répétition de 10 Hz.

Pour économiser la batterie, un appareil peut se mettre en veille lorsqu'il n'attend pas de transmission de données. Dans un système ad hoc, l'appareil doit se réenclencher pour chaque beacon. En mode infrastructure, le point d'accès est informé sur chaque mise en veille ; les appareils se remettent donc moins souvent en service pour écouter le beacon et pour tenter de savoir si des données sont présentes dans la mémoire tampon du point d'accès.

Dans la norme h, la puissance d'émission est régulée automatiquement en fonction de la qualité de réception. En outre, la puissance d'émission des points d'accès des normes g et h peut être régulée en fonction de la portée demandée. A l'intérieur d'une norme, la puissance émettrice effective dépend en premier lieu du trafic de données. Si un point d'accès de 100 mW n'émet que le beacon, la puissance émettrice moyenne est de 0,5 mW. Si, toutefois, de nombreuses données sont émises, la puissance d'émission peut pratiquement atteindre la puissance maximale permise, soit 100 mW.

L'intensité d'un signal émis par une antenne diminue fortement avec la distance. En outre, le signal peut être atténué ou réfléchi par des obstacles tels que les murs. Pour un émetteur de 100 mW de la norme 802.11b, les portées normales sont de l'ordre de 200 m dans un espace dégagé et de 40 m à l'intérieur des bâtiments ayant des murs peu épais. Des murs en béton armé ou des verres isolants avec couches réfléchissantes ne laissent pratiquement passer aucun rayonnement. La portée des appareils de la norme h est plus grande dans un espace dégagé en raison de la puissance d'émission plus élevée. En raison de sa fréquence plus élevée le signal est toutefois plus fortement atténué par les murs, ce qui conduit à une portée réduite à l'intérieur des bâtiments.

Hotspots WLAN

L'espace dans lequel un accès à Internet est disponible via un réseau WLAN est appelé «hotspot». Les hotspots peuvent être publiques (gares, aéroports, etc.) ou n'être accessibles qu'à un cercle restreint d'utilisateurs (hôtels). L'accès à Internet via des hotspots est généralement payant mais il existe également des offres gratuites. A l'intérieur des bâtiments, les points d'accès sont principalement montés au plafond ou aux murs, rarement dans les planchers doubles ; à l'extérieur, ils sont placés sur les façades ou sur les toits des bâtiments. Lorsque plusieurs points d'accès sont installés sur un hotspot, ils le sont généralement à des intervalles de 10 à 20 m.

Charge de rayonnement : les pires scénarios

Mesures d'immissions

A la demande de l'OFSP, des points d'accès WLAN, des cartes PC et un PDA aux normes 802.11a, b et g ont été examinés[9,10]. On a déterminé les champs électriques et les valeurs TAS, toujours dans les conditions du pire scénario, avec un débit de données maximal. Les champs électriques ont été mesurés près de deux points d'accès différents, de deux cartes PC différentes et d'un PDA (figure 4). Certains appareils WLAN pouvant être exploités sous plusieurs normes, les mesures relatives au point d'accès 2 (figure 4) ont été effectuées pour les normes a, b et g. Aucun appareil fonctionnant sous la norme h n'était disponible ; elle est cependant comparable à la norme a dans les conditions du pire scénario. Dans les conditions réelles, la charge de rayonnement due à la norme h devrait être inférieure à celle due à la norme a, en raison du fait que la première doit disposer d'une régulation de la puissance d'émission qui soit dynamique.

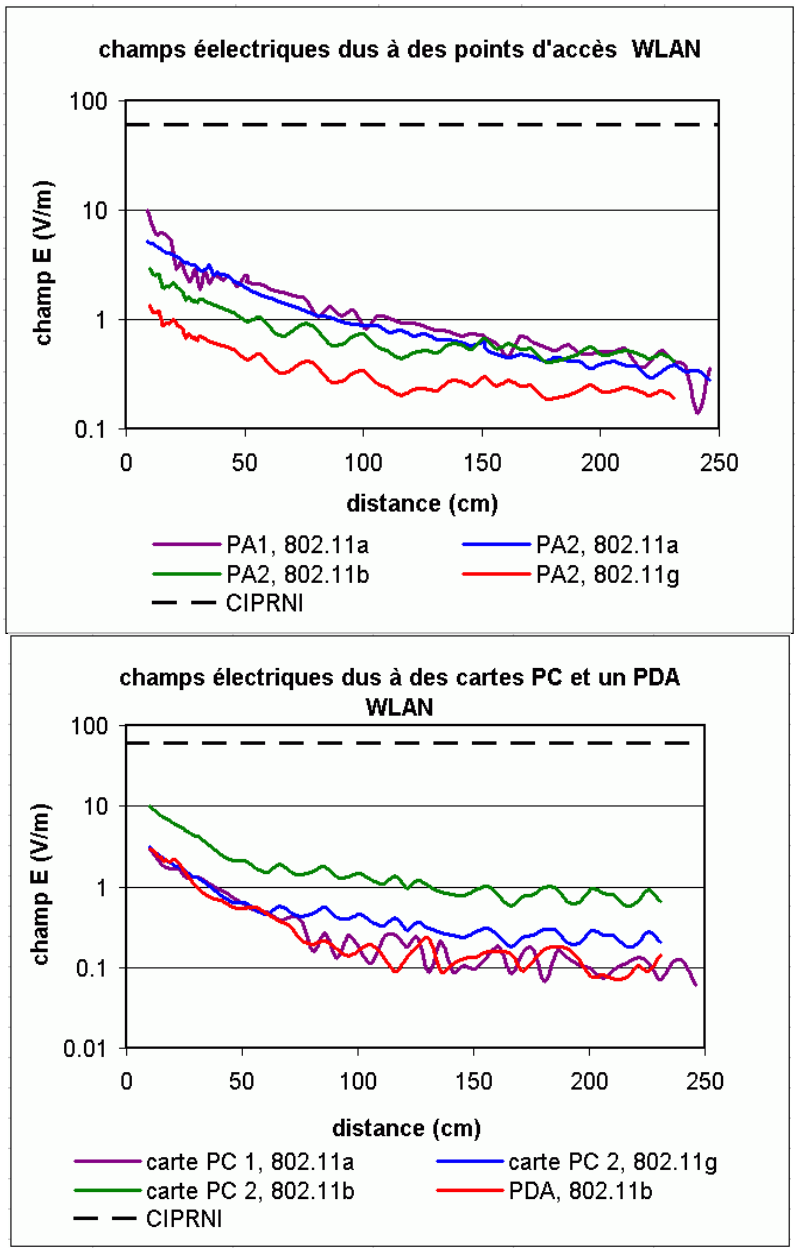


Figure 4 *Champ électrique (champ E) en fonction de la distance pour divers produits WLAN (points d'accès, cartes PC et PDA). Le champ est représenté dans une échelle logarithmique.*

Les champs électriques diminuent fortement lorsqu'on s'éloigne de l'émetteur. Les intensités sont toujours inférieures à la valeur limite de 61 V/m, recommandée par la CIPRNI. A une distance de 20 cm, aucun des appareils n'atteint plus de 10 % de cette valeur limite, à 1 m même pas 2,5 %.

Les immissions générées par les réseaux WLAN publics devraient être environ égales à celles dues aux réseaux WLAN privés, les deux comportant des émetteurs fonctionnant sous la même norme. Le Tableau 3 présente des valeurs des intensités de champ électrique dues à des points d'accès WLAN publics.

Tableau 3 *Intensité de champ électrique de points d'accès publics avec des puissances d'émission de 100/200 mW*[12]

Distance / point d'accès (m)	Intensités de champ électrique (V/m)
1	0,7 – 3
2	0,4 – 1,5
5	0,1 – 0,7
10	0,05 – 0,4

Taux d'absorption spécifique TAS

Pour mesurer les valeurs TAS correspondantes, les appareils WLAN ont été fixés à un fantôme. Le tableau 4 présente les valeurs TAS des appareils. La charge de rayonnement due au réseau WLAN dépendant aussi de la puissance d'émission de l'appareil et du débit de données, ceux-ci y figurent également. On notera que les diverses normes utilisent des méthodes de transmission de données différentes conduisant à des charges de rayonnement différentes. Bien que la norme g ait une transmission de données plus élevée que la norme b, la charge de rayonnement qu'elle génère est plutôt inférieure.

Tableau 4 *Valeurs TAS de points d'accès (PA), de cartes PC et d'un PDA*

802.11a			
Dispositif	**Puissance d'émission (mW)**	**Débit de données (Mb/s)**	**TAS (W/kg)**
PA 1	40	30	0,54
PA 2	100	6	0,18
PA 4	40	7,5	0,1
PA 5	40	28	0,36
Carte PC 1	32	13,3	0,05
Carte PC 2	63	13,3	0,07
Carte PC 3	89	13,3	0,06

802.11b			
Dispositif	**Puissance d'émission (mW)**	**Débit de données (Mb/s)**	**TAS (W/kg)**
PA 3	95	6	0,44
PA 2	100	6	0,73
Carte PC 4	214	6,3	0,43
Carte PC 5	89	6	0,13
PDA	non spécifié	3.8	0,067

802.11g			
Dispositif	**Puissance d'émission (mW)**	**Débit de données (Mb/s)**	**TAS (W/kg)**
PA 3	95	26	0,25
PA 2	100	26	0,27
Carte PC 4	151	21,5	0,11
Carte PC 5	89	26	0,06

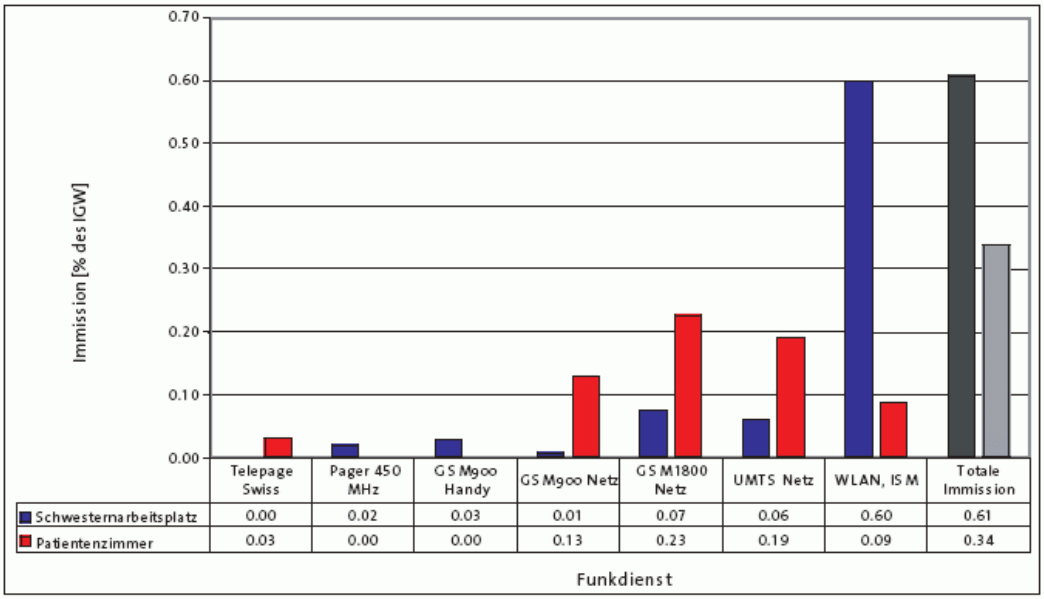
Toutes les valeurs TAS sont inférieures à celles de la recommandation sur les valeurs limites de la CIPRNI, soit à 2 W/kg (tête, corps) ou à 4 W/kg (extrémités). En réalité, les valeurs TAS des points d'accès importent probablement peu, ceux-ci n'étant pas proches du corps lors de leur exploitation. En revanche, les cartes PC ou le PDA peuvent très bien être exploités à proximité du corps.

[12] « L'électrosmog dans l'environnement », OFEFP, Berne 2005, page 54

Charge de rayonnement : scénarios réels

Mesures d'immissions

Oertle et al.[13] ont effectué des mesures d'immissions à l'hôpital de Thoune lors de l'exploitation normale d'un réseau WLAN. Tout l'hôpital est équipé de systèmes WLAN afin que les actes électroniques relatifs aux patients soient également disponibles au pied du lit de ceux-ci. Les mesures ont été effectuées à un poste de travail d'infirmière et dans une chambre de patient. Lors des mesures, le réseau WLAN, normalement chargé, transmettait en outre un gros fichier. En plus du rayonnement dû au réseau WLAN ont également été déterminés les rayonnements dus aux réseaux de téléphonie mobile et des pagers.



