Quels réseaux de communication électronique pour la sécurité intérieure et les services d'importance vitale ?

David Krembel, Vincent Jugé

Quels réseaux de communication électronique pour la sécurité intérieure et les services d'importance vitale ?

Juillet 2012

David KREMBEL
Vincent JUGÉ

Pilote Jean-Pierre DARDAYROL

Avertissement
Ce mémoire ne représente que l'opinion de ses rédacteurs et ne saurait engager la responsabilité des personnes consultées.

Remerciements
Nous tenons à remercier ici toutes les personnes sans qui ce mémoire n'aurait pas pu être possible en particulier notre pilote Jean-Pierre Dardayrol qui nous a conseillé tout au long de l'année. Nous remercions aussi tous nos interlocuteurs qui ont pris le temps de nous rencontrer et de nous faire partager leur expérience et leur point de vue.

Sommaire

Résumé

Pour mener à bien leurs missions régaliennes et pour assurer la continuité économique de la vie de l'Etat, les services liés à la sécurité intérieure (Police, Pompiers, Gendarmerie, urgences…) et les opérateurs d'importance vitale ont besoin de moyens de communication adaptés à la spécificité de leurs besoins, aux situations de crise et d'urgence. Historiquement, ils ont développé séparément des réseaux répondant à leurs besoins spécifiques. À l'heure où les communications numériques introduisent de nouveaux usages mais également des contraintes nouvelles, il convient de repenser ces réseaux : dans quelle mesure doit-on conserver la structure parcellaire d'aujourd'hui ?

Ce mémoire nous invite tout d'abord à nous interroger sur les besoins des forces de sécurité et de secours et des opérateurs d'importance vitale, en les comparant aux besoins et aux offres commerciales actuelles, et en posant deux questions : la question d'économies d'échelles, puis celles des améliorations ou de dégradations du service rendu sur un plan opérationnel, en observant la situation dans d'autres pays du monde, en particulier les États-Unis.

Nous étudions ensuite les avantages attendus d'une mutualisation des réseaux de communication, en prenant en compte plusieurs aspects de cette mutualisation : quelles infrastructures fixes et mobiles, quelles ressources spectrales mutualiser ? Comment et avec qui ?

Enfin, nous nous interrogeons plus spécifiquement sur les problèmes qui s'opposent encore à une mutualisation des réseaux de communication, sur le plan technique comme sur le plan organisationnel ; en particulier, nous nous intéressons aux horizons temporels qui peuvent structurer l'évolution que nous avons envisagée, ainsi que sur l'adéquation aux missions d'un réseau commun à plusieurs acteurs de cette sécurité, tant sur les plans technique qu'opérationnel.

Introduction

Le 6 juillet 2012, Orange a été confronté à une panne gigantesque, qui a affecté ses 27 millions de clients et a énormément fait réagir. Quelques jours plus tard, O_2, second opérateur britannique, est victime à son tour d'une panne de niveau national, deux semaines à peine avant la cérémonie d'ouverture des jeux olympiques de Londres.

Face aux attaques qui se multiplient sur les réseaux de télécommunication publics et face aux défaillances dues à des catastrophes naturelles ou à des erreurs humaines, il convient de s'interroger sur l'utilisation de réseaux de télécommunication par les services vitaux pour la sécurité nationale et sur la gestion de tels réseaux. En effet, la plupart des éléments vitaux pour le fonctionnement d'un État, d'une économie et de la vie sociale sont connectés à internet, et donc peuvent être perturbés : services critiques dans les hôpitaux et les cliniques, réseaux de production et de distribution d'eau et d'électricité, transports, contrôle aérien…

Aux États-Unis, la loi créant un réseau sans fil à très haut débit couvrant l'ensemble du territoire et dédié à la sécurité intérieure, des pompiers aux policiers, a été promulguée le 23 février 2012, tirant les leçons des tempêtes tropicales et des chutes de neige catastrophiques ainsi que des attentats du 11 septembre. Qu'en est-il en Europe ? En France ? Quelle serait la gouvernance de tels réseaux ? Est-il réaliste financièrement et techniquement de développer de telles infrastructures de télécommunication dédiées ? En particulier, faut-il des réseaux dédiés pour l'avenir en termes d'infrastructure ? Quels sont les coûts des réseaux dédiés ? Quels sont les acteurs industriels présents sur ce marché ? Dans quelle mesure ces réseaux seraient-ils dédiés : entièrement ou pour certaines fonctions seulement ? Et, dans un contexte de rareté du spectre de fréquence, faut-il des fréquences dédiées ? Finalement, quelle stratégie adopter par les décideurs ?

Ce mémoire s'intéresse aux réseaux de télécommunication utilisés par les services de sécurité et de secours et par certains opérateurs d'importance vitale (OIV)[1]. Il se concentre sur leurs réseaux de radiocommunication particulièrement adaptés à leurs missions nécessitant une forte mobilité.

Il entend montrer que la notion de réseau dédié tend de plus en plus à s'estomper au profit de réseaux partagés (1). Après un état des lieux des réseaux utilisés actuellement qui met en lumière un bilan contrasté (2), nous examinerons les stratégies possibles d'évolution de ces réseaux, entre réseaux dédiés et réseaux commerciaux ouverts au public (3).

*
* *

[1] Administrations et entreprises indispensables à la continuité de la vie économique de l'État

PREMIERE PARTIE

Des réseaux dédiés, un héritage de l'histoire

Dès l'origine, les moyens de communication électroniques mobiles ont été utilisés par les pouvoirs publics dans des situations de crise, par les forces armées, pour la sécurité publique et dans l'industrie. Les radiocommunications mobiles imposent le déplacement de l'utilisateur avec un poste de radio émetteur-récepteur ou seulement récepteur, et de la source d'énergie nécessaire à son alimentation. L'extension des applications et des conditions d'emploi vont donc être intimement liées aux progrès et aux évolutions technologiques dans les domaines des sources d'énergie, de l'électronique, puis de l'informatique.

Dans cette première partie, nous présentons quelques-unes des grandes étapes de la genèse et du développement des moyens de communication électroniques mobiles employés par les forces de sécurité et de secours et par des opérateurs d'importance vitale.

1.1 Quelques jalons historiques

La genèse des réseaux mobiles de communication électronique se situe au début du 20ème siècle, concomitamment avec le développement de la téléphonie sans fil (T.S.F.).

[redacted]

En 1902, Auguste Ferrié, pionnier français de la T.S.F., parvient à rétablir une liaison avec la Martinique à la suite de l'éruption de la Montagne Pelée qui rompu le câble sous-marin la reliant à la Guadeloupe. Cet événement donna ses lettres de noblesses à la T.S.F. Ferrié suscita l'intérêt du Ministère de la Guerre. Il lui proposa notamment d'équiper les navires de postes de T.S.F., mais dû affronter l'hostilité du Ministère chargé du budget, en raison de l'importance des dépenses (voir encadrés ci-dessous).

[redacted]

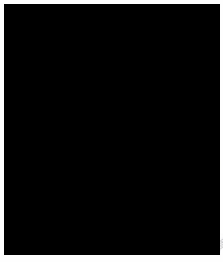
À la même époque, la criminalité augmente dans des proportions d'autant plus inquiétantes qu'une délinquance nouvelle est née qui s'appuie, elle, sur le progrès technique et fait échec à une police archaïque dont les méthodes et le matériel n'ont guère évolué depuis Vidocq. Les forces de sécurité se déplaçaient à pied, à cheval ou à bicyclette. Un chiffre est plus éloquent que tout : au cours de l'année 1906, 103 000 affaires criminelles et correctionnelles ont été classées sans que les auteurs aient pu être identifiés. L'année 1907 s'annonce pire encore. Il y va de la sécurité des villes et des campagnes.

Ces véhicules furent équipés de postes de T.S.F., préfigurant les réseaux modernes de communication utilisés par la Police. La Société française radio-électrique (couramment désignée et promue sous le sigle SFR), fondée en 1910 par Émile Girardeau, était une entreprise industrielle dédiée à la fabrication d'appareils d'émission et de réception radioélectrique, notamment de postes de TSF.

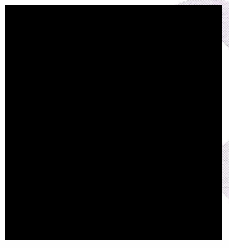
Dès les premiers mois d'activité, les « Mobilards » obtiennent des résultats spectaculaires avec la première arrestation de la « caravane à pépère » (bande d'une centaine de nomades dirigée par Jean Capello). En moins de deux ans, ils totalisent 2 695 arrestations, dont 65 meurtriers, 7 violeurs, 10 faux-monnayeurs, 283 escrocs et 193 cambrioleurs. Les Brigades du Tigre démantèleront, entre autres, la célèbre bande à Bonnot en 1912.

Véhicule des Brigades du Tigre équipé d'un poste de T.S.F.
(Image d'après la série télévisée *Les brigades du tigre* diffusée de 1974 à 1983)

Aux États-Unis, les premières utilisations d'un réseau mobile par les forces de sécurité débutent dans les années 1920. La police de Detroit expérimente un équipement de radio installé à l'arrière de leur véhicule de patrouille, une Ford T. La police de Detroit initia un service régulier à partir d'avril 1928. Il s'agissait de la première liaison mobile en phonie, en modulation d'amplitude (AM) et unidirectionnelle (mode dit « simplex »). Cependant, la réception des signaux était très perturbée lors du passage devant de grands immeubles ou sous les ponts des chemins de fer. Ce système permettait au commissariat de transmettre des alertes et des informations directement aux véhicules des agents équipés d'une radio.



Dès 1934, les liaisons bidirectionnelles (mode dit « semi-duplex ») devinrent d'usage courant pour la police. En combinant un émetteur à un récepteur, il fut possible d'établir des liaisons permettant de communiquer entre les véhicules de patrouille et leur commissariat. Cependant, les transmissions pâtissaient toujours d'une qualité de son très médiocre.



La modulation de fréquence (FM) fut inventée en 1935 et l'amélioration de la qualité du son permit de convertir pratiquement tous les postes de la police de la modulation d'amplitude vers la modulation de fréquence aux alentours de 1940.