	Telepage Swiss	Pager 450 MHz	GSMgoo Handy	GSMgoo Netz	GSM1800 Netz	UMTS Netz	WLAN, ISM	Totale Immission
Schwesternarbeitsplatz	0.00	0.02	0.03	0.01	0.07	0.06	0.60	0.61
Patientenzimmer	0.03	0.00	0.00	0.13	0.23	0.19	0.09	0.34

***Figure 5** (Source :[13]) Intensités de champ électrique dues à divers services de radiocommunication comparées aux valeurs limites d'immissions (IGW, correspond aux recommandations sur les valeurs limites de la CIPRNI). Schwesternarbeitsplatz: poste d'infirmière, Patientenzimmer: la chambre du patient*

Au poste d'infirmière, d'où le point d'accès était visible, le rayonnement dû au réseau WLAN apporte la contribution la plus importante à la charge de rayonnement locale, et il se monte à 0,6 % de la recommandation sur les valeurs limites de la CIPRNI concernant la population en général. Dans la chambre du patient, c'est le rayonnement de la téléphonie mobile qui prédomine. L'immission globale dans le domaine des hautes fréquences n'atteint pas 1 % de la recommandation sur les valeurs limites de l'CIPRNI. Sur la figure 5, il apparaît clairement qu'en présence d'une source de rayonnement proche, comme le WLAN du poste d'infirmière, la majeure partie de l'immission globale provient de ladite source.

A la demande de l'Office fédéral allemand de la radioprotection, ARC Seibersdorf research GmbH procède actuellement à des simulations et des mesures d'immissions relatives à des hotspots WLAN[14]. Dans un café équipé d'un point d'accès situé sous le bar et de deux ordinateurs portables, des mesures ont été effectuées en divers endroits du local pendant le téléchargement de données. Afin que les valeurs mesurées aient pu être comparées à la valeur de référence de la CIPRNI (cf. paragraphe 3.2 et Tableau 5), on a effectué une moyenne spatiale sur tout le corps et une moyenne temporelle sur 6 minutes. La valeur la plus élevée (à peine 2 V/m) a été mesurée à proximité du point d'accès situé derrière le bar ; elle représente 3,2 % de la valeur limite recommandée par la CIPRNI[15]. Dans ce cas concret, le champ pourrait être réduit simplement en installant le point d'accès au plafond.

---

[13] Oertle M et al. Elektromagnetische Felder im Akutspital: Wireless-LAN & Co als Risiko?. Praxis 2006; 95:933-941.

[14] Schmid G. et al. Bestimmung der realen Feldverteilung von hochfrequenten elektromagnetischen Feldern in der Umgebung von Wireless LAN-Einrichtungen (WLAN) in innerstädtischen Gebieten. 2. Zwischenbericht zum Forschungsvorhaben FM 8826

[15] Dans la publication on indique la densité de puissance, à partir de laquelle la valeur du champ électrique est calculée. Les deux grandeurs n'étant pas reliées de manière linéaire, les pourcentages par rapport à la valeur limite sont donc également différents.

2.3 Réseaux de type WMAN (Wireless Metropolitan Area Networks), WiMAX

Applications et normes

Les réseaux sans fil métropolitains (WMAN) sont conçus pour étendre les réseaux sans fil au-delà du domaine local. Au contraire des réseaux locaux sans fil WLAN, qui ont des portées de 40 à 200 m, les réseaux WMAN, avec des portées de plusieurs kilomètres, peuvent couvrir des villes entières.

La norme IEEE 802.16 relative aux réseaux WMAN est conçue de manière très ouverte et comprend les fréquences allant de 2 à 66 GHz. Afin de contrer le danger lié à des installations trop différentes et à une offre trop diversifiée, présentant des coûts de fabrication correspondants plus élevés, les fabricants de systèmes et de composants ont fondé le Forum WiMAX (WiMAX : Worldwide interoperability for microwave access). Celui-ci sélectionne, parmi les nombreuses options offertes par la norme 802.16, diverses combinaisons et les offre sous forme de « profils ». Actuellement, WiMAX prévoit trois profils se différenciant principalement par la bande de fréquence (état août 04) : régime de la concession : 2,5 GHz et 3,5 GHz, fréquence libre : 5,8 GHz. A la demande des clients WiMAX, d'autres profils peuvent être définis. Les premiers appareils (stations de base et terminaux) ont été certifiés par WiMAX en janvier 2006. Les applications possibles de WiMAX sont présentées sur la figure 6.

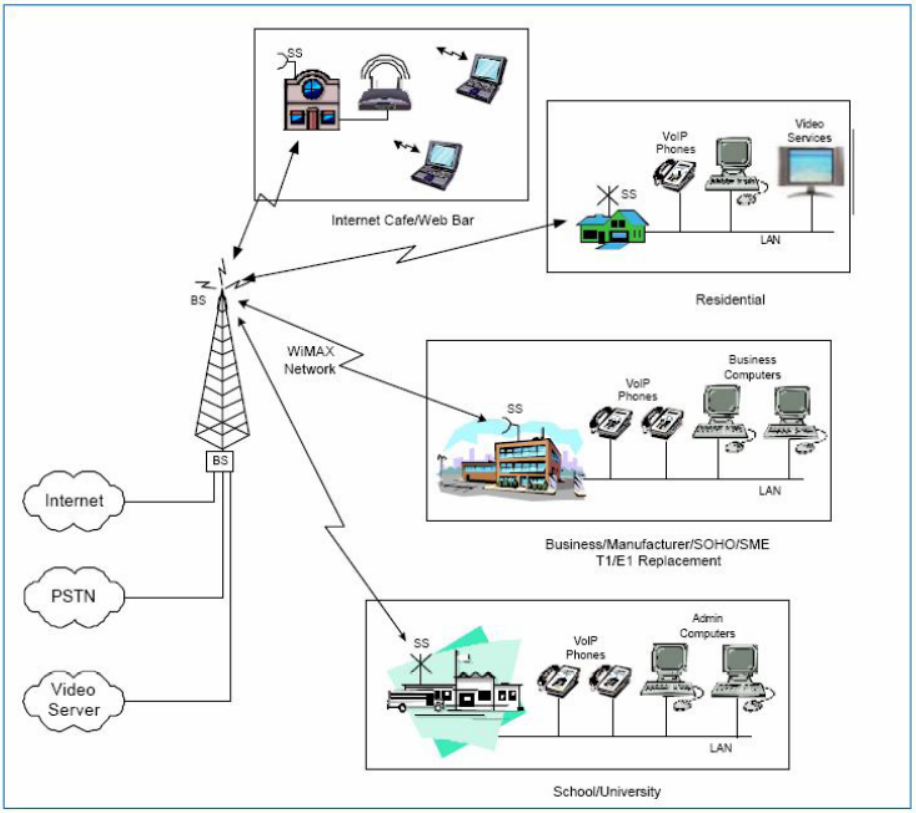


Figure 6 *Applications possibles de WiMAX. Source :* [16]

Les concessions en Suisse

Le 7 juin 2006, la Commission fédérale de la communication (ComCom) a octroyé à Swisscom Mobile une concession WiMAX pour la bande des 3,5 GHz[17]. Le concessionnaire est tenu de lancer l'exploitation commerciale d'ici au 31 décembre 2007 et d'exploiter, d'ici à fin 2009, au moins 120 unités

[16] www.wimaxforum.org
[17] http://www.bakom.ch/dokumentation/medieninformationen/00471/index.html?lang=fr&msg-id=5474

d'émission/réception. Lors de la construction du réseau, les conditions de l'ordonnance sur la protection contre le rayonnement non ionisant (ORNI, cf. paragraphe 5.3) doivent être respectées.

Mode de fonctionnement et charge de rayonnement

WiMAX constitue un accès à large bande (Broadband Wireless Access, BWA), permettant des débits de données plus élevés et étant, par conséquent, prévu en premier lieu pour un accès sans fil à Internet (en remplacement des modems câble ou ADSL). Les services sont surtout intéressants dans des régions non câblées. Le débit de données maximal n'est cependant atteint que sur de courtes distances. Il dépend de la largeur de bande du canal utilisée et peut atteindre, dans des conditions optimales, jusqu'à 75 Mbit/s pour un canal de 20 MHz. Le débit de données diminue cependant lorsque les distances augmentent. Selon la configuration du système, la portée peut aller jusqu'à 30 à 40 kilomètres avec un débit de données réduit.

Dans le cas des normes actuelles, il s'agit de services fixes de type point à multipoint. Pour une application fixe, une unité d'émission/réception est montée sur la façade de la maison du client (figure 7). A l'intérieur de celle-ci, les terminaux peuvent être reliés à une boîte.

Figure 7 *Installations d'émission/réception WiMAX fixées aux façades ou sur les toits. Source :*[18]

Afin de pouvoir offrir aux clients le débit de données élevé prévu, avec les capacités correspondantes, il y aura lieu de créer des structures de réseau analogues à celles des réseaux de téléphonie mobile. Cela signifie qu'on devra construire un plus grand nombre de stations de base. Bien que des puissances d'émission allant théoriquement jusqu'à 3 kW PIRE soient possibles dans les bandes pour lesquelles une concession a été octroyée, la puissance d'émission effectivement nécessaire dépend fortement de la structure du réseau et est fixée par l'opérateur. Les stations de base ayant des puissances émettrices supérieures à 6 W ERP doivent respecter la valeur limite de l'installation de l'ORNI (6 V/m). Il faut s'attendre à ce que les stations de base WiMAX présentent des puissances émettrices supérieures à 10 W ERP. Les valeurs limites concernant les stations de base WiMAX correspondent à celles des stations de base de la téléphonie mobile.

Les réseaux WiMAX sont en phase de développement, mais il reste à voir s'ils couvriront tout le territoire. L'intensité dépend fortement du réseau. Mais on peut supposer que les valeurs se situent dans un ordre de grandeur analogue à celui des réseaux de téléphonie mobile.

2.4 Développement ultérieur

Il règne à l'heure actuelle une intense activité aussi bien dans le domaine de l'élaboration de nouvelles normes de télécommunication que dans celui du développement et de la fabrication d'appareils comportant des dispositifs d'émission/réception correspondants, l'objectif étant d'augmenter le débit de données pour tous les services.

[18] www.wimaxxed.at

A l'avenir, les liaisons filaires entre les appareils seront de plus en plus souvent remplacées par des liaisons Bluetooth. Cela est également intéressant pour les applications médicales impliquant une transmission de données vitales. Grâce à Bluetooth on peut réduire le nombre de câbles à proximité du lit du patient et celui-ci peut ainsi se mouvoir plus librement. La portée de Bluetooth peut être augmentée grâce à des liaisons à plusieurs bonds (multihop), le signal entre l'émetteur et le récepteur final transitant par des émetteurs Bluetooth intermédiaires[19].

Les réseaux WLAN sont perfectionnés, entre autres, dans le but de pouvoir également transmettre des données prioritaires, pour lesquelles la qualité de transmission et l'immunité aux perturbations sont importantes, par exemple téléphoner par Internet (voice over IP) ou transmettre des films et de la musique dans les appartements.

Dans le cas de WiMAX, il est également prévu d'autoriser à l'avenir des services nomades et, à moyen terme, des services mobiles (IEEE 802.16e). Par service nomade on entend l'utilisation d'un terminal en n'importe quel lieu pour autant que le terminal reste fixe lors de l'utilisation.

A présent on fabrique également des chips compatibles WiMAX dont on équipe les ordinateurs portables et qui permettent ainsi, dans les zones couvertes par WiMAX, d'accéder à Internet à des distances plus élevées que celles permises par les réseaux WLAN actuels. On peut admettre que la charge de rayonnement due à ces appareils soit également plus élevée.

La gestion des fréquences constitue une problématique particulière. Les applications WLAN s'effectuent aujourd'hui dans la bande de fréquence des 5 GHz, avec des puissances d'émission pouvant aller jusqu'à 1 W. En Suisse, le domaine de fréquence supérieur (à partir de 5,725 GHz) est à l'heure actuelle principalement utilisé par les militaires. On envisage de libérer ce domaine pour le BWA (Broadband Wireless Access) avec des puissances d'émission pouvant aller jusqu'à 4 W. Il s'agit d'une bande ISM, c'est-à-dire une bande dans laquelle diverses autres applications radio à courte distance peuvent également être librement exploitées. A l'avantage de la liberté font face les inconvénients des interférences réciproques de divers services et de la faible puissance d'émission. En supposant que la coexistence avec d'autres services soit possible, des applications BWA pourraient se développer dans cette bande.

[19] Andreas Kuntz et al. ScatterNetz-Routing (SNR) - Multihopkommunikation für medizinische Bluetooth Ad Hoc Netzwerke. Proceedings der Gemeinsamen Jahrestagung der Deutschen, Österreichischen und Schweizerischen Gesellschaft für Biomedizinische Technik, 6.-9. September 2006, Zürich.

3. Effets sur la santé

3.1 CEM à haute fréquence : effets thermiques

Les seuls effets exercés par le rayonnement à haute fréquence sur la santé, démontrés de manière scientifique, sont les effets thermiques. Les CEM à haute fréquence pénètrent dans le corps et, ce faisant, ils peuvent échauffer les tissus, l'énergie de rayonnement absorbée se transformant en chaleur. Dans de nombreuses études portant sur les animaux, on a montré qu'un échauffement du corps entier ou d'une partie de celui-ci, conduisant à une élévation de la température de plus de 1 °C, peut entraîner une altération irréversible des tissus. Les données concernant les réactions des êtres humains, acquises lors d'essais de laboratoire sur des volontaires ou lors d'études épidémiologiques sur des personnes travaillant avec des radars ou des dispositifs de diathermie, montrent également clairement qu'un échauffement des tissus de plus de 1 °C peut entraîner des altérations de tissus et des réactions fiévreuses.

La grandeur dosimétrique correspondant aux effets thermiques est le *taux d'absorption spécifique TAS* (exprimé en W/kg), soit l'énergie absorbée par unité de temps et par unité de poids corporel. Bien qu'il existe divers effets thermiques et que la sensibilité thermique varie beaucoup d'un tissu à l'autre, les expériences et les calculs réalisés montrent clairement que seule une exposition de 30 minutes avec un TAS pour le corps entier de plus de 4 W/kg peut entraîner une élévation de température de 1 °C. Dans ces conditions, en effet, les mécanismes de régulation thermique de l'organisme (p. ex. la transpiration) n'arrivent plus à éliminer l'excédent de chaleur.

Outre ces effets thermiques, des CEM très fortement pulsés, d'une durée de pulsation de moins de 30 μs et d'une fréquence de 300 MHz à 6 GHz, peuvent provoquer des perceptions auditives.

3.2 CEM à haute fréquence : valeurs limites internationales (protection contre les effets thermiques)

En matière de CEM haute fréquence, les effets thermiques sont les seuls effets dont la relation de cause à effet a pu être démontrée. Comme évoqué au chapitre précédent, il s'agit d'effets aigus, apparaissant à partir d'un TAS seuil de 4 W/kg. Ces effets et la valeur seuil constituent le point de départ de la fixation des valeurs limites.

La plupart des pays ont fixé des valeurs limites légales fondées sur les recommandations de la CIPRNI (Commission internationale de la protection contre le rayonnement non ionisant, en anglais ICNIRP). Celle-ci vérifie périodiquement les publications scientifiques en relation avec les caractéristiques physiques de sources de CEM et les effets biologiques et sanitaires de celles-ci. Elle évalue ces derniers et émet des recommandations[20].

Les données de laboratoire tout comme les essais limités effectués sur l'homme montrent que la capacité de régulation thermique de l'organisme varie fortement d'un individu à l'autre et qu'elle dépend également d'autres facteurs tels que la température ambiante, la consommation d'alcool, etc. C'est pourquoi la CIPRNI utilise, dans le calcul de la valeur limite, un facteur de sécurité de 10 pour les personnes exposées dans l'exercice de leur profession et de 50 pour la population en général.

Ces valeurs limites, définies pour le TAS en tant que grandeur dosimétrique, sont qualifiées de valeurs limites de base. Le TAS ne pouvant pas être déterminé facilement, on a défini, dans l'optique de l'évaluation des expositions, des valeurs limites de référence plus simples à mesurer. Elles sont valables pour une exposition uniforme du corps entier à des champs électromagnétiques. Les valeurs limites de

[20] http://www.icnirp.de/

référence sont déduites des valeurs limites de base de manière conservatrice, le respect des valeurs limites de référence signifiant dans tous les cas également le respect des valeurs limites de base. Les valeurs limites de base et de référence significatives pour les réseaux sans fil figurent dans le tableau 5.

Tableau 5 *Valeurs limites de base et valeurs de référence (CIPRNI) pour les personnes exposées dans l'exercice de leur profession et la population en général, dans la gamme de fréquence 10 MHz - 10 GHz.*

Personne exposée	TAS moyen du corps entier (W/kg)	Champ électrique (V/m) Valeur de référence pour le TAS du corps entier	TAS local tête et tronc (W/kg)	TAS local membres (W/kg)
Personnes exposées dans l'exercice de leur profession	0,4	137	10 (0,1 W/10g)	20 (0,2 W/10g)
Population en général	0,08	61	2 (0,02 W/10g)	4 (0,04 W/10g)

Ces valeurs limites sont également applicables en Suisse. Comme le montre les résultats des mesures effectuées (cf. chapitre 2), les expositions dues aux réseaux actuels se situent très en dessous des valeurs limites.

3.3 CEM à haute fréquence : investigation des effets non thermiques

Outre les effets thermiques prouvés exercés par les CEM à haute fréquence, il existe des indications quant à d'autres effets dus à des expositions plus faibles, inférieures aux valeurs limites. Les études correspondantes ont portés principalement sur la téléphonie mobile. On a par exemple constaté que les CEM à haute fréquence des téléphones mobiles pouvaient provoquer de légères modifications de l'activité cérébrale. On ne sait cependant pas si et dans quelle mesure ces modifications exercent une influence sur la santé. Actuellement il n'est pas possible d'établir une relation de cause à effet entre une fréquente utilisation du téléphone mobile et l'apparition de tumeurs du cerveau. Les effets exercés par le rayonnement des antennes de téléphonie mobile sur le bien-être de la population vivant aux alentours (insomnies, maux de tête et autres symptômes non spécifiques) ne sont pas non plus prouvés scientifiquement. En outre sont ouvertes les questions de l'électrosensibilité de certaines personnes (problèmes de santé que les personnes concernées attribuent à l'influence des CEM) et d'une éventuelle sensibilité particulière des enfants.

Des évaluations de toutes les données disponibles concernant les effets exercés par les CEM à haute fréquence sur la santé sont prévues pour 2008 par le CIRC (Centre international de recherche sur le cancer ; en anglais, IARC - International Agency for Research on Cancer) pour ce qui est du risque de cancer et par l'OMS pour ce qui est des effets généraux. Les résultats seront publiés dans les *Monographies du CIRC* et dans le *WHO-Environmental Health Criteria*. En parallèle, la CIPRNI élabore une nouvelle évaluation des bases scientifiques et envisage de publier éventuellement de nouvelles recommandations sur les valeurs limites.

3.4 Problématique spécifique aux réseaux sans fil

Jusqu'ici aucune étude portant sur les effets biologiques et sanitaires exercés par le rayonnement de réseaux sans fil comme le WLAN et Bluetooth n'a été réalisée. Des études générales portant sur les effets non thermiques des CEM à haute fréquence sont toutefois menées, qui permettront peut-être de tirer des conclusions quant aux effets exercés par les réseaux sans fil sur la santé.

L'évaluation des effets exercés par les réseaux sans fil sur la santé est cependant rendue difficile par le fait que les caractéristiques des expositions peuvent être totalement différentes d'une utilisation à l'autre;

il n'existe pas d'exposition spécifique aux réseaux sans fil. Des expositions locales plus fortes apparaissent là où des unités émettrices sont positionnées très près du corps. L'intensité du rayonnement dépendant fortement de la distance, les expositions du corps entier par rapport à des points d'accès plus éloignés sont quant à elles très faibles.

En outre, les technologies des réseaux sans fil évoluent de manière fulgurante. Elles ont une durée de vie courte, sont remplacées rapidement et peuvent être dépassées en l'espace de deux à trois ans. Les caractéristiques du rayonnement des nouvelles technologies sont en partie totalement différentes de celles du rayonnement des technologies qui ont précédé. Les études scientifiques portant sur les effets exercés par des technologies spécifiques sur la santé présentent le risque que lesdites technologies n'existent plus au terme de l'étude.

Il existe en outre de plus en plus d'appareils multifonctionnels (comme le PDA étudié) combinant divers services comme le WLAN, Bluetooth et la téléphonie mobile, et pouvant être utilisés en partie simultanément.

A l'avenir, la charge de rayonnement pourrait augmenter, de plus en plus de postes de travail et de ménages étant équipés de WLAN, et les technologies nouvelles présentant en outre des puissances émettrices maximales plus élevées. On introduit également de plus en plus de réseaux WLAN à l'échelle d'une ville ou de parties de ville[21]. Les expositions pourraient aussi augmenter du fait de la présence de plusieurs appareils ayant des caractéristiques de rayonnement différentes.

3.5 Effets indirects, compatibilité électromagnétique

Par effets indirects, on entend les effets exercés sur la santé, non pas par le rayonnement lui-même, mais par la perturbation et, partant, par le dysfonctionnement d'un appareil, en général dans le domaine médical. L'insensibilité fonctionnelle des appareils électromagnétiques aux différents CEM est appelée compatibilité électromagnétique (cf. paragraphe 5.4).

Par principe on distingue deux modes de perturbation :

- Le rayonnement des réseaux sans fil perturbe la fonctionnalité d'autres appareils électroniques.
- Les réseaux sans fil sont perturbés par des appareils électriques à micro-ondes. Le rayonnement de ces appareils couvre celui des réseaux sans fil, ce qui peut provoquer un dysfonctionnement de ces derniers.

Concernant l'influence électromagnétique exercée par les réseaux sans fil sur des dispositifs médicaux, il existe quelques rares études portant sur des appareils utilisés dans les hôpitaux et des dispositifs électroniques d'aide physique et des implants.

Perturbation des stimulateurs cardiaques et des défibrillateurs par les réseaux WLAN[22]
La sensibilité des stimulateurs cardiaques unipolaires et bipolaires et des défibrillateurs aux perturbations dues à des réseaux WLAN a été étudiée au moyen d'un PDA émettant directement sur les différents implants (non implantés) à une puissance maximale de 100 mW. Aucun effet n'a pu être détecté. Les auteurs recommandent de répéter l'étude avec des porteurs d'implants, de manière à pouvoir confirmer les résultats en situation réelle. Selon les normes relatives aux produits, les stimulateurs cardiaques et les défibrillateurs doivent résister à des fréquences allant jusqu'à 2,5 GHz. Il faudrait donc impérativement réaliser l'étude portant sur les appareils WLAN de la norme a ou h à une fréquence de 5 GHz.

[21] P. ex. Saint-Gall (www.openwireless.ch) ou Lucerne (« surf-on-the-fly »)
[22] Tri JL, Trusty JM, Hayes DL. Potential for Personal Digital Assistant interference with implantable cardiac devices. Mayo Clin.Proc. 2004;79:1527-30.

Perturbation d'autres appareils par les réseaux WLAN des hôpitaux[23]
Une étude a montré que la plupart des appareils examinés étaient insensibles au rayonnement émis par un réseau WLAN. Des appareils Doppler à ultrasons, utilisés pour la surveillance des fonctions cardiaques, ont été perturbés. Le rayonnement WLAN a généré des interférences acoustiques supplémentaires, pouvant être source d'erreurs d'interprétation du rythme cardiaque normal du patient.

Une étude[24] a montré que les réseaux WLAN exerçaient une influence sur des systèmes de dilution et sur un ventilateur, dans les domaines de fréquence des 2,45 et des 5,2 GHz. Les auteurs recommandent de tester chaque appareil utilisé quant à son immunité aux perturbations rayonnées lors de l'introduction de réseaux WLAN dans les hôpitaux.