Gustave Ferrié, pionnier français de la télégraphie sans fil (TSF) et les premières utilisations d'un réseau de communication électronique lors de la catastrophe de la Montagne Pelée (1902)

Le 8 mai 1902, une éruption de la Montagne Pelée détruisit la ville de Saint-Pierre, alors Sous-Préfecture de la Martinique, faisant environ 30 000 morts. « *Le câble sous-marin reliant la Martinique à la Guadeloupe ayant été rompu, l'île sinistrée se trouva isolée de la métropole. Au début de septembre le Capitaine Ferrié (X 1887), pionnier français de la télégraphie sans fil, fut attaché à la seconde mission envoyée par le Ministre des Colonies non seulement pour étudier les phénomènes volcaniques, mais aussi pour veiller à la sécurité de l'île. C'est ainsi que Ferrié reçut mandat de relier la Martinique à la Guadeloupe au moyen de la T. S. F., alors à ses débuts pour les communications à grande distance (environ 480 km).*

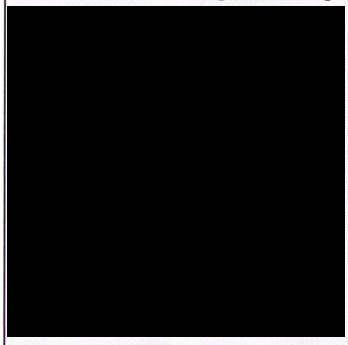
En moins de deux semaines, il réunissait à Bordeaux le personnel et le matériel indispensables et s'embarquait, avec ses deux principaux collaborateurs, l'inspecteur des Postes et Télégraphes Magne et un jeune lieutenant; à peine arrivé, il se hâtait d'installer deux stations de T. S. F., l'une à Beauséjour (Martinique), l'autre à la Verdure (Guadeloupe) et réussissait à passer son premier radiogramme le 4 décembre 1902, moins de trois mois après que la demande du Ministre des Colonies fut parvenue au Service de la Télégraphie militaire (12 Septembre 1902). Ce service radiotélégraphique improvisé put ensuite fonctionner sans interruption jusqu'au complet rétablissement du câble sous-marin (fin 1903). L'installation terminée, Ferrié, qui s'était surmené, rentrait en France légèrement éprouvé par le climat tropical, mais ayant donné une preuve éclatante des services que pouvait déjà rendre la T. S. F. quand les autres procédés de télégraphie étaient inutilisables ».

Source : Institut de France, Académie des Sciences, Notices et discours, Tome second 1937-1948 Paris Gauthier-Villars – Notice sur la vie et les travaux de GUSTAVE FERRIE présentée en la séance du 31 mai 1937 par M. Jean TILHO Membre de l'académie des sciences

Le combat administratif de la Marine nationale pour équiper 130 de ses navires d'un poste TSF

Comme le relate Olivier X, surnommé Olivier le Tigre, parisien, haut fonctionnaire au ministère de l'Intérieur et au cabinet de la Présidence du Conseil, le ministère du Budget ne voit pas d'un très bon œil les nouveaux projets de Gustave Ferrié :

" Diable ! Il faut soutenir Ferrié. Le ministère des Finances va le manger tout cru ! ". La consigne de Clemenceau est claire. Je dois voler au secours du capitaine Ferrié, pionnier français de la Télégraphie Sans Fil.
De quoi est-il coupable pour le ministère en charge des deniers publics ? Il propose des projets de plus en plus coûteux, dont l'intérêt militaire ne saute pas aux yeux des bureaucrates de la rue de Rivoli.
Ferrié a compris depuis longtemps que la force des armées modernes, en cas de conflit important, repose sur leur capacité de coordination. Il faut que l'État-major sache à tout moment où se situent ses unités et que les mouvements des régiments des différentes armes soient coordonnés.
Pour cela, Ferrié propose ni plus ni moins d'utiliser la Tour Eiffel comme antenne gigantesque pour transmettre sur une longue distance des ondes vers des appareils de réception détenus par des unités militaires à des centaines de kilomètres plus loin.
Si M. Eiffel est ravi de ces expériences – ainsi sa Tour ne sera pas démontée – le ministère des Finances n'apprécie guère ces dépenses engagées sur des démarches imprécises, aux coûts exponentiels.
Lorsque je rencontre Ferrié, j'ai le plaisir de discuter avec un passionné. Il me raconte, par le menu, le combat administratif qu'a déjà dû engager la Marine nationale pour que 130 de ses navires soient équipés d'un poste TSF avec le brevet de M. Marconi. Seuls des navires pouvaient embarquer l'électronique volumineuse et les sources d'énergie nécessaires. La rue de Rivoli ne voulait rien entendre non plus sur ce sujet jusqu'à ce qu'elle découvre que si l'un des navires sombrait (par exemple lors des manœuvres dangereuses au nord de Terre Neuve), il serait bon que d'autres bâtiments puissent se dérouter pour venir porter secours aux naufragés.
Je prends en main moi-même la nouvelle négociation avec les Finances. Ferrié a fini par se fâcher, la négociation avec l'armée est au point mort ; je suis donc le seul, comme représentant du Président du Conseil, à pouvoir prendre le relais.
Pour convaincre le sous-directeur qui bloque depuis longtemps le dossier, je me rappelle soudain qu'il aime beaucoup la musique classique et qu'il est plus original qu'il ne veut bien le laisser paraître.
Je n'axe donc pas mon argumentation sur le rapport coût/efficacité comme il s'y attend mais ... sur le rêve.
Comme on conte une belle histoire, je lui parle de l'expérience de radiotéléphonie qui s'est déroulée la veille de Noël 1906 : un opérateur radio TSF, embarqué à bord d'un navire en mer des Caraïbes a pu entendre sur son poste un poème, puis le chant d'une femme et enfin un solo de violon. Cette expérience menée par Fessenden a fait grand bruit outre-Atlantique.



" Un solo de violon, au milieu de l'Atlantique ? " s'écrie, ravi, mon sous-directeur du budget, " ... mais c'est merveilleux votre truc ! ". Son regard n'est plus à ce moment celui d'un fonctionnaire revêche mais celui d'un gosse qui contemple un jouet en bois dont il rêve depuis des mois.
La partie est gagnée. Les financements tant attendus par l'armée arrivent. Notre marine et notre armée de terre auront tous les postes TSF qu'elles veulent.

Ne le répétez pas : j'ai promis au sous-directeur de la rue de Rivoli que les postes TSF diffuseraient chaque soir aux militaires, si cela est techniquement possible ... un solo de violon.

Source : 15 avril 1908 : la TSF et le bureaucrate, d'après un site frère d'Il y un siècle publié sur la plate-forme du Monde.fr

Du côté des opérateurs d'importance vitale, par exemple des exploitants de réseaux électriques, il y a également la recherche de moyens rapides et fiables permettant de communiquer avec les équipes intervenant sur les installations. Il s'agit d'améliorer la qualité et de réduire les temps de coupure de la clientèle.

En 1923, Eugène Meyer alors directeur de l'électricité de Strasbourg résume ainsi l'attente des exploitants :

« Tout entrepreneur d'une affaire de production, de transport ou de distribution d'énergie électrique s'est trouvé fréquemment aux prises avec la question des moyens de communication indispensables pour donner, rapidement et à n'importe quel moment, de jour ou de nuit, les ordres nécessaires en vue d'assurer la bonne marche de ses services : vérification des lignes, recherche d'un défaut, réparation d'un accident, etc. Ce problème de moyens de communication rapides et efficaces a depuis longtemps attiré l'attention des exploitants et des constructeurs [...]. Le développement extraordinaire que prennent chaque jours la production, le transport et la distribution de l'énergie électrique, l'obligation de correspondre rapidement avec les postes de transformation ou de sectionnement reliés d'autre part entre eux par des lignes à haute tension et la nécessité de plus en plus grande d'une interconnexion entre grandes centrales situées à des distances considérables les unes des autres, ont donné à cette question une importance considérable et ont mis les chercheurs devant des problèmes à résoudre chaque jour plus complexes. L'interconnexion des réseaux, en effet, amène avec elle une série de tâches nouvelles, telles que le réglage de la tension, la répartition de la charge sur les centrales, le réglage du facteur de puissance, etc., qui ne peuvent être réalisées de façon satisfaisante que lorsqu'on dispose de moyens sûrs de communication entre les différentes parties des réseaux. Les principales qualités demandées à ces moyens de communication sont : une marche parfaite du point de vue transmission des ordres et de sécurité du personnel, une absolue régularité et des conditions économiques d'installation, d'entretien et de service »[2].

La T.S.F. trouve des adeptes dans la profession et certains militent même, pour demander une gamme d'ondes réservée aux producteurs d'énergie électrique. En effet, ce moyen s'adapte bien à des configurations spécifiques de réseaux électriques tels que celui de grandes villes et de leurs banlieues. Une compagnie lyonnaise, la compagnie du Gaz de Lyon, expérimente un système de radiocommunication conçu par ses propres ingénieurs, pour relier par ondes hertziennes son siège social à ses différentes installations : centrales électriques et postes de coupure, implantés dans la ville et les agglomérations spécifiques.
Mais dès 1923, on parle déjà de saturation du spectre de fréquence du fait de la demande toujours croissante de ce moyen de communication et de l'étroitesse de la bande de fréquence alors réservée en France à cet usage. De plus, cette technique présente un autre inconvénient, majeur pour les professionnels de la distribution d'énergie électrique de l'époque : elle ne permet pas le secret des échanges car n'importe quel amateur équipé de poste récepteur peut écouter et suivre les conversations. De fait, et en l'absence de réseau téléphonique public adapté, les sociétés d'électricité ont alors cherché à établir des liaisons téléphoniques qui leur soient propres, réservées à leur usage, donc disponibles à tout instant.
La seconde guerre mondiale interrompt complètement les expérimentations dans le domaine des radiocommunications.

À la création d'EDF en 1946, les priorités de l'Entreprise ne concernent pas la radiotéléphonie, mais des exploitants reprennent les idées de l'avant-guerre et des utilisations de liaisons radio

[2] Source :E.-O. Meyer, « Les moyens de communication des entreprises électriques », Rapport de la Conférence internationale des grands réseaux électriques (CIGRE),1923

apparaissent. À compter des années 1950 des initiatives pour la mise en place de réseaux se multiplient. Les postes mobiles sont encore encombrants, fragiles, et leur emploi ne suscite pas l'enthousiasme des utilisateurs...
À partir des années 1960, les semi-conducteurs apportent des améliorations en poids, volume et performances et une décennie plus tard, le développement des filtres, l'apparition des circuits intégrés permettent de faciliter l'utilisation des équipements mobiles. Un raccordement des réseaux radio aux installations téléphoniques est de plus en plus systématique. La radio devient un prolongement du téléphone de l'entreprise. Les réseaux de radio professionnelle mobile (PMR) se développent.

Dès les années 1980, l'informatique et les transmissions de données appliquées aux réseaux radio vont permettre l'établissement de systèmes dits cellulaires. Le projet de réseau radiophonique mobile automatique pour GDF et EDF (RAMAGE) est engagé à cette époque avant son abandon au bout de quelques années (voir § 2.6.3). Avec ce réseau, EDF a lancé l'étude et le développement du premier réseau privé analogique partagé dit « trunk » d'envergure nationale. Cette technologie permet une utilisation optimale du spectre en partageant la ressource entre les utilisateurs du réseau par une gestion dynamique des fréquences.