Une étude[25] a porté sur l'influence exercée par un réseau WLAN de la norme g sur six dispositifs médicaux différents. On a ainsi pu mesurer des déviations sur une pompe à perfusion (2,4 % de déviation dans le volume du bolus) et un stimulateur nerveux et musculaire (jusqu'à 10 % de déviation). Les déviations étaient cependant inférieures à celles admises par la norme concernant ces produits.

Perturbation d'appareils électroniques des hôpitaux par Bluetooth[26]
Une étude a porté sur les effets exercés par Bluetooth sur les appareils électroniques utilisés dans les hôpitaux (soins intensifs et salle d'opération). Aucun des dispositifs testés n'a été sensible au rayonnement Bluetooth. Les auteurs en concluent que la technologie Bluetooth pourrait contribuer à réduire le câblage autour des patients. Ils recommandent cependant de garantir la fonctionnalité des applications Bluetooth par des tests stricts.

Perturbation des réseaux WLAN par d'autres dispositifs[27]
Dans une étude portant sur la perturbation des réseaux WLAN par des dispositifs médicaux à micro-ondes (fours à micro-ondes, électrochirurgie, système de télémétrie), on a pu montrer qu'un réseau WLAN était parasité lorsque des fours à micro-ondes étaient disposés près des points d'accès. Cela a eu pour effet une diminution de la qualité de réception ainsi que du taux de transmission des données. Les auteurs en concluent que les fours à micro-ondes industriels, utilisés dans les hôpitaux, ne doivent pas être positionnés près des points d'accès.

Perturbation de Bluetooth par d'autres dispositifs
Dans l'étude portant sur les effets exercés par Bluetooth sur les appareils électroniques[26], on a également examiné la perturbation de Bluetooth par 44 autres appareils électroniques. Aucun effet n'a pu être détecté. Toutefois, les auteurs rendent attentifs au fait que les liaisons par Bluetooth peuvent être perturbées par des réseaux WLAN.

3.6 Résumé

Selon les connaissances actuelles et sur la base des mesures d'exposition disponibles, le rayonnement à haute fréquence généré par les réseaux sans fil est trop faible pour provoquer, par absorption et via une élévation de température consécutive, des effets sanitaires aigus et détectables. Les effets à long terme et les effets non thermiques ont encore été trop peu étudiés. A l'heure actuelle, les études effectuées sur les effets exercés par les CEM à haute fréquence dans le domaine des faibles doses, en des-

[23] Wallin MK, Marve T, Hakansson PK. Modern wireless telecommunication technologies and their electromagnetic compatibility with life-supporting equipment. Anesth.Analg. 2005;101:1393-400.
[24] Hanada E et al. Negligible electromagnetic interaction between medical electronic equipment and 2.4 GHz band wireless LAN. J Med Syst. 2002;26:301-8.
[25] Schröttner J et al. Are electro medical devices influenced by electromagnetic WLAN emissions? Proceedings der Gemeinsamen Jahrestagung der Deutschen, Österreichischen und Schweizerischen Gesellschaft für Biomedizinische Technik, 6.-9. September 2006, Zürich.
[26] Wallin MK, Wajntraub S. Evaluation of Bluetooth as a replacement for cables in intensive care and surgery. Anesth.Analg. 2004;98:763-7
[27] Tan KS, Hinberg I. Effects of a wireless local area network (LAN) system, a telemetry system, and electrosurgical devices on medical devices in a hospital environment. Biomed.Instrum.Technol. 2000;34:115-8.

sous des valeurs limites en vigueur, ne permettent pas de conclure que les réseaux sans fil constituent une menace pour la santé. Cela s'applique aussi aux enfants et aux adolescents.

Bien que les appareils des réseaux sans fil émettent individuellement un rayonnement relativement faible, des rayonnements plus intenses pourraient apparaître localement à l'avenir pour les raisons suivantes : plus forte densité de points d'accès dans les bureaux, utilisation de points d'accès à proximité des postes de travail (p. ex. appareils utilisés sur la table de travail), utilisation accrue d'ordinateurs portables en réseau sans fil aux postes de travail et en privé, ainsi que l'utilisation de normes avec un débit de données plus élevé, une plus grande portée et des puissances émettrices plus élevées.

En raison de ces évolutions et des lacunes existant encore en matière de connaissances relatives aux conséquences sur la santé publique, il apparaît nécessaire de poursuivre la recherche sur les réseaux sans fil, en particulier dans les domaines suivants :

- détermination et surveillance des expositions liées aux nouvelles technologies des réseaux sans fil (La tendance en la matière va dans le sens de puissances plus élevées nécessitées par une plus grande portée et un débit de données plus élevé. L'attention devrait principalement porter sur les expositions à faible distance, comme celles dues aux ordinateurs portables, aux clés USB Bluetooth, aux PDA, etc. ainsi que sur les expositions combinées.) ;
- effets sur la santé dus à des expositions d'une partie du corps typiques pour les applications liées aux réseaux sans fil (autres que l'exposition de la tête dans le cas des téléphones mobiles) ;
- effets dus à un rayonnement non continu (pulsé) avec des caractéristiques typiques pour les réseaux sans fil ;
- sensibilité des enfants et des adolescents aux rayonnements et effets possibles des réseaux sans fil sur ceux-ci.

Les connaissances actuelles concernant l'utilisation de réseaux sans fil dans les hôpitaux sont par trop lacunaires. Si l'on utilise des réseaux sans fil dans les hôpitaux, le fonctionnement des appareils médicaux utilisés dans les zones de diffusion ainsi que la fiabilité des liaisons radio doivent être testés rigoureusement dans chaque cas. La plupart des études ayant porté sur la compatibilité électromagnétique des dispositifs médicaux ont été réalisées avec des réseaux WLAN de la norme b ou g. Il faudrait également procéder à des études réalisées avec des réseaux WLAN fonctionnant dans le domaine des 5 GHz, ceux-ci étant également de plus en plus utilisés. Ces aspects liés à la sécurité devraient en tout cas primer sur tout avantage lié à l'utilisation de réseaux sans fil.

4. Sécurité des données

4.1 Risques de base

A côté des avantages connus, les technologies sans fil présentent également certains inconvénients, entre autres dans le domaine de la sécurité des données et de l'information. La question de la sécurité de l'information, mais ne faudrait-il pas dire plutôt de l'insécurité de l'information, concerne tous les systèmes de communication. Dans le cas des réseaux sans fil, les problèmes sont cependant accrus en comparaison de ceux des réseaux filaires. Prenons l'exemple de l'interception de données Internet. Lorsqu'on est connecté à Internet par câble, un cercle déterminé de personnes peut surveiller la transmission de données, par exemple le personnel technique des prestataires de service et d'autres opérateurs de réseau sur la voie de transmission, des criminels ayant un accès physique à l'infrastructure du réseau et les autorités de poursuite pénale nationales et internationales. Cela constitue certes un cercle restreint de personnes pratiquant une écoute clandestine, mais il serait tout de même préférable d'éviter que lesdites personnes puissent avoir accès à des données sensibles, comme celles liées à l'e-banking. Lorsque la connexion à Internet s'effectue par un réseau WLAN, il existe un risque accru que les liaisons soient surveillées. Dans ce cas, le cercle des espions s'élargit en effet à toutes les personnes se trouvant à portée du réseau WLAN (éventuellement à une distance de plusieurs centaines de mètres). L'accès Internet sans fil est, en ce sens, moins sûr que l'accès filaire. Dans les deux cas, il est cependant judicieux de protéger les données sensibles devant passer par Internet.

Le danger accru lié aux réseaux sans fil résulte du fait que la dispersion des signaux radio ne peut pas être limitée comme on le souhaiterait. Dans de nombreux cas, il est même souhaitable de disperser le plus possible le signal radio. Celui-ci peut être capté et transformé par un pirate. Un pirate peut également introduire à son usage des signaux radio dans le réseau. En utilisant des dispositifs spéciaux on peut également attaquer à des distances qui sont nettement supérieures à la portée usuelle du système attaqué.

4.2 Sécurité de l'information

La question de la sécurité des informations est souvent subdivisée en quatre thèmes : confidentialité, authentification, intégrité, disponibilité. Dans le cas des réseaux sans fil, toutes ces questions se posent de manière accrue. Ces aspects sont traités plus en détails ci-dessous.

Confidentialité

Par confidentialité des informations, on entend le fait que les informations ne puissent pas être interceptées ou surveillées par des personnes non autorisées. Elle est particulièrement importante lors de la transmission de données protégées comme celles de l'e-banking. Dans ce domaine, le fait que l'agression (l'action d'enregistrer) soit en général passive, et qu'elle ne puisse donc pas être découverte directement, constitue un problème particulier. Quelques exemples de non respect de la confidentialité dans le cas des systèmes sans fil :

- une conversation téléphonique effectuée avec un appareil sur lequel aucun cryptage n'est installé est enregistrée, traitée et écoutée par un pirate du voisinage ;
- les signaux d'un clavier PC sans fil sont enregistrés par un pirate et les frappes sont décodées (« keystroke logging ») permettant ainsi la reconstitution du travail effectué sur le PC, la découverte de mots de passes, etc. ;
- une société construit un réseau local sans fil (WLAN) dans ses locaux. Un pirate positionné sur un parking situé à proximité peut surveiller les transmissions effectuées sur ce réseau au moyen d'un ordinateur portable équipé de manière appropriée, même si les mécanismes de sécurité (p. ex. cryptage WEP, filtres MAC) usuels inhérents au point d'accès sont activés. Les applications de piratage nécessaires à cet effet sont disponibles librement sur Internet.

Authentification

L'authentification doit confirmer l'identité des instances en communication et autorisées à l'être et rendre impossible la communication aux non autorisés. Elle peut être utilisée à diverses fins, par exemple pour l'utilisation d'un réseau, l'utilisation d'une application, l'accès à des données. Lorsque le mécanisme d'authentification présente des lacunes de sécurité, un pirate peut accéder à des ressources bien qu'il n'ait pas l'autorisation de le faire. Exemples de défaillance de l'authentification :

- par l'écoute informatique d'un réseau WLAN et l'introduction ciblée de certaines fausses notifications, un pirate peut prendre à son compte l'identité d'un utilisateur autorisé et agir avec ses droits dans le réseau ;
- dans la zone couverte par un réseau WLAN, un pirate peut installer un point d'accès étranger émettant un signal amplifié afin de diriger les liaisons sur lui et d'obtenir ainsi les données d'authentification des utilisateurs ;
- dans le cas d'un réseau Bluetooth, c'est l'appareil qui est authentifié et non l'utilisateur. Lorsqu'un appareil tombe entre les mains d'un pirate, celui-ci jouit des mêmes droits dans le réseau que le propriétaire de l'appareil.

Intégrité

Par intégrité, on entend la confirmation que les données ne sont pas altérées durant la transmission et qu'elles arrivent intégralement à destination. Cela peut être important pour diverses raisons, par exemple dans le cas d'un contrat pour des raisons juridiques ou dans le cas de données scientifiques pour des raisons scientifiques. Les technologies sans fil sont vulnérables à de telles attaques par le fait qu'elles facilitent l'enregistrement de données vraies interceptées et l'introduction de données modifiées. Exemples de violation de l'intégrité :

- Bluetooth : la garantie de l'intégrité protège contre les perturbations aléatoires de données mais pas nécessairement contre une modification volontaire de celles-ci. Un pirate pourrait modifier un flux de données de manière ciblée.
- Une faiblesse analogue se retrouve dans les réseaux WLAN (fonctionnant souvent sous la norme IEEE 802.11) ; elle permet également la modification volontaire des données transmises.

Disponibilité

Par disponibilité, on entend le fait que des réseaux sont en exploitation, que des services sont accessibles, que des données sont disponibles, etc. Les dangers liés à la disponibilité sont les pannes techniques, les catastrophes naturelles ou les catastrophes de civilisation ainsi que les « attaques de déni de service » (en anglais « Denial of Service », abrégé en DoS). Exemples de non disponibilité :

- dans une prison, les autorités pénitentiaires installent un émetteur de brouillage afin de parasiter la réception dans les locaux et d'empêcher ainsi que les prisonniers puissent communiquer avec le monde extérieur ;
- un appareil Bluetooth (p. ex. un mini-ordinateur) est interrogé en permanence (l'appareil attaquant demande des données ou simplement d'être relié) jusqu'à ce que sa batterie soit déchargée, ce qui entraîne une indisponibilité de l'appareil et l'impossibilité pour l'utilisateur de se relier au réseau ;
- les inondations provoquent des coupures de courant à grande échelle. Après quelques heures, les alimentations électriques de secours de la plupart des stations de base pour téléphonie mobile ou des stations de base WiMAX, situées dans la zone sinistrée, sont épuisées et les services de télécommunication correspondants ne fonctionnent plus que de manière très lacunaire.