La fin des années 1980 et le début des années 1990 marquent l'avènement des systèmes numériques de radio mobile professionnelle utilisés de nos jours. La Gendarmerie nationale[3] s'équipe du premier réseau de ce type au monde, le réseau RUBIS. Pour la première fois, le cryptage numérique des communications permet de garantir la sécurité des échanges. Si la voix reste le moyen principal de communication, il devient également possible d'échanger des données en bas débit.

1.2 Bilan : une grande variété de réseaux conçus à partir de technologies spécifiques et la méfiance à l'égard des premiers réseaux mobiles commerciaux

La question de l'utilisation de réseaux radio commerciaux ouverts au public ne se pose pas avant la fin des années 1980, puisqu'il n'existait pas de réseau radio public en France, rappelle EDF[4]. Mais, en 1988, le réseau public Radiocom 2000 se développe et, outre l'offre radiotéléphone, il propose la fourniture de réseaux d'entreprise en groupes fermés d'utilisateurs. Cependant, les organismes auxquels nous nous intéressons sont réticents à son utilisation. La couverture ne correspond pas à leurs besoins, Radiocom 2000 couvrant en priorité les zones urbaines et les grands axes de circulation. Il n'offre pas de priorité en cas d'incident, ni même de saturation du réseau radio. Il y a également une question de principe, parce qu'ils hésitent à être tributaires d'un tiers pour leur exploitation.
Radiocom 2000 est un réseau analogique qui permet à France Telecom de prendre date auprès de la clientèle en attendant la génération radio suivante (le GSM). Selon EDF, France Telecom ne souhaitait pas accueillir un nombre important de mobiles d'entreprises sur ce réseau.

[3] La Gendarmerie nationale est une force de Police militaire. Elle dépend, comme la Police nationale, du ministère chargé de l'Intérieur
[4] Les télécommunications au cœur du système électrique français, Editions TEC & DOC 2007, p.216

Au siècle dernier, les utilisateurs de radio professionnelle ont donc construit leurs propres réseaux, conçus pour satisfaire à leurs propres exigences. Il en a résulté une grande variété de réseaux, chacun disposant de ses propres fréquences et conçu à partir de technologies spécifiques. Les possibilités de coopération étaient minimales du fait de l'utilisation de technologies spécifiques et non coordonnées. Cet héritage a souvent été lié au fait que les technologies commerciales ne satisfaisaient pas aux besoins des forces de sécurité et que les modes d'attribution des fréquences pour les réseaux à bande étroite ne facilitaient pas la mutualisation, commente un équipementier. Ce problème d'allocation parcellaire a été résolu en Europe grâce à l'accord dit de Schengen en 1996 (voir § 2.4.2) et une des améliorations importantes qui en a résulté dans les années 2000 partout en Europe est le déploiement progressif de réseaux numériques nationaux multi-organisations (donc offrant une interopérabilité native entre police, pompiers et services d'urgences), fonctionnant en bande étroite. Ces réseaux spécifiques utilisés par les forces de sécurité et de secours sont encore appelés systèmes de radiocommunication de protection du public et de secours en cas de catastrophe (PPDR, Public protection and disaster relief, ou PSS, public safety and security).

Parallèlement, à partir des années 1990 et de l'adoption de la norme de téléphonie mobile GSM de (deuxième génération ou 2G) en Europe par les opérateurs commerciaux, les réseaux radio commerciaux ouverts au public ont connu une succession d'évolutions technologiques caractérisées par plusieurs autres changements générationnels : la technologie UMTS (3G) vers 2005 et à partir de 2012, le déploiement de réseaux de 4ème génération avec une technologie telle que la norme Long Term Evolution (LTE) permettant l'échange de données numériques à très haut débit, une durée d'établissement des communications très courte et une interopérabilité native.

Génération	2G	2,5G	2,75G	3G	3G+	4G
Technologie	GSM	GPRS	EDGE	UMTS	HSDPA	LTE
Année	1990	2001		2005	2007	2012

Aujourd'hui, dans un environnement des radiocommunications en pleine mutation, la question se pose de plus en plus de savoir dans quelle mesure il serait possible de recourir aux nouvelles technologies utilisées par les réseaux commerciaux ouverts au public, voire même d'emprunter ces réseaux, afin de satisfaire aux exigences spécifiques des forces de sécurité et de secours ainsi qu'aux opérateurs d'importance vitale, traditionnellement attachés à des réseaux dédiés.

DEUXIEME PARTIE : État des lieux

Dans cette partie, nous présentons les objectifs généraux et spécifiques ainsi que le fonctionnement des réseaux de communication mobiles utilisés par les forces de sécurité et de secours et par les opérateurs d'importance vitale.

2.1 Moyens de communication des services de sécurité et de secours

Les systèmes de radiocommunication de protection du public et de secours en cas de catastrophe visent à atteindre des objectifs généraux, techniques et d'exploitation qui ont été spécifiés par l'Union internationale des télécommunications (UIT)[5].

Les objectifs généraux de ces réseaux visent à maintenir l'ordre public, à répondre aux situations d'urgence et protéger les vies humaines et les biens matériels et à répondre aux situations de catastrophe exigeant l'organisation de secours. Ces services doivent pouvoir être disponibles dans un vaste éventail de zones géographiques, notamment en milieu urbain, suburbain, rural et isolé, alors que les réseaux commerciaux ouverts au public ne couvrent que les zones les plus densément habitées. Ces réseaux doivent prendre en charge l'interopérabilité et l'interfonctionnement des réseaux, pour une exploitation tant nationale que transfrontière, dans les situations d'urgence et afin d'organiser les secours en cas de catastrophe. Ils doivent permettre de faire un usage rationnel et économique du spectre radioélectrique, compatible avec la fourniture de services à un coût acceptable, et autoriser le fonctionnement d'un vaste éventail de terminaux mobiles depuis ceux qui sont suffisamment petits pour être portés sur soi, jusqu'aux terminaux installés sur des véhicules. Enfin, il y a lieu d'assurer la possibilité d'établir des radiocommunications de PPDR à des coûts raisonnables sur tous les marchés.

Au plan technique, les systèmes conçus pour les applications de PPDR visent à assurer l'intégration des transmissions de la voix, des données et des images; ils doivent assurer les niveaux supplémentaires de sécurité associés au type d'information acheminé par les canaux de télécommunications liés aux diverses applications et activités de PPDR et prendre en charge des équipements fonctionnant dans des conditions d'exploitation extrêmes variées (mauvaises routes, poussière, température extrême, atmosphères explosives) ; ces moyens doivent autoriser l'utilisation de répéteurs afin de couvrir des distances importantes entre terminaux et stations de base dans les zones rurales et les zones isolées, ainsi que dans les zones localisées d'opérations intenses sur place ; ils doivent assurer un établissement rapide des communications, l'émission d'appel abrégée (en mémoire), et enfin, les appels de groupe.

Les objectifs d'exploitation visent à garantir la sécurité notamment par le cryptage de bout en bout, et l'authentification des terminaux/réseaux; ils doivent permettre une gestion des télécommunications dirigée par les organismes et les organisations de PPDR, grâce à des dispositions telles que la reconfiguration instantanée/dynamique, la constitution de groupes de conversation (ou conférences), la garantie d'accès, notamment les appels prioritaires et la préemption d'appel, les appels de groupe ou les appels généraux, la disponibilité des ressources spectrales pour plusieurs organismes et organisations de PPDR, la coordination et le reroutage; l'exploitation de ces moyens doit permettre d'acheminer les télécommunications par le système/réseau et/ou indépendantes du réseau, notamment par une exploitation en mode direct (DMO, direct mode operation), en simplex et avec actionnement d'un bouton poussoir d'émission-

[5] Objectifs et spécifications des systèmes de radiocommunication de protection du public et de secours en cas de catastrophe, RAPPORT UIT-R M.2033 (2003)

réception ; elle doit permettre d'assurer une couverture individualisée et fiable, en particulier dans les espaces intérieurs, tels que les zones souterraines et inaccessibles. Prévoir en outre la possibilité d'étendre la taille des cellules ou la capacité dans les zones rurales et isolées, ou encore dans des conditions difficiles lors de situations d'urgence ou en cas de catastrophe ; une continuité de service intégrale doit être garantie par des mesures telles que la redondance pour les opérations en situation d'urgence, l'augmentation rapide de capacité, afin de surmonter les pertes partielles d'infrastructures essentielles à l'accomplissement effectif des missions, comme à la sécurité des personnels de PPDR ; une qualité de service élevée doit être assurée, notamment par l'établissement instantané des appels et le fonctionnement immédiat par poussoir émission-réception, la tolérance aux charges extrêmes, des taux très élevés d'établissement d'appels réussis, etc., et la prise en charge de différentes applications de PPDR.

2.2 Moyens de communication des opérateurs d'importance vitale

Les objectifs des moyens de communication des opérateurs d'importance vitale partagent de nombreuses similarités avec celles des forces de sécurité. Cependant, ces réseaux ont des besoins fonctionnels complexes et sensibles faisant l'objet d'exigences très spécifiques liées à la nature même des activités (réseaux de transport et de distribution d'énergie électrique, de gaz, d'eau, réseaux ferroviaires, métros, aéroports,...)

Des exigences spécifiques s'appliquent par exemple aux systèmes de télécommunications utilisés pour faciliter la circulation des trains et améliorer la sécurité :

- Radio sol-train (communication entre conducteurs de train et régulateurs de trafic) ;
- Etablissement de communication sol-train lorsque le train se déplace à grande vitesse ;
- Système de contrôle commande des trains, de signalisation ;
- Numérotation fonctionnelle (appel par numéro de train ou de locomotive) ;
- Alarme de veille automatique par contrôle appui (AVACMA) ;
- Communications et alerte pour les équipes de maintenance des voies ferrées ;
- Interopérabilité au passage des frontières.

L'Union internationale des chemins de fer (UIC) édicte des exigences particulières destinées à garantir la sécurité des transports ferroviaires[6].

Dans le secteur de la production d'électricité, des exigences spécifiques s'appliquent également. L'exploitation de lignes électriques haute tension nécessite, aussi bien pour l'exécution des manœuvres que pour la protection des personnes et des matériels, des moyens de communication sûrs et disponibles en permanence.

Pour assurer la gestion de la production et du transport, les dispatchings ont besoin d'informations issues des postes haute tension, des usines et des centrales, (télémesures et télésignalisations) ainsi que de systèmes de téléréglage (puissance et tension), de dispositifs d'alerte et de sauvegarde du réseau. L'exigence de fiabilité est très grande et nécessite des voies de transmission diversifiées et sans mode commun. Les délais d'établissement des communications sont très courts pour assurer la protection du réseau.

Pour mieux comprendre comment les différents besoins des divers groupes d'utilisateurs et applications sont remplis, il convient d'examiner les structures de base d'un système de radio mobile professionnelle (PMR).

[6] European integrated railway radio enhanced network Functional Requirements Specification Version 7.3.0 (Mars 2012)

Un réseau PMR fonctionne grâce à des ondes radio propagées dans l'air sur une fréquence. Le cas le plus simple est la liaison radio mobile, ou en mode direct, entre deux stations mobiles ou portables, généralement en mode dit simplex (communication dans une seule direction), sur une fréquence porteuse unique f 1. Ces liaisons n'ont qu'une couverture limitée mais elles peuvent être établies rapidement et sont bien adaptés aux tâches réalisées par un petit groupe d'utilisateurs dans une zone locale. Le mode simplex signifie qu'une personne parle alors que le reste du groupe est en écoute. L'état des stations mobiles est commandé par une clé d'émission (PTT) actionnée par la personne qui souhaite prendre la parole. Bien sûr, les zones de couverture de toutes les stations impliquées dans un appel doivent se chevaucher.
Un répéteur (RE) (antenne relais ou station de base) peut être utilisé si une plus grande distance de couverture est nécessaire que ce qui est réalisable dans le mode direct. Les antennes-relais reçoivent et transmettent les communications. De différents types (perches, panneaux…), les antennes sont reliées par des câbles au matériel radio, lui-même contenu dans une armoire ou un local situé près de l'antenne. Perchées en moyenne à une hauteur de 12 à 50 mètres, les antennes utilisent en général des supports tels que les châteaux d'eau, les toits d'immeubles, les pylônes…
Le répéteur doit recevoir les signaux sur une fréquence f 1 et retransmettre chaque message sur une autre fréquence f 2. Ce mode est appelé semi-duplex ou half-duplex (communication dans deux directions mais pas simultanément). Dans de nombreux cas, il y a une station de base centrale avec un commutateur qui contrôle un groupe de terminaux mobiles.
Lorsque plusieurs stations de base sont reliées entre elles, il est possible de constituer un réseau de type cellulaire pour couvrir de vastes zones. La configuration peut être beaucoup plus complexe si les stations de base supplémentaires ou répéteurs appartiennent au réseau, si d'autres réseaux fixes ou mobiles sont présents, si les appels directs entre mobiles sont une exigence, ou si une combinaison de toutes ces exigences est nécessaire. Parfois, des véhicules peuvent également être utilisés temporairement en tant que répéteurs.
Les répéteurs, qui doivent apparaître à tous les mobiles comme la station de base elle-même, peuvent être reliés à la station de base par l'intermédiaire d'un câble métallique ou par une paire de fréquences supplémentaires.

Enfin, dans les grands systèmes avec de nombreux abonnés, une seule paire de fréquence porteuse, à la fois pour les liaisons montantes et descendantes, ne suffit pas pour réaliser l'ensemble du trafic ; par conséquent, des systèmes multicanaux sont construits. Ensuite, le trafic doit être

soigneusement distribué entre les différents canaux pour obtenir une charge équilibrée sur chacun d'eux, qui est la condition nécessaire pour l'utilisation la plus efficace du système. Cela nécessite un protocole sophistiqué automatique pour servir tous les utilisateurs rapidement et avec un minimum d'interférence, de temps d'attente, et d'appels manqués ou de blocage.
Pour éviter les interférences entre les différents signaux des stations de base à des mobiles, les stations de base doivent utiliser des fréquences porteuses différentes. Ainsi, les assignations de fréquence dans les systèmes multi-sites avec de nombreuses chaînes par station de base doivent permettre de minimiser le nombre de fréquences nécessaires, de limiter les interférences entre canaux adjacents, et de maximiser le débit de communication.
Parfois, les systèmes PMR doivent être adaptés aux besoins particuliers. Cela s'applique, par exemple pour la communication mobile dans les tunnels, notamment si une partie de la communication se passe sur la surface et une autre en partie souterraine. La propagation dans les tunnels est généralement mauvaise, en particulier à des fréquences basses. Par conséquent, des câbles rayonnants sont utilisés le plus souvent, mais malheureusement, leur perte permet à l'équipement de combler seulement des distances relativement courtes et donc des moyens et des compétences spécifiques sont nécessaires pour construire correctement des réseaux importants en tunnel. En France, la réglementation impose la couverture de ces zones (Voir retour d'expérience de l'incendie tunnel Mont Blanc, (§ 2.6.3).

Notre intention ici n'est pas de décrire tous les cas possibles, mais simplement de donner au lecteur une idée sur différentes configurations possibles des systèmes PMR.

En complément, nous souhaitons également rappeler brièvement les paramètres qui influencent la couverture d'un réseau radio.

Pour permettre une couverture maximale du territoire, celui-ci est divisé en une multitude de cellules. Chaque cellule constitue une zone dans laquelle une communication peut être passée autour d'une antenne-relais. La portée des antennes-relais, et par conséquent la taille des cellules, dépend de multiples critères tels que le type d'antennes-relais, le relief (plaine, montagne, vallée…), le lieu d'implantation (zone rurale, zone urbaine…), etc.
La taille des cellules varie également en fonction du nombre d'utilisateurs susceptibles d'être présents sur la zone de couverture. En effet, une antenne-relais a une capacité limitée d'écoulement du trafic (c'est-à-dire des appels passants par le relais). C'est la raison pour laquelle, en zone dense (en milieu urbain par exemple), les cellules sont toujours de petite taille, ce afin d'assurer un bon écoulement du trafic des communications et donc de garantir la qualité du réseau. Les fréquences ou "ressources radio" sont limitées. Elles sont réparties sur les cellules pour satisfaire la demande du trafic (voix, données).

Le champ électromagnétique émis par une antenne se propage principalement à la manière du faisceau d'un phare. L'énergie du champ décroît très rapidement, à mesure que l'on s'éloigne de l'antenne. Selon leur puissance, les relais couvrent des zones allant de quelques centaines de mètres à plusieurs kilomètres. On distingue les stations micro-cellulaires et macro-cellulaires. En moyenne, la puissance émise par une antenne est de l'ordre de quelques dizaines de watts.

Enfin, pour une puissance d'émission donnée, la couverture d'une antenne évolue en fonction de la fréquence (voir figure ci-dessous). Les fréquences basses permettent d'augmenter la couverture. Toutefois, pour la transmission de données, l'efficacité spectrale (nombre de bits transmis par

seconde par hertz de fréquence) est d'autant plus importante que la fréquence est élevée (théorème de Shannon-Nyquist).

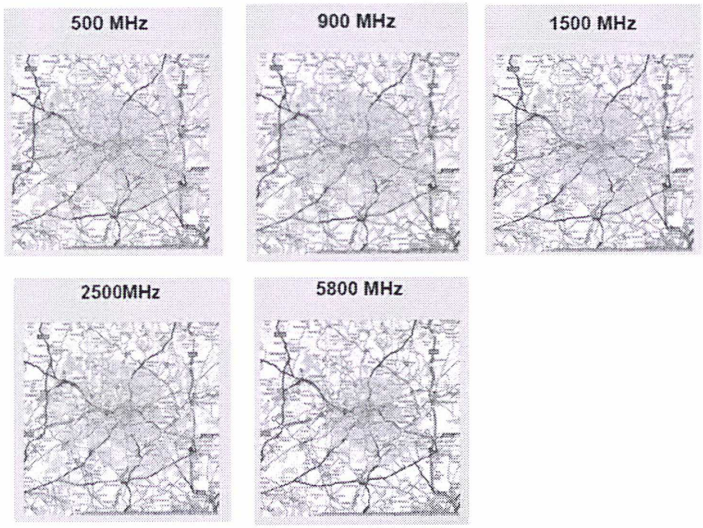


Figure : illustration de l'évolution de la couverture d'une antenne-relais en fonction de la fréquence pour une puissance d'émission donnée[7].

2.3 Les différentes situations de fonctionnement prises en compte

Les réseaux de communication employés par les forces de sécurité et de secours doivent tenir compte pour leur dimensionnement des opérations au quotidien, des manifestations programmées, des crises et des situations de catastrophe imprévues.

2.3.1 Utilisation au quotidien

Les utilisations au quotidien englobent les opérations de routine que les organismes PPDR mènent au sein de leur juridiction. En règle générale, ces opérations sont à l'intérieur des frontières nationales. Généralement, les exigences de spectre et de l'infrastructure sont déterminés en utilisant ce scénario avec une capacité supplémentaire pour couvrir les événements d'urgence non prévus.

2.3.2 Crise importante ou événement public programmé

L'infrastructure et le spectre doit être dimensionnés afin de répondre à des crises de grande ampleur (typiquement un incendie de forêt) pour lesquels des plans de réponse existent et à des manifestations publiques programmées (jeux olympiques, sommets G8-G20), en complément des opérations de routine. L'ampleur de la crise et la nature de l'événement peuvent nécessiter des ressources supplémentaires d'organismes en provenance d'autres régions adjacentes, frontalières ou au plan international.

Des moyens de radiocommunication supplémentaires peuvent être acheminés sur site en tant que de besoin. Ces équipements pouvant ou non être reliés au réseau existant.

[7] Source: Safety First - Reinvesting the Digital Dividend in Safeguarding Citizens (Wik consult, mai 2008)

2.3.3 Catastrophe majeure

Les catastrophes peuvent être celles qui sont causées soit par l'activité humaine ou naturelle. Par exemple, les catastrophes naturelles comprennent un tremblement de terre, une tempête tropicale majeure, les inondations, etc. Les événements d'origine humaine comprennent des actes terroristes ou des situations de conflit armé. Des moyens de communication satellitaires viennent généralement en complément des réseaux utilisés par les forces de sécurité et de secours ou les réseaux commerciaux susceptibles d'être hors service.

Examinons à présent la situation en France en Europe et dans le monde des utilisations de la PMR par les forces de sécurité et les opérateurs d'importance vitale.

2.4 Situation en France, en Europe et dans le reste du monde

2.4.1 La France, pionnière dans le passage au numérique

Deux réseaux complémentaires pour les forces de sécurité et de secours

À la fin des années 1980, la Gendarmerie décidait de s'équiper au niveau national du réseau RUBIS basé sur la technologie TETRAPOL. Cette technologie offre un niveau de sécurisation des transmissions renforcé. Les mécanismes dont la liste suit[8] ont été définis afin de contrôler l'accès au réseau et la confidentialité des communications:

- Détection d'intrusion,
- Chiffrement de bout en bout,
- Mot de passe au niveau du terminal,
- Authentification mutuelle mobile et réseau,
- Gestion automatique sécurisée des clés d'authentification et de chiffrement,
- Utilisation d'identités temporaires,
- Désactivation du terminal,
- Contrôle d'identité du terminal

La Gendarmerie a été à l'avant-garde d'une technologie utilisée aujourd'hui par plus de 1,5 millions de personnes dans 35 pays[9]. RUBIS a été le premier réseau PMR numérique au monde et il continue à fonctionner au sein de la Gendarmerie. Des délégations du monde entier ont été accueillies par la Gendarmerie pour mieux connaître sa façon d'utiliser la technologie PMR.