4.3 Autres problèmes

Dans le présent paragraphe sont décrits quelques problèmes n'entrant pas dans le cadre spécifique de la sécurité de l'information.

Parasitages

De nombreux systèmes sans fil utilisent la bande ISM (Industrial, Scientific and Medical) des 2,4 GHz. Cette bande de fréquence est un domaine du spectre, ouvert à tous, pouvant donc être utilisé librement. Il existe simplement une réglementation concernant la puissance d'émission, valable pour tous les systèmes dans ladite bande. L'absence d'un régime de concession radio a contribué de manière essentielle au succès des réseaux sans fil comme WLAN et Bluetooth. Cette liberté implique cependant un inconvénient majeur, de nombreux systèmes partageant le même domaine de fréquence sans aucune coordination des fréquences. Cela ne concerne pas uniquement les réseaux de communication mais également d'autres appareils comme les fours à micro-ondes. Il en résulte un parasitage réciproque des réseaux de communication ainsi que la perturbation de ceux-ci par d'autres appareils. De telles interférences peuvent conduire à une réduction du débit ou même à des pertes de données.

Vol d'appareils portables

Les ordinateurs portables et les PDA sont souvent utilisés en liaison avec les réseaux sans fil et en public. De tels appareils high-tech sont très recherchés par les voleurs, le vol d'un tel appareil provoquant généralement plus de dommages que la seule perte de l'appareil. Toutes les données enregistrées sur celui-ci sont en effet perdues et peuvent être consultées si elles ne sont pas cryptées. Des informations concernant la perte de données d'affaires sensibles en raison du vol d'un ordinateur portable paraissent souvent dans les médias. D'autres conséquences sont à craindre lorsque l'utilisateur a enregistré des mots de passe sur l'appareil. Lorsqu'une personne non autorisée trouve de tels mots de passe, de nouvelles portes s'ouvrent à elle : elle peut en effet se connecter, par exemple, à un réseau d'entreprise avec tous les droits d'un utilisateur autorisé.

Lorsqu'on utilise un appareil portable en public, on s'expose à des attaques très faciles. En observant l'utilisateur, on peut en effet noter des données importantes, par exemple le processus de connexion à l'appareil ou au réseau, identification de l'utilisateur et mots de passe compris.

Les appareils portables peuvent offrir une entrée dans un réseau d'entreprise contournant les mécanismes de sécurité usuels du réseau. L'appareil peut, par exemple, être infecté par un virus sur le réseau public et ultérieurement faire entrer le virus dans le réseau de l'entreprise après connexion à celui-ci.

Resquilleurs

Les resquilleurs ont la vie facile dans les réseaux sans fil non sécurisés. Un réseau local sans fil sur lequel les mécanismes de sécurité ne sont pas activés est ouvert, dans sa zone de diffusion, à tout utilisateur, y compris aux non autorisés. Une personne ou une société laissant son réseau WLAN ainsi ouvert peut certes être prémunie contre des conséquences graves comme la perte de données critiques, mais elle peut aussi être confrontée au fait que sa liaison Internet à large bande, payée au prix fort, soit fortement chargée en permanence au point de n'être plus disponible pour ses propres applications.

Cela pourrait s'avérer plus grave encore si les ressources non sécurisées du réseau étaient utilisées à des fins illégales. Par le biais du réseau, l'accès Internet pourrait être utilisé pour télécharger des contenus illégaux comme de la pornographie, des morceaux de musique ou des films ou pourrait être utilisé à des fins de pollupostage (pourriels, spamming), de piratage ou d'attaques par déni de service (DoS). Les conséquences juridiques ne pourraient être exclues pour l'opérateur de réseau.

4.4 Développement ultérieur

Ces dernières années, les réseaux sans fil se sont fortement développés. De nouvelles technologies, en liaison avec les bandes de fréquences libres, ont permis une large diffusion de WLAN et Bluetooth. L'évolution de la technologie se poursuit et de nouveaux systèmes, plus puissants, apparaîtront. Le nombre de réseaux va augmenter. On s'attend également à une augmentation des raccordements sans fil (Wireless Local Loop, WLL ; Broadband Wireless Access, BWA). De plus en plus de personnes couvriront leur besoin de communication au moyen de réseaux sans fil. Parallèlement, les dangers liés à Internet augmentent : on a déjà remarqué une évolution claire vers une professionnalisation de la criminalité liée à Internet. Les victimes ne seront plus seulement soumises à une forme de vandalisme mais devront également s'attendre plus souvent à des dommages financiers. Dans la lutte contre ces dangers, qui concernent non seulement les réseaux sans fil mais également Internet dans son ensemble, toutes les parties concernées – opérateurs de réseaux, prestataires de service et utilisateurs - auront leurs rôles à jouer et leurs intérêts à sauvegarder.

4.5 Résumé et mesures à prendre

Les réseaux sans fil offrent des possibilités de communication pratiques et flexibles. Ils présentent cependant des dangers pour la sécurité de l'information. Ces dangers existent aussi dans le cas des réseaux filaires mais sont accentués dans celui des réseaux sans fil. Les utilisateurs comme les opérateurs de réseaux devraient par conséquent prendre des mesures appropriées pour protéger leurs données.

La première mesure, qui est en même temps une condition pour toutes les autres, vise à rendre toutes les parties concernées, mais particulièrement les utilisateurs, plus ouvertes aux questions de la sécurité de l'information. Ce n'est que lorsque les dangers sont reconnus que l'on est en mesure de prendre des dispositions adéquates. Un bon comportement des utilisateurs constitue déjà un pas important en direction de la sécurité de l'information. Les mesures techniques n'ont vraiment de sens que fondées sur ces principes.

Les utilisateurs disposent de diverses possibilités pour agir activement et de manière préventive. Les terminaux devraient être protégés par des mesures de sécurité appropriées. Pour les ordinateurs portables, cela signifie, par exemple, l'installation d'un antivirus et d'un antiespiogiciel, d'un pare-feu, etc. Les données sensibles ne sont pas uniquement en danger durant leur transmission. Elles peuvent également être menacées sur un support de mémoire (p. ex. serveur, PC, clé de mémoire). Les piratages et les tentatives de piratage, sont à l'ordre du jour des divisions informatiques. Les données enregistrées sur des appareils portables comme des ordinateurs ou des PDA sont, en cas de vol, perdues en même temps que l'appareil. C'est la raison pour laquelle il est recommandé d'enregistrer les données sensibles de manière cryptée.

Les utilisateurs de réseaux, que ce soient les personnes privées disposant de petits réseaux ou de grandes sociétés disposant de réseaux nationaux, devraient impérativement utiliser les mécanismes de sécurité existants offerts par le système sans fil correspondant. Certes, ces mécanismes peuvent présenter des lacunes, mais il vaudra toujours mieux être partiellement protégé que pas du tout. Les mesures les plus appropriées sont différentes selon les cas. Quelques mesures simples concernant les personnes privées sont décrites au paragraphe 6.2. La sécurisation de la liaison radio n'élimine cependant pas les autres lacunes sécuritaires de l'ensemble du système ; elle ne résout pas le problème de la sécurité.

Lors de la transmission de données sensibles, celles-ci doivent être impérativement protégées durant tout le processus. A cet effet, la transmission d'importantes données d'affaires implique souvent l'utilisation de solutions hautement sophistiquées. Les réseaux privés virtuels VPN (pour Virtual Private

Network), utilisés par les collaborateurs d'une entreprise pour se connecter, depuis l'extérieur, via Internet, au réseau d'entreprise et les systèmes de l'e-banking, qui permettent de protéger les données bancaires des clients sur le chemin du PC au serveur de la banque, en constituent des exemples connus. De tels systèmes sont appelés des systèmes « end-to-end ». Ces solutions offrent une authentification sûre et un cryptage robuste sur l'ensemble de la voie de transmission, indépendamment de la technologie utilisée lors des diverses étapes de celle-ci.

5. Règlement juridique

5.1 Généralités

Les aspects de la télécommunication liés aux réseaux sans fil ainsi que certains aspects liés à la sécurité des données sont réglés principalement par la loi sur les télécommunications et les ordonnances associées. Cela vaut aussi pour la protection de la santé en liaison avec les appareils faisant partie des réseaux sans fil. La protection de la santé au sens de la limite des immissions de rayonnement provenant d'installations stationnaires est réglée dans la loi sur la protection de l'environnement et, plus spécifiquement, dans l'ordonnance sur la protection contre le rayonnement non ionisant. Dans les paragraphes suivants, cette juridiction est davantage précisée.

Le règlement concernant les réseaux sans fil, en liaison avec l'exposition durant une activité professionnelle ou avec les dispositifs médicaux, n'est pas traité précisément ici, les informations à ce sujet figurant dans le rapport « Rayonnements non ionisants et protection de la santé en Suisse »[1]. Dans le cas des dispositifs médicaux, on ne traitera que l'aspect de la compatibilité électromagnétique, qui est une question particulièrement importante dans le contexte des réseaux sans fil.

La sécurité des données est réglée de manière générale par la loi sur la protection des données[28] et de manière ponctuelle par diverses ordonnances du domaine des télécommunications.

5.2 Télécommunications (protection de la santé publique contre les CEM produits par des appareils de télécommunication)

Loi sur les télécommunications LTC[29]

La loi sur les télécommunications (LTC) règle la transmission d'informations au moyen de techniques de télécommunication. Elle a pour but d'assurer aux particuliers et aux milieux économiques des services de télécommunication variés, avantageux, de qualité et concurrentiels sur le plan national et international.

Les aspects réglementaires suivants concernent les réseaux sans fil :

- régime et octroi de la concession ;
- gestion des fréquences ;
- offre, mise sur le marché et mise en service ainsi qu'installation, exploitation et contrôle des installations de télécommunication ;
- perturbations et compatibilité électromagnétique ;
- protection de la santé et sécurité ;
- secret des télécommunications.

Ces aspects sont réglés plus précisément dans les ordonnances d'application correspondantes liées à la LTC.

Le 24 mars 2006, une loi sur les télécommunications révisée a été adoptée par le Parlement. Cette modification a également pour conséquence le remaniement des ordonnances découlant de ladite loi. Le droit révisé entrera probablement en vigueur le 1er avril 2007. Les modifications concernent les réseaux sans fil uniquement dans le domaine de la concession de services et n'ont aucune incidence sur les aspects des réseaux sans fil examinés dans le cadre du présent rapport.

[28] Loi fédérale du 19 juin 1992 sur la protection des données LPD, RS 235.1
[29] Loi du 30 avril 1997 sur les télécommunications, RS 784.10

Ordonnance sur la gestion des fréquences et les concessions de radiocommunication OGC[30]
Ordonnance sur les services de télécommunication OST[31]

Selon la loi sur les télécommunications[32], toute utilisation du spectre des fréquences requiert une concession. Toutefois, le Conseil fédéral peut prévoir des exceptions lorsque les moyens techniques mis en œuvre pour utiliser les fréquences sont de faible importance[33].

L'ordonnance sur les services de télécommunication règle, entre autres, l'étendue du service de télécommunication, les dérogations au régime de la concession et à l'obligation de notifier, l'utilisation du spectre des fréquences radio, les concessions pour les services de télécommunication ainsi que les droits et devoirs généraux des prestataires de services de télécommunication.

L'exploitation de réseaux sans fil requiert une concession de service[34] et les exploitants sont tenus de la notifier[35] lorsque les réseaux sans fil sont utilisés pour l'exploitation d'un réseau de télécommunication et qu'un prestataire de services offre par leur biais des services de télécommunication (p. ex. transmission de communications vocales, services de transmission de données, etc.) à des tiers (utilisateurs ou autres prestataires de services de télécommunication). Peu importe que le réseau sans fil soit utilisé pour les raccordements sans fil ou pour la mise en réseau d'installations de télécommunication.