Déployé entre 1993 et 2000, RUBIS est un système sécurisé de radiocommunication numérique cellulaire, privilégiant les communications à longue portée en territoire rural. Il utilise des fréquences de la plage des 80 MHz, ce qui permet de couvrir environ 90 % du territoire avec un nombre de relais radios restreint (476). Ces relais sont reliés entre eux par 750 faisceaux hertziens, ce qui garantit un niveau élevé de robustesse. Ils desservent 42 800 terminaux radio (fixes et mobiles, généralement implantés dans les véhicules).

Le réseau offre de nombreux services, principalement aux gendarmes départementaux, d'un haut degré de disponibilité, de confidentialité et de gestion des priorités : des services de phonie (conférences, communications individuelles, appels multiples, appels en mode direct [talkie-walkie], appel d'urgence) et des applications de transmission de données (messagerie et consultation des bases de données, transmission de fiches de signalement de personnes disparues).

---

[8] D'après Direction technique TDF, Fiche Savoir + , TETRAPOL, 17 avril 2005

[9] Le programme RUBIS a donné naissance à la technologie propriétaire TETRAPOL soutenue par une soixantaine d'industriels, en sus du maître d'œuvre industriel du programme, EADS-DCS.

Lancé en 1995, ACROPOL est le réseau de radiocommunications numérique sécurisé de la police nationale, basé également sur une technologie TETRAPOL. Son déploiement s'est achevé en 2007. ACROPOL, privilégiant les communications en milieu urbain, utilise des fréquences de la bande des 400 Mhz. Les distances de propagation à cette fréquence étant plus courtes, ACROPOL a un nombre plus important de relais radio que RUBIS (1 150 au lieu de 476), alors qu'il couvre un territoire moindre (85 % au lieu de 90 %). 40 % de ces relais radios sont reliés entre eux par faisceaux hertziens et 60 % par liaisons louées à France Télécom.
Les personnels de police sont équipés de terminaux portatifs dits « P2G » et les véhicules de postes fixes dits « boitiers émetteurs récepteurs » (BER). Tout utilisateur d'ACROPOL accède à tous les services par un poste fixe ou embarqué à bord d'un véhicule. Inversement, chaque agent peut être joint partout, ou presque, en composant simplement son numéro de poste. ACROPOL répond aux besoins opérationnels urgents auxquels les moyens précédents ne pouvaient pourvoir : la sécurité (le réseau est chiffré), l'homogénéité (trois gammes de fréquence sont possibles), le partage des moyens (une seule infrastructure est ouverte à l'ensemble des services de police).

Une évolution tendancielle vers la mutualisation : l'Infrastructure nationale partagée des transmissions (INPT)

Dans le prolongement de la loi d'orientation pour la sécurité intérieure (LOPSI) du 29 août 2002, le réseau ACROPOL a été intégré dans l'Infrastructure nationale partagée des transmissions (INPT) créée par un décret du 3 février 2006[10] pris en application de l'article 9 de la loi de modernisation de la sécurité civile du 13 août 2004. Ce texte vise à rendre interopérables, au moyen d'un ensemble de règles et normes techniques, dénommé « Architecture unique des transmissions » (AUT), les réseaux de communication radioélectriques des moyens nationaux de la sécurité civile, des services d'incendie et de secours, de la brigade des sapeurs-pompiers de Paris, du bataillon de marins-pompiers de Marseille, de la police nationale, de la gendarmerie nationale ainsi que des services d'aide médicale urgente.

ACROPOL a constitué l'ossature de base de l'INPT, infrastructure sur laquelle se déploient les autres réseaux. L'INPT permet les communications de groupe grâce auxquelles les agents en mission peuvent suivre l'action de leurs collègues et rester en communication continue avec le centre de commandement. Elle permet aussi les communications individuelles, soit en mode direct (type talkie-walkie), soit via l'infrastructure. Par ailleurs, la transmission de données sur l'INPT facilite l'interrogation de fichiers de police (Fichier véhicule volé, Fichier personne recherchée etc.) à partir des terminaux informatiques embarqués (TIE). Comme pour RUBIS, des outils de géolocalisation, *via* un module GPS connecté à l'INPT, permettent au centre de commandement de visualiser en temps réel les équipes en patrouille. De surcroît, l'INPT permet une communication directe (type talkie-walkie ou via l'infrastructure) entre les policiers et les pompiers.
Le réseau ANTARES, système de radio des forces de sécurité civile, a également été intégré à l'INPT. Cette intégration a porté la couverture du territoire national par l'INPT de 85 à 95 %. Le déploiement du réseau ANTARES, à partir de 2007, a induit une forte augmentation du nombre de sites de l'INPT, passé de 1 150 à près de 1450, et un renforcement de certains sites existants (ajout de 140 relais). Les nouveaux relais radio créés pour ANTARES ont permis de couvrir des zones blanches, de par l'absence initiale de besoin police. Le déploiement du réseau est encore incomplet. L'objectif cible pour 2015 est de 92 000 terminaux équipant les services de secours.

[10] Décret n° 2006-106 du 3 février 2006 relatif à l'interopérabilité des réseaux de communication radioélectriques des services publics qui concourent aux missions de sécurité civile

Une convergence à terme des réseaux de la Police et de la Gendarmerie nationale

Les deux forces sont dotées de réseaux mobiles de transmission distincts mais complémentaires. Seul, le réseau CORAIL-NG, utilisé par la gendarmerie en région parisienne pour les besoins de ses forces mobiles, de ses unités de recherches, de la garde républicaine et de la sécurité des transports aériens, est conçu pour être interopérable avec le réseau ACROPOL-INPT employé par la police nationale. Il en est de même des réseaux déployés lors de grands événements (sommets de l'OTAN ou du G20).

CORAIL-NG

Au début des années 2000, la gendarmerie s'est trouvée confrontée à l'obsolescence des réseaux radio analogiques CORAIL 1G (dédié aux forces de gendarmerie mobile) et CRISTAL (dédié aux unités de recherches) qui utilisaient la bande des 400 MHz, ces unités effectuant l'essentiel de leurs missions en milieu urbain. Depuis 2005, elle a déployé un réseau de radiocommunication numérique, baptisé CORAIL NG, pour les besoins de la gendarmerie mobile, la garde républicaine, les unités de recherches et la gendarmerie des transports aériens (région parisienne). Ce réseau, moyennant un investissement de 21,3 M€, devait desservir 7500 terminaux, nombre qui a été ramené à 1 260.

Le principe d'accoler CORAIL NG sur l'infrastructure du réseau ACROPOL a été agréé par un protocole d'accord du 3 mars 2004. Le réseau ACROPOL étant devenu partie intégrante de l'INPT à sa création en 2006 (*cf. supra*), CORAIL NG a été intégré à l'INPT. Cette intégration permet des communications opérationnelles, directes ou via la chaine hiérarchique, entre l'ensemble des acteurs de la sécurité intérieure et des secours, à Paris et en petite couronne. Compte tenu de la densité des communications à Paris, le réseau est doté d'une infrastructure fixe à Paris propre à la gendarmerie. Dans un souci de mutualisation, la Direction générale des services extérieurs (DGSE) bénéficie dans le cadre d'un protocole d'accord, d'une partie des ressources radioélectriques du réseau CORAIL NG déployées sur Paris.

Source : Cour des comptes, Rapport « La mutualisation entre la Police et la Gendarmerie nationale », tome 2 (octobre 2011)

ACROPOL et RUBIS recourent à la même technologie de radiocommunication professionnelle, mais sous des versions logicielles incompatibles. Ils utilisent des bandes de fréquences et des clés de chiffrement différentes. Leur conception technique et leur configuration fonctionnelle rendent impossible leur compatibilité « native ». Ces différences correspondent à leurs conditions d'utilisation, en zone urbaine dense pour la police et dans des espaces souvent dégagés et étendus pour la gendarmerie. Leur interopérabilité complète en tout lieu serait d'ailleurs sans utilité selon les responsables de la Gendarmerie nationale. Cependant, plusieurs aménagements techniques ont permis de la renforcer.

La décision a été prise de mutualiser la maintenance de ces deux réseaux en recourant à un marché unique d'externalisation alors que jusqu'à présent, la maintenance d'ACROPOL-INPT était externalisée, mais celle de RUBIS restait assurée par des services de la gendarmerie. La maintenance des terminaux, quant à elle, commence à être prise en charge, au sein des deux forces, par un service de la gendarmerie.

Une réflexion a été engagée sur la constitution à horizon 2020 - 2025 d'un réseau unique qui procurerait des économies de fonctionnement sans doute importantes, bien que non évaluées, mais elle nécessiterait des investissements également importants. Ni les unes ni les autres n'ont été évalués, notamment parce que des choix techniques et fonctionnels restent à faire. Deux évolutions techniques, préalables à un réseau unique et nécessaires pour optimiser le fonctionnement des réseaux, seraient sans attendre source d'économie : la substitution de faisceaux hertziens à des liaisons louées pour relier entre eux les relais radios du réseau de la police (voir § 2.5.7 sur les ordres de grandeur des coûts d'un réseau dédié), l'homogénéisation des sous-systèmes de commutation IP des deux réseaux. Une stratégie est donc à définir par les directions compétentes du ministère de l'Intérieur vers un réseau unifié avec des étapes de mise en cohérence au plan technique et organisationnel. Cette stratégie doit également prendre en compte

la question de durée de vie de la technologie TETRAPOL (commune aux deux réseaux) pour amortir les investissements.

Des modes d'exploitation spécifiques à chaque entité pour les forces de sécurité et de secours

Un consultant nous a présenté les différents modes d'exploitation actuels des réseaux utilisés par les forces de sécurité et de secours (Police, Gendarmerie, Pompiers, SAMU). Il nous a fait part de son point de vue sur les moyens de communication actuels.

Les forces de police sont dirigées par un centre d'information et de commandement (CIC) qui reçoit les appels d'urgence en provenance du 17. Le CIC dirige les vacations dès qu'un véhicule a quitté le commissariat de police. Les véhicules sont géolocalisés. L'idée est d'avoir un maximum d'équipes sur le terrain. Le CIC appelle le véhicule le plus proche du lieu de l'intervention, puis informe l'ensemble des équipages sur le terrain. La géolocalisation a été difficile à mettre en place, indique ce consultant, mais elle a considérablement amélioré l'efficacité des interventions. Le réseau est conçu essentiellement pour la voix. Le débit théorique est de 9 kbits/s, mais en réalité, il se situe plutôt autour de 1,2 kb/s. Il existe une application pour le contrôle des plaques d'immatriculation des véhicules en interrogeant les fichiers centraux du ministère chargé de l'Intérieur. L'application est ancienne et très sécurisée. De fait, la procédure est très longue et en cas d'échec, du fait de l'absence de protocole d'authentification centralisée de type Single Sign On (SSO), il est nécessaire de reprendre toute la procédure. Aussi, les équipes interrogent actuellement le CIC à la voix, ce qui est également fastidieux. Pour ce consultant, il serait nécessaire d'élargir la bande passante pour disposer d'applications web sécurisées permettant l'échange rapide de données et améliorer ainsi l'efficacité de ces procédures de contrôles. Une autre piste d'amélioration consisterait à équiper les véhicules de terminaux embarqués permettant de formaliser les procédures en cours de mission, mais actuellement le réseau ne le permet pas.

Les gendarmes ont le même mode de travail. Ils dépendent d'un centre opérationnel et de renseignement de la Gendarmerie (CORG). Il y a un CORG par département qui coordonne le travail des équipes sur le terrain. Typiquement, la patrouille part le matin et revient en fin de journée. Elle a besoin de moyens mobiles. Selon ce consultant, la Gendarmerie a beaucoup développé d'outils informatiques en utilisant des logiciels libres et a su se doter d'applications intéressantes fonctionnant même avec peu de débit.

Chez les pompiers, l'exploitation est très différente. Le centre de traitement d'alerte (CTA) dépêche les pompiers depuis la caserne la plus proche sur le lieu d'intervention. La direction se projette sur le terrain. Le premier responsable de l'équipe d'intervention qui arrive sur les lieux prend les fonctions de commandement des opérations de secours. C'est lui qui va diriger les communications et demander des renforts en fonction de ses constats sur le terrain. De plus, les pompiers utilisent beaucoup la communication de poste à poste en utilisant plusieurs fréquences tactiques, par exemple entre le fourgon pompe tonne et l'équipier qui déroule le tuyau sur de grandes distances (200 ou 300 mètres) ou pour le déploiement d'une grande échelle. Des rapports périodiques sont transmis via le réseau relayé.
En ce qui concerne l'utilisation de nouvelles applications, l'une d'entre elles concernerait l'emploi de la vidéo à partir d'un hélicoptère permettant de déterminer des contours de feu. Les images seraient transmises par radio vers un logiciel de propagation de feu permettant d'effectuer des calculs précis afin de prévenir les populations et de procéder aux évacuations nécessaires. Des essais ont été réalisés avec les marins pompiers à Marseille. Les données vidéo ont été transmises via le réseau 3G d'Orange. L'essai s'est révélé concluant mais a nécessité d'adapter le réglage des antennes.

Au SAMU, le médecin urgentiste dirige les communications à la voix depuis le centre d'appel du 115. Les fréquences d'écoute sont communes entre les équipes de secours et de soins d'urgence. Les urgentistes souhaiteraient disposer d'outils plus performants pour la transmission de données. Par exemple, une caméra pourrait être fixée sur la chasuble du médecin urgentiste et permettrait de renvoyer des images à sa salle de régulation afin de recueillir un avis. Le télédiagnostic permettrait par l'envoi de paramètres acquis sur place (électrocardiogramme,...) de gagner du temps dans l'accueil du patient à son arrivée aux urgences.

Vers de nouveaux partenariats pour l'INPT ?

Nous nous sommes interrogés sur la possibilité d'intégrer d'autres services de l'État chargés de missions de sécurité publique à l'INPT, tels que le service des douanes ou les polices municipales, ainsi que des opérateurs d'importance vitale qui peuvent être amenés à mettre en œuvre des procédures d'intervention conjointes.

À la Direction générale des douanes et des droits indirects, il nous a été précisé que les actions de surveillance ne mettent pas en œuvre d'infrastructure dédiée de communication. Les douaniers utilisent actuellement un système de radio mobile professionnelle numérique utilisant la technologie dite DMR[11]. Les terminaux DMR sont utilisés sans infrastructure, mais occasionnellement, ils peuvent être relayés à partir d'une station relais embarquée à bord d'un véhicule. Ce dispositif se heurte toutefois à deux difficultés : d'une part, le mode semi-duplex ne convient pas aux agents, d'autre part le dispositif trouve rapidement ses limites lors d'interventions de type « go fast[12] » routiers. Aussi, les agents sont équipés en compléments de terminaux mobiles utilisant le réseau 3G d'un opérateur commercial ouvert au public. L'abonnement à ce réseau permet la mise en place de conférences qui sont adaptées aux interventions, quand le réseau fonctionne bien. Mais les utilisateurs ne disposent pas d'un mécanisme de préemption en cas difficulté de fonctionnement. Nos interlocuteurs estiment que la PMR, du moins en l'état actuel des services offerts, est mal adaptée à leurs missions. Les forces veulent disposer d'un système d'information permettant de piloter au mieux leurs interventions, donnant accès à la géolocalisation, aux bases de données pour le contrôle des individus, la passation de consignes, ou à la saisie dématérialisée de procès-verbaux.

Concernant les polices municipales, il nous a été précisé au Sénat que, à moins de redéfinir leurs missions, ces entités n'ont aucun pouvoir en matière de police judiciaire et d'investigation. Il revient aux maires de décider des moyens de communication pour leur police et il semble difficile d'imposer d'entrée de jeu leur intégration à l'INPT. La question des prérogatives des policiers municipaux reste un sujet sensible. On estime qu'ils sont plus de 18000 aujourd'hui, répartis dans quelque 3500 communes en France[13].

L'état-major de l'Armée de l'air nous a fait part de son expérimentation de l'INPT afin d'assurer l'interopérabilité de ses propres moyens de secours (pompiers, ambulances) avec ceux de la sécurité civile. Des terminaux ont été mis à disposition sur les bases aériennes à vocation nucléaire. Les responsables de l'Armée de l'air se sont félicités de la réussite de cette expérimentation qui repose sur une démarche très pragmatique et permet de s'affranchir des problèmes d'interface.

---

[11] Il s'agit d'une technologie de radio professionnelle mobile numérique offrant quelques fonctionnalités basiques

[12] Le go fast (« aller vite ») est une technique utilisée par les trafiquants pour importer des produits stupéfiants ou de contrebande, en utilisant des voitures de grosse cylindrée, souvent volées.

[13] Police municipale: quelles missions, quelles prérogatives? (Libération, 1er juin 2010)

Au Ministère chargé de l'Intérieur, nous avons été informés du projet de rénovation du réseau national d'alerte (RNA). Le projet de système d'alerte et d'information des populations (SAIP)[14] qui remplacera le RNA empruntera l'INPT et des réseaux mobiles commerciaux ouverts au public. La mise en œuvre de ce système fait l'objet d'un programme s'étalant sur une période de 7 ans (2009-2015). Le coût total estimé du projet est de 80 millions d'euros financés sur le budget de l'Etat[15]. Le SAIP est présenté plus en détail dans l'encadré ci-après.

Enfin, d'autres opérateurs d'importance vitale, dans le domaine de l'énergie notamment ou des réseaux d'eau pourraient trouver un intérêt à rejoindre l'INPT en raison de procédures conjointes avec les forces de sécurité et de secours que ces opérateurs peuvent être amenés à mettre en œuvre à l'occasion de crises.

Le projet de système d'alerte et d'information des populations (SAIP)

L'alerte des populations consiste à diffuser un signal destiné à avertir des individus d'un danger, imminent ou en train de produire ses effets, susceptible de porter atteinte à leur intégrité physique. Les messages diffusés visent à informer les populations sur la nature de l'événement et à délivrer des consignes de comportement précises à suivre impérativement.

[redacted]

Le Livre Blanc de la Défense et de la Sécurité Nationale, adopté en juin 2008, a désigné la modernisation de l'alerte des populations comme un objectif prioritaire de l'action gouvernementale. Il s'agit de doter la France d'un « réseau d'alerte performant et résistant » en remplacement du Réseau National d'Alerte (RNA) dont la vétusté grandissante et l'architecture héritée de la seconde guerre mondiale ne permettent pas de répondre aux enjeux actuels de protection des populations. Le dispositif actuel d'alerte repose sur le réseau national d'alerte (RNA), constitué d'environ 3 800 sirènes reliées par un réseau dont le bon fonctionnement est assuré par France Télécom.

La mise en place du nouveau système d'alerte, dénommé SAIP (système d'alerte et d'information des populations) érige en priorité la fonction de « protection » des populations en intégrant, une capacité à avertir les populations de tout événement de sécurité civile : catastrophes naturelles (inondations, séisme…) technologiques (accident industriel, transport de matières dangereuses…), outre les attentats terroristes. La vocation initiale du RNA qui était d'avertir les populations d'un danger aérien est donc largement dépassée.

Dans un souci de diversification, le SAIP mobilisera plusieurs moyens d'alerte mis en réseau de façon à assurer une mobilisation maximale des populations, ces moyens pouvant être activés concomitamment. Aussi est envisagée la mise en place d'une première couche de sirènes par des autorités diverses (État, communes, établissements industriels soumis à plan particulier d'intervention), renforcé par d'autres moyens d'alerte et d'information (automates d'appel, panneaux à messages variables, Radio Data System et cell broadcast[16]...). L'activation des sirènes utilisera les canaux du réseau ANTARES (INPT). Parallèlement, la diffusion de messages sur les téléphones mobiles sera fortement privilégiée, l'objectif étant de cumuler les moyens d'alerte avertissant le plus grand nombre et chacun, individuellement, de la survenue d'un danger. Enfin, le partenariat noué avec les radios et télévisions du service public (Radio France et France Télévisions en particulier) sera maintenu, ces médias demeurant des vecteurs efficaces de diffusion de l'information, après déclenchement de l'alerte. Il pourra être élargi à des médias autres que publics.

[14] Source : L'alerte et l'information des populations, site Internet de la direction de la sécurité civile, Ministère chargé de l'intérieur
[15] Le Système d'Alerte et d'Information des Populations, Présentation Direction de la sécurité civile (2010)
[16] Le cell broadcast permet de diffuser un message sur tous les téléphones portables situés sur une zone déterminée

La convergence des réseaux mobiles aussi au niveau des armées

Il faut d'avantage raisonner en termes de service dédié que de réseau dédié, estime un équipementier. Dans la défense, au début (années 1980-90), chaque armée avait son réseau dédié. Il s'agissait de bons réseaux, surtout celui de l'armée de l'air. Il a fallu les renouveler au début des années 1990 lors du passage au numérique. Cet équipementier a réussi à convaincre les armées de s'équiper d'un réseau partagé (réseau virtuel partagé). C'était une petite révolution. Des fonctions de priorités ont été intégrées. Ce qui est important, ce n'est pas l'infrastructure, mais de pouvoir transmettre d'un point A à un point B avec la bonne priorité. Le temps de persuasion est long. Le réseau SOCRATE a vu le jour au début des années 2000.