Sont exclues du régime de la concession les installations radio utilisées sur certaines fréquences collectives et à une puissance limitée[36]. Pour les réseaux sans fil, l'OFCOM a libéré, dans la bande ISM (Industrial, Scientific and Medical), les domaines de fréquence des 2,4 GHz et des 5 GHz. Cette dérogation au régime de la concession n'est toutefois valable que pour certaines puissances, le régime de la concession entrant à nouveau en vigueur dès que celles-ci sont dépassées. Dans ces bandes de fréquence, il n'existe pas de protection contre les interférences avec d'autres systèmes. La plupart des réseaux sans fil, à l'exception de WiMAX, fonctionnent dans ce domaine libre.

Ordonnance sur les installations de télécommunication OIT[37]

L'offre, la mise sur le marché et la mise en service d'installations de télécommunication est réglée par l'ordonnance sur les installations de télécommunication (OIT), qui reprend la teneur de la directive 1999/5/CE concernant les équipements hertziens et les équipements terminaux de télécommunications et la reconnaissance mutuelle de leur conformité[38].

Par installation de télécommunication, on entend les appareils, les liaisons ou les dispositifs qui sont nécessaires à ou qui sont utilisés pour la transmission d'informations par des techniques de télécommunication. La transmission est réalisée par l'émission ou la réception, par voie électrique, magnétique, optique ou autre voie électromagnétique, d'informations par des liaisons filaires ou radio (entre 9 kHz et 3000 GHz).[39]

Une installation de télécommunication ne peut être mise en place et exploitée que si, au moment où elle a été mise sur le marché, mise en service ou mise en place pour la première fois, elle répondait aux prescriptions en vigueur et si elle a été maintenue dans cet état.[40] Les installations de télécommunication stationnaires doivent en outre répondre, lors de leur exploitation, aux exigences de l'ordonnance sur

[30] Ordonnance du 6 octobre 1997 sur la gestion des fréquences et les concessions de radiocommunication, RS 784.102.1
[31] Ordonnance du 31 octobre 2001 sur les services de télécommunication, RS 784.101.1
[32] Art. 22, al. 1, LTC
[33] Art. 22, al. 3, LTC
[34] Art. 4, al. 1, LTC
[35] Art. 4, al. 2, LTC
[36] Art. 8, al. 1, let. a, OGC
[37] Ordonnance du 14 juin 2002 sur les installations de télécommunication, RS 784.101.2
[38] Directive 1999/5/CE du 9 mars 1999 du Parlement européen et du Conseil concernant les équipements hertziens et les équipements terminaux de télécommunications et la reconnaissance mutuelle de leur conformité
[39] Art. 3, let. c et d, LTC
[40] Art. 32, LTC

la protection contre le rayonnement non ionisant ORNI[41] (stations émettrices pour téléphonie mobile et radiodiffusion).

Par principe, les exigences fondamentales suivantes [42] doivent être respectées :
- la protection de la santé et de la sécurité des utilisateurs et d'autres personnes ;
- la compatibilité électromagnétique ;
- l'utilisation effective du spectre attribué.

Les normes techniques posant, en cas de respect, une présomption de conformité aux exigences fondamentales sont désignées par l'Office fédéral de la communication (BAKOM)[43] selon le modèle européen de la « nouvelle approche globale ». Les normes définissant le respect des valeurs limites pour les CEM, dus à des appareils faisant partie de réseaux sans fil, sont présentées dans le tableau 6.

Concernant les CEM, il s'agit principalement du respect des valeurs limites recommandées au niveau international (cf. chapitre 4). On notera que chaque appareil individuel peut à lui seul atteindre toute la valeur limite.

En matière de protection en rapport avec la compatibilité électromagnétique, les appareils, lorsqu'ils sont utilisés ou exploités conformément à leur usage premier, ne doivent pas parasiter d'autres appareils afin de ne pas entraver la fonctionnalité de ceux-ci. Chaque appareil doit cependant présenter une certaine forme de protection contre les parasitages qui lui soit propre. En rapport avec la protection de la santé, cela est important en particulier pour certains dispositifs médicaux (p. ex. stimulateurs cardiaques).

Les exécutions concernant la protection de la santé contre les CEM à haute fréquence, la compatibilité électromagnétique ainsi que l'utilisation effective du spectre relèvent de l'OFCOM[44], alors que l'Inspection fédérale des installations à courant fort (ESTI) est compétente en matière de sécurité électrique et de protection de la santé qui est liée à celle-ci.[45]

Normes techniques du CENELEC (Comité européen de normalisation électrotechnique)
Les normes CENELEC spécifient les conditions techniques de mesure et de procédure dans lesquelles les aspects fondamentaux de la protection de la santé liés aux CEM provenant de produits doivent être testés. L'organisation européenne de normalisation CENELEC[46] a publié les normes CEM ci-dessous, couvrant également le domaine du rayonnement à haute fréquence, et une norme relative à la compatibilité électromagnétique des produits médicaux (Tableau 6).

[41] RS 814.710
[42] Art. 6, al. 1 en liaison avec l'art. 7, al. 1 et 3, OIT
[43] Normes techniques pour les installations de télécommunication http://www.bakom.admin.ch/org/grundlagen/00563/00575/01142/index.html?lang=de&download=M3wBUQCu/8ulmKDu36WenojQ1NTTjaXZnq
[44] Art. 22, al. 1, OIT
[45] Ordonnance du 7 décembre 1992 sur l'Inspection fédérale des installations à courant fort, RS 734.24
[46] http://www.cenelec.org/Cenelec/Homepage.htm

Tableau 6 *Normes CENELEC réglant les CEM à haute fréquence.*

Norme	Année	Titre
EN 50371	2002	Norme générique pour démontrer la conformité des appareils électriques et électroniques de faible puissance aux restrictions de base concernant l'exposition des personnes aux champs électromagnétiques (10 MHz - 300 GHz) – Grand public
EN 50392	2004	Norme de base pour démontrer la conformité des appareils électriques et électroniques, aux restrictions de base pour l'exposition du corps humain aux champs électromagnétiques (0 Hz - 300 GHz)
EN 50383	2002	Norme de base pour le calcul et la mesure des champs électromagnétiques et TAS associés à l'exposition des personnes provenant des stations de base radio et des stations terminales fixes pour les systèmes de télécommunications sans fil (110 MHz - 40 GHz)
EN 50385	2002	Norme de produit pour démontrer la conformité des stations de base radio et des stations terminales fixes pour les communications sans fil, par rapport aux restrictions de base ou aux niveaux de référence relatifs à l'exposition du public aux champs électromagnétiques (110 MHz - 40 GHz) – Population en général
EN 50400 / EN 50401	2006	Norme de base/produit pour démontrer la conformité des équipements fixes de transmission radio (110 MHz - 40 GHz), destinés à une utilisation dans les réseaux de communication sans fil, aux restrictions de base ou aux niveaux de référence relatives à l'exposition des personnes aux champs électromagnétiques de fréquence radio, lors de leur mise en service

EN 60601-1-2	2001 A1:2006	Appareils électromédicaux -- Partie 1-2 : Exigences générales pour la sécurité de base - Norme collatérale : Compatibilité électromagnétique – Prescriptions et essais

5.3 Protection de l'environnement (protection de la santé publique contre les CEM dus à des installations stationnaires)

Loi sur la protection de l'environnement

Dans la loi sur la protection de l'environnement LPE[47], les rayons non ionisants sont, à côté des pollutions atmosphériques, du bruit, des vibrations, également considérés comme des atteintes à l'environnement devant être limitées de manière à ce qu'elles ne deviennent ni nuisibles ni incommodantes pour l'homme et l'environnement. Le concept de protection comporte deux niveaux :

- Le niveau de la lutte contre les menaces :
  les immissions nuisibles ou incommodantes ne sont pas autorisées et doivent être impérativement réduites. Les seuils de nocivité et d'incommodité doivent être fixés de manière contraignante sous forme de valeurs limites d'immissions par le Conseil fédéral.
- Le niveau de la prévention:
  En plus des principes de la lutte contre les atteintes nuisibles ou incommodantes prouvées, la loi sur la protection de l'environnement énonce le principe de prévention selon lequel il importe, à titre préventif, de limiter les atteintes qui *pourraient* devenir nuisibles ou incommodantes, dans la mesure que permettent l'état de la technique et les conditions d'exploitation, et pour autant que cela soit économiquement supportable. Cela vaut également dans le domaine situé en dessous de la valeur limite d'immissions. Il n'est pas nécessaire qu'une menace concrète ait été prouvée. Le principe de prévention sert à réduire les risques potentiels – en particulier les risques à long terme – qui ne peuvent pas être évalués de façon satisfaisante en raison d'un état des connaissances lacunaire.

Ordonnance sur la protection contre le rayonnement non ionisant (ORNI)

L'ordonnance sur la protection contre le rayonnement non ionisant[48] règle exclusivement la protection contre les champs électromagnétiques (rayons non ionisants du domaine de fréquence allant de 0 Hz jusqu'à 300 GHz). Pour la population en général, des valeurs limites d'immissions ont été définies pour tout le domaine de fréquence évoqué si le corps entier est exposé aux CEM, indépendamment de l'origine de ceux-ci. Elles correspondent aux recommandations de la CIPRNI et doivent garantir la pro-

[47] Loi fédérale du 7 octobre 1983 sur la protection de l'environnement (loi sur la protection de l'environnement, LPE), RS 814.01
[48] Ordonnance du 23 décembre 1999 sur la protection contre le rayonnement non ionisant, RS 814.710 (ORNI)

tection de l'homme contre les effets nuisibles aigus, scientifiquement établis. Les valeurs limites d'immissions doivent être respectées partout où des personnes peuvent séjourner, ne serait-ce qu'un court instant. Elles ne s'appliquent cependant qu'au rayonnement qui agit uniformément sur l'ensemble du corps humain.

Les mesures concrètes visant à réduire les émissions et les compétences dont il est question ne concernent que les installations fixes (p. ex. lignes à haute tension, lignes de contact des chemins de fer et des trams, stations émettrices pour la téléphonie mobile, raccordements sans fils ou radiodiffusion). En concrétisation du principe de prévention on a en outre introduit les valeurs limites de l'installation, plus sévères que les valeurs limites d'immissions. Elles sont fondées sur les possibilités de réduction du rayonnement offertes par la technique et les conditions d'exploitation, qui sont supportables économiquement. Elles sont inférieures aux valeurs limites d'immissions d'un facteur 10 à 300 et sont valables dans les lieux à utilisation sensible (p. ex. appartements, bureaux).

L'exécution des dispositions fédérales relatives au droit environnemental incombe aux cantons dans la mesure où elle n'est pas réservée à la Confédération par la loi. L'exécution relève de la Confédération lorsque les autorités fédérales prennent des décisions au sujet d'installations produisant des RNI (p. ex. pour les installations électriques, les installations de chemins de fer) en application d'autres lois fédérales. Dans les autres cas, la compétence relève des cantons (p. ex. antennes pour la téléphonie mobile, émetteurs radio, radiocommunication à usage professionnel, installations de radioamateurs).

WLAN
Les points d'accès de hotspots publics sont à considérer comme des installations émettrices stationnaires ; ils relèvent donc du champ d'application de l'ORNI.

La valeur limite d'immissions[49] est applicable aussi longtemps que le corps dans son entier est exposé uniformément au rayonnement d'une installation stationnaire. En ce qui concerne les points d'accès WLAN actuels, lorsqu'il s'agit de distances où c'est le cas, les valeurs limites sont toujours respectées.

Lorsqu'on s'approche d'une antenne, comme c'est le cas dans la pratique pour des points d'accès WLAN, l'exposition qui en résulte ne concerne qu'une partie du corps. Dans cette situation, la valeur limite d'immissions de l'ORNI n'est plus applicable ; s'appliquent alors les exigences de l'ordonnance sur les installations de télécommunication (cf. paragraphe 5.2) et la valeur limite de la CIPRNI de 2 W/kg pour les TAS locaux. Cette valeur limite pourrait également être respectée, même à de petites distances. Les fabricants sont responsables du fait que les utilisateurs installant le matériel soient informés au sujet d'éventuelles distances minimales.