La volonté de certains opérateurs d'importance vitale de s'associer compte tenu des enjeux de compétitivité pour l'accès au très haut débit

Le souhait de renforcer les coopérations se manifeste également au niveau de certains opérateurs d'importance vitale. Dans le cadre de ce mémoire, nous avons pu rencontrer le représentant de l'association des grands utilisateurs de réseau radio d'exploitation (AGURRE), association récemment constituée. AGURRE souhaite fédérer notamment des entreprises réalisant des missions de service public (transport, énergie,...) et des entreprises industrielles. En mai 2012, cinq membres ont déjà rejoint l'association : Aéroport de Paris, Air-France, la Régie autonome des transports parisiens (RATP), Réseau Ferré de France (RFF), et la Société nationale des chemins de fer (SNCF). Des contacts étaient en cours avec Électricité de France (EDF) et sa filiale de distribution ERDF. Les objectifs de l'association sont de rassembler les demandes des utilisateurs de réseaux radio professionnels, de les représenter dans les discussions devant les instances de régulation, d'assurer une veille technologique et d'aider les adhérents dans le développement de leurs réseaux. AGURRE souhaite en particulier être présent dans le débat concernant l'évolution des réseaux actuels vers le très haut débit. En effet, selon AGURRE, l'existence de ce type d'infrastructures d'accès radio deviendra un élément clé de la compétitivité des utilisateurs. Nous avons pu faire le point sur les enjeux pour la RATP et RFF, membres d'AGURRE représentant le secteur des transports.

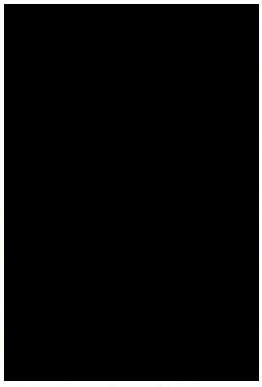
Le réseau TETRA de la Régie autonome des transports parisiens (RATP)

En 2003, les enjeux stratégiques de sécurité, de régulation du trafic et de politique de service ont conduit la RATP à se doter d'un réseau ultra performant, conforme à la norme TETRA[17]. Ce réseau permet d'assurer la sécurité des biens et des personnes sur ses lignes de bus et de métro à Paris. La RATP assure le transport annuel de plus de 3 milliards de passagers. Pour réguler la circulation de 1000 rames de métro, gérer 300 stations et 4500 bus, la régie s'appuie sur ses équipes d'ingénierie et de maintenance et sur son service de sécurité, auxquels il faut ajouter les conducteurs, les guichetiers et les personnels des stations. Tous ces agents ont besoin de moyens de communication robustes et fiables pour assurer la continuité des transports. Le réseau, qui assure une couverture sur 15 à 20 km autour de Paris, comprend 450 relais, dont 80 en surface. 15000 terminaux portatifs ou embarqués dans les véhicules sont utilisés au quotidien.

Le réseau TETRA de la RATP provient du rachat du réseau de l'opérateur Dolphin Telecom en dépôt de bilan (100 M€), qui a été redéployé pour tenir compte des applications métier de la

[17] Tetra est un système aux caractéristiques très proches de la norme Tetrapol, notamment en termes d'architecture et de services. A l'origine Tetra, norme approuvée par l'Institut européen des normes de télécommunication (ETSI) est censée définir un système ouvert. Par définition, un système ouvert permet de déployer un réseau à partir d'équipements provenant de différents constructeurs.

RATP. Il s'agit d'un investissement conséquent pour une entreprise publique structurellement endettée (5 milliards d'euros) et dont la vocation première est le transport, estime un représentant de la RATP. Pourtant, ce réseau est indispensable au métier. « *On n'imagine pas un conducteur de métro qui ne puisse remonter d'information à son poste de commandement* », ajoute-t-il.
Le réseau TETRA a contribué à améliorer la performance de la gestion des transports. Auparavant, la régie utilisait plusieurs réseaux analogiques qui n'étaient pas interopérables entre eux. Par ailleurs, la RATP a ouvert son réseau à des tiers. Elle a développé le concept Tétracité[18] qui leur donnera accès à des services radio à haute valeur ajoutée sans avoir à investir par leurs propres moyens dans un réseau dédié : la Ville de Paris a fait le choix de Tétracité en 2011, pour assurer les communications de plus de 2000 de ses agents. La Direction des Espaces Verts et de l'Environnement (DEVE), la Direction de la Prévention et de la Protection (DPP) et la Direction de la Propreté et de l'Eau (DPE) utilisent désormais la PMR numérique, grâce au concept Tétracité. Pour la RATP, l'ouverture de son réseau améliore le retour sur investissement par des revenus commerciaux nouveaux permettant de garantir le développement à long terme d'un réseau régional de communication devenu stratégique.



Si les besoins actuels du réseau sont bien couverts dans les cinq années à venir, la RATP s'interroge sur son évolution au moment où les projets du Grand Paris prévoient l'extension de plusieurs lignes (par exemple, extension de la ligne 14 dont l'ouverture est prévue en 2018). L'exploitant s'interroge en particulier sur le choix des futures normes pour le très haut débit et les fréquences, sachant que la bande des 400 MHz utilisée actuellement est très convoitée. Par exemple, l'automatisation des métros implique d'avantage de vidéo surveillance, qui augmentera les flux d'information critique à échanger. La modernisation des lignes sert de vitrine technologique pour la régie. Il y a de réels enjeux dans l'exportation de son savoir-faire industriel estime la RATP[19]. Les marchés d'infrastructure de transport sont à passer actuellement, alors que l'exploitant ne dispose pas encore d'une grande visibilité sur les technologies et sur les fréquences additionnelles qu'il pourrait obtenir. En outre, un changement de fréquence remettrait en cause tout l'investissement réalisé dans son réseau.

Les télécommunications ferroviaires: le réseau GSM-R de Réseau ferré de France

Pour faciliter la circulation des trains et améliorer la sécurité, Réseau ferré de France, propriétaire et gestionnaire des infrastructures ferroviaires de l'État, utilise des réseaux mobiles de télécommunication en complément de lignes fixes. Ces réseaux mobiles comprennent notamment la radio sol-train permettant d'assurer les communications entre les conducteurs de trains et les régulateurs ou agents de circulation. 14000 km de lignes sont couvertes. Un système analogique installé à partir de 1976 est en cours de remplacement par un réseau GSM-R (GSM-Rail), un réseau dérivé de la technologie GSM.

Le standard GSM-R a été développé dans le cadre de la mission que s'est donnée l'Union internationale des chemins de fer (UIC). Son but initial était la standardisation et l'amélioration des conditions de construction et d'exploitation des chemins de fer, particulièrement en matière de trafic international. Le GSM-R, qui est construit à partir de la technologie commerciale GSM, bénéficie des économies découlant de cet héritage. Il autorise une mutation numérique à un coût compétitif, permettant le remplacement de tous les systèmes de communication filaire (le long de la voie) et des réseaux radio ferroviaires analogiques existant dans chaque pays qui sont

[18] Site internet Tétracité
[19] La RATP est présente à l'international : tram de Manchester, métro d'Alger en 2011

incompatibles entre eux : on comptabilise en effet plus de 35 systèmes de communication ferroviaire différents, rien qu'en Europe…

Le GSM-R permet de transporter des informations de signalisation ferroviaire directement jusqu'au conducteur, facilitant ainsi une vitesse de circulation du train plus élevée ainsi qu'un trafic plus dense, tout en maintenant un haut niveau de sécurité.

Le GSM-R utilise des antennes relais dédiées, proches de la voie ferrée. La distance entre chaque station de base est de trois à quatre kilomètres. Cette proximité crée un haut degré de redondance et une plus grande couverture et fiabilité. Le train maintient en permanence une connexion numérique vers le centre de régulation des trains. Cette connexion a un niveau de priorité supérieur aux autres utilisateurs. Si la connexion est perdue, le train s'arrête automatiquement. Le réseau GSM-R compte 2500 stations de base. 2x4 MHz de fréquences dédiées adjacentes aux fréquences du GSM ont été attribuées pour le rail dans toute l'Europe[20].

Le déploiement de ce réseau est prévu sur 10 ans (2004-2014). 10000 engins moteurs seront équipés de postes mobiles et les utilisateurs devraient disposer de 20000 à 30000 terminaux. Une extension du réseau à la radio de manœuvre est également à l'étude.

Le réseau GSM-R est un réseau pratiquement sans trafic, mais qui doit répondre sans défaillir à toutes les sollicitations. L'exploitant attend une qualité de service et une disponibilité élevée :

- 99,51% du temps pour les cellules ordinaires
- 99,99% du temps pour les cellules couvrant une ligne à grande vitesse.

Les critères de choix du GSM-R portent sur des fonctionnalités spécifiques qui ne sont pas proposées sur les réseaux commerciaux ouverts au public telles que l'alerte radio, la numérotation fonctionnelle (utilisation du numéro de train pour les appels, les mécanismes de préemption et de priorité).

RFF suit de près les évolutions technologiques en cours. Compte tenu des temps de déploiement très longs et d'une durée d'exploitation d'environ 10-15 ans, l'une des questions cruciales pour l'exploitant concerne la pérennité des technologies de 4ème génération (LTE). Le problème se pose à l'identique au plan international. L'UIC a pris contact avec l'association internationale des utilisateurs de technologies TETRA[21] pour anticiper les changements à venir.

2.4.2 En Europe, les enjeux de l'interopérabilité et du très haut débit

En Europe, une bande de fréquence harmonisée de 2x5 MHz entre 380 et 400 MHz a permis le développement de réseaux nationaux de communication numériques PPDR dédiés en bande étroite à la suite d'un accord politique entre l'OTAN et la CEPT[22] (Accord dit de Schengen). Pour être exact, certains pays de l'OTAN disposent de 2x5 MHz [380-385] et [390-395] MHz, d'autres de moins (toujours dans la même bande), suivant les accords nationaux entre ministères de l'Intérieur et de la Défense. À noter que l'harmonisation du spectre n'a pas encore vraiment été abordée pour les autres bandes utilisées pour les technologies en bande étroite sur les plages [410-430] MHz et [450-470] MHz.