Etant donné que la puissance d'émission des points d'accès WLAN se situe au-dessous de 6 W ERP, ceux-ci ne sont pas soumis à une limitation préventive des émissions conformément à l'ORNI[50], c'est-à-dire qu'il n'y a pas de valeur limite de l'installation à respecter. Il semble toutefois que la puissance émettrice maximale des points d'accès dans la bande libre ISM des petits exploitants (y compris les communes) ne soit pas toujours respectée (p. ex. parce que les antennes sont installées avec un gain d'antenne trop élevé). En raison d'un manque de connaissances techniques et d'une expérience lacunaire en matière de rayonnement non ionisant, de tels exploitants de hotspot ne sont sans doute pas conscients du fait que leur comportement, qui peut provoquer des immissions plus élevées, n'est pas légal.

[49] Annexe 2, ch. 11, ORNI
[50] Annexe 1, ch. 61 et 71, ORNI

WiMAX
Les stations de base des réseaux WiMAX sont assujetties à l'ORNI. Elles sont traitées de manière analogue aux stations de base de téléphonie mobile[51]. Pour les stations de base avec une puissance totale d'émission supérieure à 6 W ERP, une demande de permis de construire doit être présentée à la commune compétente et la charge en RNI doit être calculée à l'aide d'une fiche de données spécifique au site. Le permis de construire ne peut être délivré que si la charge en RNI due à l'émetteur respecte la valeur limite de l'installation dans tous les endroits à utilisation sensible (habitations, écoles, zones à bâtir non construites). Pour les installations avec une puissance d'émission ne dépassant pas 6 W ERP, l'autorité peut exiger qu'un formulaire d'annonce soit rempli. Les stations de base ayant, à l'intérieur de la bande de fréquence libre, une puissance émettrice maximale de 1 W ou respectivement de 2 W doivent respecter la valeur limite de l'installation uniquement à partir du moment où plusieurs émetteurs sont installés de manière fixe sur un même site et atteignent à eux tous une puissance d'émission dépassant 6 W ERP.

On ne peut pas donner pour l'instant d'indications sur usages des antenne des utilisateurs nomades , car les configurations techniques concrètes de ces systèmes ne sont pas encore connues.

5.4 Compatibilité électromagnétique des dispositifs médicaux

En Suisse, les dispositifs médicaux sont réglés, comme les installations de télécommunication, selon le modèle européen de la « nouvelle approche globale »; les bases légales figurent dans la loi sur les produits thérapeutiques (LPTh)[52] et dans l'ordonnance sur les dispositifs médicaux (ODim)[53]. Le Conseil fédéral fixe les exigences fondamentales posées aux dispositifs médicaux et l'Institut suisse des produits thérapeutiques (Swissmedic) définit les normes techniques appropriées à la concrétisation de ces exigences[54] - entre autres, les exigences en matière de compatibilité électromagnétique. La norme correspondante figure dans le tableau 6.

Lors du processus de la mise sur le marché d'un dispositif médical et en vertu du modèle de la « nouvelle approche globale », la responsabilité propre des fabricants est fortement mise à contribution. Ils sont en effet non seulement tenus de veiller à ce que les procédures d'évaluation de la conformité soient effectuées correctement et que leurs résultats soient positifs, mais leurs obligations s'étendent aussi à l'ensemble du cycle de vie des dispositifs. Dans ce cadre, l'observation permanente de ceux-ci a une importance particulière. Les fabricants sont en effet tenus d'évaluer leurs dispositifs par rapport aux risques résultant de nouvelles ou de futures technologies, telles que des réseaux sans fil fonctionnant à de nouvelles fréquences par exemple. En cas d'apparition de nouvelles menaces, les dispositifs devront être adaptés aux nouvelles conditions, voire perfectionnés.

Swissmedic a mis en place un système de vigilance dans le but d'augmenter la sécurité : les fabricants de dispositifs médicaux et tous ceux qui mettent ces derniers sur le marché sont tenus de notifier à Swissmedic les évènements graves et les mises en danger qui sont survenus ainsi que les rappels de leurs produits et les autres mesures prises. L'objectif de ce service de notification des incidents (vigilance) est d'empêcher la récidive. L'examen des causes d'un incident et la réalisation de mesures correctives éventuelles incombent au fabricant et au responsable de la mise sur le marché. Ces processus sont surveillés par Swissmedic.

Le service de vigilance devrait avoir repéré et corrigé tout dysfonctionnement de dispositif médical qui aurait été provoqué par un réseau sans fil.

---

[51] voir « Stations de base pour téléphonie mobile et raccordements sans fil (WLL). Recommandation d'exécution de l'ORNI. », OFEV, 2002
[52] Loi fédérale du 15 décembre 2000 sur les médicaments et les dispositifs médicaux (loi sur les produits thérapeutiques, LPTh), RS 812.21
[53] Ordonnance du 17 octobre 2001sur les dispositifs médicaux (ODim, RS 812.213)
[54] Art. 45, al. 3 et 4, LPTh

5.5 Résumé des règlements juridiques

Les plus importantes réglementations existantes concernant divers aspects des réseaux sans fil figurent dans le Tableau 7.

Tableau 7 *Règlements significatifs en rapport avec les réseaux sans fil*[55]

Thème	Arrêté	Remarque
Normes Gestion des fréquences	LTC OGC	La plupart des réseaux sans fil émettent dans la bande libre ISM – sensibles aux interférences
Concessions	LTC OST OGC	La plupart des réseaux sans fil ne sont pas soumis au régime de la concession (exception : WiMAX)
Protection de la santé en liaison avec des dispositifs	OIT	Des valeurs limites relatives à certains produits sont fixées dans des normes internationales sur les produits (Tableau 6)
Protection de la santé en liaison avec des installations stationnaires (concerne WLAN et WiMAX)	LPE ORNI	Valeurs limites d'immissions pour tous les lieux où des personnes peuvent séjourner + valeur limite de l'installation pour les lieux à utilisation sensible
Protection des travailleurs en liaison avec des installations émettrices stationnaires	ORNI	Valeurs limites d'immissions + valeur limite de l'installation pour les bureaux en tant que lieux à utilisation sensible
Protection des travailleurs en liaison avec des dispositifs et des installations en service	LAA	Valeurs limites d'immissions pour les expositions dans l'exercice d'une profession (valeurs VME)
Compatibilité électromagnétique	OCEM ODim	Norme européenne sur les produits relative à la compatibilité électromagnétique des dispositifs médicaux (Tableau 6)
Sécurité des données	LPD LTC OST	Dispositions pénales Secret des télécommunications

5.6 Nécessité de réglementer

Les réseaux sans fil ne présentant pas de menaces pour la santé au vu des connaissances actuelles, il n'est pas nécessaire, d'un point de vue sanitaire, de réglementer davantage les appareils. C'est la raison pour laquelle la multiplication des points d'accès ne doit actuellement pas être limitée. Les points d'accès ayant des puissances émettrices au moins égales à 6 W ERP relèvent en outre de la limitation préventive des émissions de l'ORNI, si bien que la question du respect des valeurs limites de l'installation se pose dans le cas des hotspots les plus puissants.

Selon les connaissances actuelles on ne peut rien affirmer au sujet des effets à long terme exercés sur la santé par le rayonnement à haute fréquence des réseaux sans fil. Pour une meilleure information des consommateurs concernant une utilisation pauvre en immissions de réseaux sans fil, il serait souhaitable d'introduire une déclaration du rayonnement émis par les produits.

Il serait également souhaitable d'introduire une nouvelle réglementation dans les normes internationales sur les produits selon laquelle il ne serait plus possible qu'un appareil puisse à lui seul atteindre la totalité de la valeur limite de la CIPRNI. On garantirait ainsi que la valeur limite ne serait pas dépassée lors de l'utilisation simultanée de plusieurs appareils.

En matière de sécurité des données liée aux réseaux sans fil, il existe davantage un besoin de sensibilisation qu'un besoin de réglementation. La Confédération a déjà agi en ce sens par exemple dans le

[55] **LTC** : loi sur les télécommunications, **OGC** : ordonnance sur la gestion des fréquences et les concessions de radiocommunication, **OST** : ordonnance sur les services de télécommunication, **OIT** : ordonnance sur les installations de télécommunication, **LPE** : loi sur la protection de l'environnement, **ORNI** : ordonnance sur la protection contre le rayonnement non ionisant, **LAA** : loi fédérale sur l'assurance-accidents, **VME** : valeurs limites d'exposition aux postes de travail, **OCEM** : ordonnance sur la compatibilité électromagnétique, **ODim** : ordonnance sur les dispositifs médicaux, **LPD** : loi sur la protection des données

cadre de la société de l’information et par la mise en place du service de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information. Des organisations privées sont également actives en matière de sécurité des données comme la société Infosurance, qui s’occupe des besoins des petites et moyennes entreprises.

En ce qui concerne la compatibilité électromagnétique, il n’y a pas de nécessité de réglementation immédiate non plus. On a toutefois constaté que la norme existante, relative à la compatibilité électromagnétique des dispositifs médicaux, ne prend en compte que les fréquences allant jusqu’à 2,5 GHz. Il y aurait lieu définir également des obligations au sujet des fréquences plus élevées, comme celles pouvant être utilisées par des réseaux sans fil.

6. Recommandations sur une utilisation sûre et pauvre en immissions des réseaux sans fil

6.1 Diminution du rayonnement

La charge de rayonnement due aux réseaux actuels est très faible ; elle se situe bien en dessous des valeurs limites en vigueur. Des mesures appropriées permettent de lutter contre les incertitudes concernant les effets à long terme sur la santé, l'utilisation d'appareils de plus en plus puissants ainsi que les technologies s'utilisant tout près du corps. Etant donné que les réseaux sans fil sont utilisés non seulement dans les bureaux mais également dans le cadre privé, les mesures préventives sont pertinentes notamment dans les ménages avec enfants. La charge de rayonnement subie par un individu peut être réduite à titre préventif grâce aux mesures suivantes :

- enclencher le réseau WLAN seulement lorsqu'il est utilisé. Il est en particulier judicieux d'éteindre le réseau WLAN dans le cas des ordinateurs portables car ceux-ci recherchent en permanence un réseau, ce qui provoque un rayonnement inutile et décharge la batterie ;
- utiliser de préférence des oreillettes pour téléphoner avec un PDA ;
- utiliser des oreillettes Bluetooth de la classe de puissance 3, la plus faible, et les éteindre lorsqu'elles ne sont pas utilisées ;
- ne pas tenir l'ordinateur portable près du corps lors d'une liaison WLAN ;
- placer si possible le point d'accès à une distance d'un mètre d'un poste de travail, d'un lieu de séjour ou de places de jeux ou de repos longuement occupés ;
- placer le point d'accès de manière centrale afin que tous les appareils à connecter aient une bonne réception ;
- préférer la norme g à la norme b. Cette norme offre, à cause de la transmission plus efficace des données, une charge de rayonnement réduite ;
- lorsqu'une régulation de la puissance est possible, il y a lieu pour un point d'accès d'optimiser la puissance d'émission en fonction de la zone à couvrir ;
- un émetteur WLAN ne doit être exploité qu'avec une antenne prévue à cet effet par le fabricant. Si une antenne avec gain d'antenne plus élevé est utilisée, la puissance d'émission maximale autorisée peut être dépassée et contrevenir à la loi sur les télécommunications.

6.2 Augmentation de la sécurité des données

Les remarques suivantes sont à considérer comme sources d'informations destinées aux utilisateurs privés. Ces mesures ne constituent qu'une première étape en vue d'une utilisation sûre d'Internet via les réseaux WLAN. La Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI - Melde- und Analysestelle Informationssicherung[56]) donne des informations plus détaillées relatives à la sécurité de l'information, destinées à tout utilisateur – des personnes privées jusqu'aux grandes sociétés.

Mesures concernant les réseaux privés

- Le mot de passe standard relatif à la gestion du point d'accès devrait être modifié.
- La gestion du point d'accès devrait autant que possible être réalisée via un câble, par exemple Ethernet, et la fonction relative à la gestion sans fil devrait être désactivée.
- Les possibilités de télégestion des points d'accès via Internet devraient être désactivées.
- L'identifiant du point d'accès (SSID) devrait être changé et son émission (SSID Broadcast) être désactivée.
- Il faudrait utiliser le cryptage le plus puissant permis par le point d'accès et compatible avec les terminaux (de préférence WPA 2 ou WPA, sinon WEP). Il faudrait utiliser une clé la plus longue possible, respectivement un mot de passe complexe.

[56] http://www.melani.admin.ch

- Si le réseau le permet et si les connaissances nécessaires sont présentes, il faudrait utiliser des adresses IP statiques plutôt que le DHCP (Dynamic Host Configuration Protocol).
- Il faudrait utiliser le filtre MAC afin de limiter l'accès au réseau WLAN à des terminaux donnés du réseau.
- Lorsque la fonction est présente sur le point d'accès et qu'elle ne perturbe pas l'exploitation du réseau, la puissance d'émission devrait être réduite afin de diminuer la portée du WLAN .
- Le réseau WLAN ne devrait être enclenché qu'en cas d'utilisation.

7. Annexe

7.1 Abréviations et définitions

Access point	Voir point d'accès
Ad hoc (réseau)	Voir réseau ad hoc
Attaque DoS	Denial of Service, attaque ayant pour objectif de rendre un ordinateur ou tout un réseau inutilisable
Bande ISM	Industrial Scientific Medical-Band, domaine de fréquence librement accessible
Beacon	Information régulière d'un point d'accès par émission d'un signal
BWA	Broadband Wireless Access
canal, canal de transmission	Intervalle de temps, respectivement de fréquence, réservé à la transmission de données
Carte PC	Unité d'émission/réception WLAN pour un ordinateur personnel
CEM	Champ électromagnétique
CENELEC	Comité Européen de Normalisation Électrotechnique
Champ E	Champ électrique
Champ lointain	Cf. champ proche
Champ proche, champ lointain	Dans le domaine des hautes fréquences, on distingue le champ proche et le champ lointain selon que la distance par rapport à la source est plus petite ou plus grande que la longueur d'onde du rayonnement. Dans le champ lointain, l'intensité de champ électrique est inversement proportionnelle à la distance (1/r), la densité de puissance au carré de la distance ($1/r^2$)
CIPRNI	Commission Internationale de la Protection contre le Rayonnement Non Ionisant
Clé mémoire, clé USB	Petit support de données portable, USB : Universal Serial Bus
Débit de données	Quantité de données transmises par unité de temps
DoS (attaque)	Voir attaque DoS
Dose	Constitue la grandeur physique décrivant le mieux les caractéristiques du rayonnement significatives pour une altération biologique donnée. Par conséquent, les doses significatives pour des effets biologiques et sanitaires donnés sont diverses.
E (champ)	Voir champ E
EIRP	Equivalent isotropically radiated power ou Puissance Isotrope rayonnée équivalente (PIRE) : Produit de la puissance fournie à l'antenne par son gain dans une direction donnée par rapport à une antenne isotrope.
Emission	Rayonnement émis par une source de rayonnement
ERP	Effective Radiated Power ou Puissance apparente rayonnée : Produit de la puissance fournie à l'antenne par son gain dans une direction donnée par rapport à une antenne dipôle.
Esclave	Utilisateur d'un réseau Bluetooth, par opposition au maître
Espiogiciel	Logiciel espionnant le comportant des utilisateurs de PC et transmettant les informations correspondantes
ESTI	Inspection fédérale des installations à courant fort
Ethernet	Technologie de réseau
ETSI	European Telecommunications Normes Institute
Exposition	Constitue le rayonnement (immission) auquel un objet donné (être humain, animal, plante, sol ou bien) est exposé durant un temps déterminé (durée d'exposition). On distingue les expositions du corps entier et les expositions partielles.
Filtre MAC	Medium Access Control Filter, n'autorise que certains exemplaires d'un type d'interface réseau, c'est-à-dire n'accorde l'autorisation d'accès au réseau qu'à certains appareils du réseau
Firewall	Voir pare-feu
Fréquence	Nombre d'oscillations par seconde
HiperLAN	High Performance Radio Local Area Network, norme de transmission de données
Hotspot	Zone locale (p. ex. d'une grande ville, d'un aéroport, d'un hôtel) où un fournisseur d'accès met à disposition un accès sans fil à Internet
ICNIRP	International Commission of Non-Ionizing Radiation Protection
IEEE	Institute of Electrical and Electronics Engineers
Immission	C'est le rayonnement subi en un lieu donné. Les immissions sont généralement inférieures aux émissions, le rayonnement pouvant être atténué entre la source de rayonnement et le lieu de l'immission.
Immunité	Capacité d'un dispositif de fonctionner correctement sous l'influence de signaux électromagnétiques parasites
Infrastructure (mode)	Voir mode infrastructure

Interopérabilité	Capacité d'un dispositif de communiquer valablement, dans des configurations comparables, avec d'autres dispositifs de la même norme dans un réseau
ISM (bande)	Voir bande ISM
IT'IS	Foundation for Research on Information Technologies in Society, Zurich
Kit « mains libres »	Oreillette et micro se connectant à un téléphone portable
LAA	Loi fédérale sur l'assurance-accidents
Largeur de bande	Deux significations : Capacité d'un canal de transmission Domaine de fréquence d'un canal de transmission
LPE	Loi sur la protection de l'environnement
LTC	Loi sur les télécommunications
MAC (filtre)	Voir filtre MAC
Maître	Dispositif prenant la direction des opérations dans un réseau Bluetooth
Master	Voir maître
Mbit/s	Mégabit/seconde, quantité de données transmise par unité de temps
Mode infrastructure	Organisation d'un réseau WLAN via un point d'accès
OCEM	Ordonnance sur la compatibilité électromagnétique
OFCOM	Office fédéral de la communication
OFEV	Office fédéral de l'environnement
OIT	Ordonnance sur les installations de télécommunication
OMBT	Ordonnance sur les matériels électriques à basse tension
ORNI	Ordonnance sur la protection contre le rayonnement non ionisant
OST	Ordonnance sur les services de télécommunication
Pare-feu	Dispositif ou logiciel surveillant et réglant le trafic de données dans le réseau
PDA	Personal Digital Assistant, agenda électronique
Piratage	Accès non autorisé ou connexion à un système informatique d'un tiers
PIRE	puissance isotrope rayonnée équivalente, voir EIRP
Point d'accès	Station de base d'un réseau sans fil WLAN
Réseau ad hoc	Liaison directe entre clients WLAN, sans point d'accès
Serveur	Ordinateur central d'un réseau mettant des ressources (p. ex. l'accès à Internet) et des données à la disposition des stations de travail
Slave	Voir esclave
Spyware	Voir espiogiciel
TAS	Taux d'absorption spécifique, son unité étant le W/kg. La valeur TAS constitue la grandeur physique correspondant à l'absorption de rayonnement à haute fréquence par des tissus biologiques ainsi que la mesure de celle-ci. Elle dépend de la fréquence et de la grandeur du corps exposé.
Télémétrie (système de)	Transmission automatique de résultats de mesure ou de données sur de grandes distances, surveillance à distance
WEP (cryptage)	Wired Equivalent Privacy. WEP est une norme de cryptage des signaux radio dans un réseau sans fil (WLAN).
WiFi	Wireless Fidelity, norme de fabricant pour les réseaux WLAN
WiMAX	Worldwide Interoperability for Microwave Access, norme de fabricant pour les réseaux WMAN
WLAN	Wireless Local Area Network, norme relative à la transmission de données sans fil sur des distances moyennes (p. ex. à la maison)
WLAN (carte)	Système d'émission/réception WLAN intégré dans un dispositif
WMAN	Wireless Metropolitan Area Network, norme relative à la transmission de données sans fil sur de grandes distances (p. ex. une ville)
WPAN	Wireless Personal Area Network, norme relative à la transmission de données sans fil sur de courtes distances (p. ex. au poste de travail)

7.2 Postulat Allemann (04 3594) Réseaux sans fil. Risques potentiels

Texte déposé le 8 octobre 2004

Le Conseil fédéral est chargé d'élaborer un rapport sur les risques potentiels des réseaux sans fil (réseaux locaux sans fil appelés "WLAN", Bluetooth, etc.). Le rapport portera aussi bien sur les réseaux sans fil et points d'accès des bureaux et des ménages que sur les stations Internet publiques (appelées "hotspots"). Il devra notamment mettre en évidence :

- le rayonnement des réseaux sans fil ;
- les conséquences pour la santé publique (notamment les risques encourus par les jeunes enfants) et les mesures envisageables ;
- les effets sur l'environnement ;
- la question de la sécurité des données ;
- la nécessité d'une réglementation relative à la multiplication des points d'accès privés et publics (cf. www.swisshotspots.ch).
- Les résultats seront portés à la connaissance des groupes cibles de manière appropriée.

Développement

De plus en plus de personnes sont séduites par la plus grande mobilité qu'offrent les réseaux sans fil. D'ailleurs, le nombre des points d'accès Internet publics (appelés "hotspots") progresse de manière fulgurante. Mais la technologie sans fil explose aussi bien dans les entreprises que dans les ménages. Elle investit, sans la moindre difficulté, tous les lieux possibles et imaginables : les bureaux, les maisons, les universités, les hôtels, les gares et les aéroports, les trains. Pourtant, alors que les antennes de téléphonie mobile, de radio et de télévision font l'objet de critiques véhémentes et de campagnes d'information sur les risques associés à l'électrosmog, il n'existe aucun débat sérieux ni aucune campagne d'information suffisante sur les dangers potentiels que représente la technologie des réseaux sans fil. En Suisse, autant la volonté est grande d'étendre au maximum les accès Internet à tous les lieux possibles, autant la sensibilisation aux effets néfastes des réseaux sans fil est lacunaire. Cette situation est inacceptable pour les consommateurs qui sont actuellement dans l'impossibilité d'obtenir rapidement des informations objectives sur les avantages et les inconvénients de la technologie sans fil. C'est pourquoi il est essentiel aujourd'hui d'obtenir des renseignements sur les risques potentiels des réseaux sans fil et d'en informer la population.

Prise de position du Conseil fédéral

Le Conseil fédéral estime qu'un rapport sur les risques potentiels des réseaux sans fil s'impose et qu'il est judicieux. Ces réseaux constituent en effet une part importante des nouvelles technologies de l'information. Bientôt, ils seront omniprésents du fait de leur croissance fulgurante. Or leur impact sur la santé et l'environnement n'est pas encore suffisamment étudié, ni évalué. Une étude sur les caractéristiques du rayonnement des réseaux locaux sans fil est en cours, sur mandat de l'Office fédéral de la santé publique. Des recherches nationales et internationales sont actuellement menées pour déterminer les risques sanitaires potentiels que représente le rayonnement électromagnétique des appareils de communication mobile. Il faudra déterminer si les résultats de ces examens peuvent également s'appliquer aux réseaux sans fil. Les mesures qui seront recommandées sur ces bases doivent permettre à la fois une protection élevée de la santé et un développement technologique durable. La protection des données, le besoin d'une réglementation et celui d'informer les consommateurs sont des aspects qu'il convient, en outre, d'analyser. Le rapport doit être rédigé avec la collaboration de tous les offices concernés par la thématique. Ce rapport devrait paraître vers la moitié de l'année 2006.

7.3 Membres du groupe de travail

Nom	Adresse
Burgherr Rolf rolf.burgherr@bakom.admin.ch +41 32 327 5505	OFCOM Planification des fréquences - FM-FP Zukunftstr. 44 2501 Bienne
Fitzpatrick Mark mark.fitzpatrick@bakom.admin.ch +41 32 327 5861	OFCOM Services fixes et service universel - TC-FG Zukunftstr. 44 2501 Bienne
Gruber Stefanie stefanie.gruber@bag.admin.ch +41 31 32 20098	OFSP Division Droit 3003 Berne
Meier Martin martin.meier@bag.admin.ch +41 31 32 35694	OFSP Division Radioprotection 3003 Berne
Moser Mirjana mirjana.moser@bag.admin.ch +41 31 32 29575	OFSP Division Radioprotection 3003 Berne
Reusser Daniel daniel.reusser@swissmedic.ch +41 31 323 09 39	Swissmedic Division Dispositifs médicaux Hallerstr. 7 3009 Berne
Riederer Markus markus.riederer@bakom.admin.ch +41 32 327 5542	OFCOM Planification des fréquences - FM-FP Zukunftstr. 44 2501 Bienne
Ryf Salome salome.ryf@bag.admin.ch +41 31 32 50983	OFSP Division Radioprotection 3003 Berne
Siegenthaler Andreas andreas.siegenthaler@bafu.admin.ch +41 31 32 434 17	OFEV Division Protection de l'air et RNI 3003 Berne