Le paysage européen des réseaux utilisés par les forces de sécurité et de secours soulève aujourd'hui trois constats majeurs :

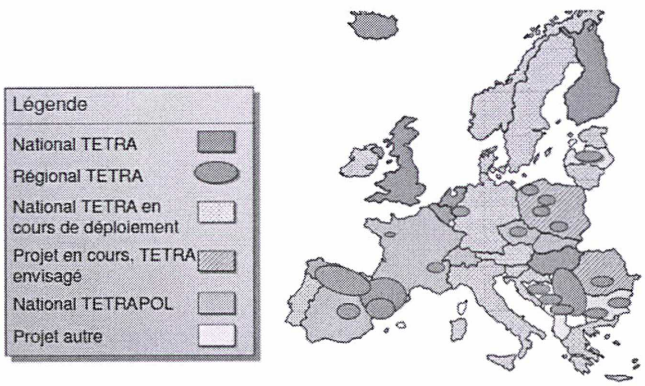
- d'une part, la coexistence de deux normes de communication distinctes TETRA et TETRAPOL (voir figure ci-après), la multiplicité des systèmes de chiffrement et les

[20] Canal montant : [876-880] MHz, Canal descendant [921-925] MHz
[21] TCCA – TETRA Critical communication association
[22] Conférence européenne des administrations des postes et télécommunications

problèmes linguistiques soulèvent des difficultés en matière d'interopérabilité aux frontières, telle que prévue par la Convention de Schengen[23].

- d'autre part, un avancement du déploiement des réseaux très inégal selon les pays. Si la France exploite des réseaux numériques partagés depuis plus de vingt ans, certains réseaux sont toujours en cours de déploiement (migration de l'analogique au numérique en Allemagne, Norvège) ou à l'état de projet (Pologne[24]). Une couverture globale au niveau européen est prévue en 2015.
- enfin, les réseaux numériques utilisés par les forces de sécurité et de secours ne permettent que des transmissions à bas débit, contrairement aux réseaux commerciaux ouverts au public de 3ème et très prochainement de 4ème génération.

Réseaux européens des forces de sécurité et de secours



Dans ce contexte, la Commission européenne nous a fait part de sa volonté d'aller de l'avant sur tous ces sujets. Plusieurs services de la Commission sont concernés : la Direction générale Société de l'information et des medias (INFSO), la Direction générale chargée de l'aide humanitaire et de la protection civile (ECHO) et la direction générale des entreprises et de l'industrie (ENTER).

La Commission européenne a tout d'abord appelé notre attention sur la question de la disponibilité de spectre pour les futurs réseaux PPDR. À cet égard, la Décision No. 243/2012/UE du Parlement européen et du Conseil du 14 Mars 2012 établit un programme pluriannuel en matière de politique du spectre radioélectrique[25].
L'article 8.3 de la Décision 243/2012/UE dispose que la Commission, en coopération avec les États membres, veille à assurer la mise à disposition en suffisance du spectre, dans des conditions harmonisées, pour soutenir le développement de services liés à la sécurité et la libre circulation des équipements qui y sont associés ainsi que le développement de solutions interopérables innovantes dans le domaine de la sécurité et de la protection du public, de la protection civile et des secours en cas de catastrophe. Cette décision est légalement contraignante et sera mise en œuvre progressivement.
La Commission consacre aux communications PPDR une page de son site Internet sur la doctrine de l'Union concernant la gestion du spectre[26].
La Commission européenne contribue également aux travaux du groupe FM 49 (créé en 2011) de la Conférence européenne des administrations des postes et télécommunications (CEPT) dont

[23] Convention de Schengen art. 44
[24] Un appel d'offre devait être organisé en 2010 en prévision du championnat européen de football EURO 2012. Mais devant l'impossibilité de respecter l'échéancier, cette procédure a été annulée. (voir Rapport TETRA for POLAND, Mikromakro Institute, 8 juillet 2011)
[25] Décision No. 243/2012/UE du Parlement européen et du Conseil du 14 Mars 2012
[26] In case of emergency – portail thématique de la DG INFSO sur les communications PPDR

l'objectif est de trouver une solution pour un spectre harmonisé pour les futures communications PPDR à très haut débit[27].
L'Institut européen des normes de télécommunication (ETSI) développe pour sa part des normes pour les futurs réseaux mobiles PPDR.

Par ailleurs, la Commission nous a indiqué que la disponibilité dans l'avenir de moyens de communication sécurisés et fiables pour les forces de police, de secours et, plus généralement, de personnels en charge de la sécurité du public a fait partie des réflexions des groupes ayant participé à la mise en place d'un thème « sécurité » dans le cadre du 7ème programme-cadre de R&D (PCRD). Ce thème a permis de financer de nombreuses actions liées aux systèmes de communication dit PPDR.
A titre d'exemple, la Commission européenne nous a cité des projets tels que "SECRICOM"[28], "EULER"[29], "HELP"[30] et quelques autres.
La Commission tente aussi de faire le lien avec une politique industrielle dans ce domaine. L'objectif de cette politique est de créer un grand marché intérieur pour des applications liées à la sécurité, en surmontant la fragmentation actuelle et en renforçant la base industrielle européenne. La politique industrielle de l'Union devrait faciliter le lien entre recherche et développement et mise sur le marché. À cet égard, il est important de garantir l'interopérabilité qui implique la disponibilité de spectre, la technologie et les normes adéquates ainsi que le business-model associé. La Commission nous précise qu'une première action dans ce domaine est la définition d'un mandat de standardisation.

La Commission rappelle également la tenue du séminaire « Interoperable communications for Safety and Security »[31] qui a eu lieu les 28 et 29 juin 2010 au centre de recherche commun (JRC) à Ispra (Italie), destiné à faire le point sur cette question et les nombreux autres séminaires qui ont suivi sur la même thématique[32].

Sur le thème de l'interopérabilité, le constat rejoint quelque part les difficultés toujours rencontrées pour l'achèvement du marché intérieur concernant les autres grands réseaux trans-européens en matière d'infrastructures de transport ou d'énergie tant au sein de l'UE qu' au niveau des régions voisines. Au-delà des initiatives rappelées ci-dessus, la question se pose de savoir si les réseaux PPDR ne pourraient pas eux aussi bénéficier du nouveau Mécanisme pour l'interconnexion en Europe[33], destiné à stimuler les réseaux européens ainsi que, en matière de financement, des futurs projects bonds[34].

L'avis des experts français sur la question de l'interopérabilité
Si le choix d'une fréquence commune est important pour garantir l'interopérabilité, l'un des experts consulté estime que cela ne suffira pas, car la problématique est surtout celle de la taille du marché. Si le marché est trop petit pour les équipementiers et pour les fournisseurs, il n'y aura pas les produits au bon coût qui permettent au marché d'exister. Aujourd'hui, les premiers réseaux privés pour la sécurité publique sont déployés aux Etats-Unis en 700 Mhz et non en 400 MHz. Il y a donc une problématique pour la France, estime cet expert.

[27] Les documents produits par ce groupe de travail sont consultables sur le site Internet de la CEPT à l'adresse http://www.cept.org/ecc/groups/ecc/wg-fm/fm-49/client/meeting-documents
[28] SECRICOM Projet de recherche collaborative dans le cadre du 7ème PCRD en 2008-2012. Son objectif est d'assurer la continuité des communications lors de la gestion des crises pour garantir la sécurité au sein de l'Union.
[29] EULER - EUropean Software Defined radio for wireless in joint security operations
[30] Project HELP (Enhanced Communications in Emergencies by Creating and Exploiting Synergies in Composite Radio Systems).
[31] Rapport du séminaire européen "Interoperable communications for Safety and Security (Ispra, Juin 2010)
[32] Driving wireless communication forward: Software Defined Radio and Cognitive Radio (Ispra, 17-18 Novembre 2011)
[33] Mécanisme pour l'interconnexion en Europe: la Commission adopte un plan de 50 milliards € pour stimuler les réseaux européens (Communiqué du 19 octobre 2011)
[34] The Europe 2020 Project Bond Initiative (Banque européenne d'investissement, 27 avril 2012)

« *Il y a 100000 raisons de ne pas être interopérable* », estime un autre équipementier. L'interopérabilité n'est pas qu'un problème de connexion. Il faut aussi décider du langage…et revoir l'organisation : les réseaux dédiés sont des réseaux hiérarchisés. On peut être distant de quelques mètres et se parler via les centres de commandement. L'interopérabilité n'est pas toujours effective, même entre deux départements voisins. Les militaires ont surmonté ce problème ; l'Otan a mis des moyens à disposition. Culturellement en France, on ne peut pas imaginer que le chef ne soit pas au courant. La gestion des canadairs est faite au niveau des services centraux. Il faudrait imaginer une structure plus décentralisée avec un commandement qui reste pertinent.

Un autre équipementier a souhaité apporter une clarification dans le cadre de ce débat sur l'interopérabilité. Selon lui, il convient de distinguer deux concepts : l'interopérabilité et l'itinérance (roaming). Dans le terme interopérabilité, il s'agit de s'interroger sur le moyen de communiquer à partir d'un réseau A vers un réseau B. Par exemple, en matière de sécurité publique, comment un policier Français peut-il discuter avec un policier Espagnol, chacun étant dans son territoire ? Il ne s'agit pas d'un problème de fréquence, estime cet expert, mais de la disponibilité de la bonne passerelle (gateway) pour permettre cette interopérabilité. Il est nécessaire de disposer d'un système, indépendamment de la fréquence, pour que l'information soit échangée au bon endroit pour permettre la communication.
En second lieu, il ne faut pas confondre l'interopérabilité avec l'itinérance (ou roaming). Le roaming, au sens opérateur commercial du terme, désigne plus généralement la capacité des clients à accéder à leurs services de téléphonie mobile (voix ou données) depuis différents réseaux au fur et à mesure d'un déplacement. Cette fonctionnalité est particulièrement utile en déplacement dans un pays étranger. C'est typiquement le cas par exemple du policier Espagnol, qui vient en France, à qui aujourd'hui, dans les faits, on va prêter un terminal, ou autoriser son terminal Espagnol à trafiquer sur le territoire français. L'accord de roaming entre opérateurs, mais également le fait que ce téléphone a la particularité de travailler dans toutes les bandes de fréquences, permettent d'accéder au service demandé. Il y a donc deux notions qu'il ne faut pas mélanger : certaines sont liées à la fréquence, d'autres ne le sont pas.

Concernant la question des fréquences, cet équipementier nous précise en outre que les américains ont, un peu plus tôt qu'en Europe, fait un exercice de dividende numérique au moment de l'arrêt de la télévision analogique. Les États-Unis ont décidé de longue date d'allouer une certaine bande de fréquences pour déployer les réseaux moyen – haut débit – avec 2 x10 MHz, dans la bande des 700 MHz (telecom Act de 1996). Deuxième précision sur les fréquences, l'Europe se pose aujourd'hui la question de savoir quelles sont les bandes de fréquences pouvant être allouées de manière uniformisée et harmonisée. Cet expert évoque deux raisons :

- développer un écosystème afin que les équipementiers n'aient pas un nombre démesuré de variantes de produits à développer ;
- pour permettre le roaming précité. Le groupe de travail FM 49 de la CEPT a pour objectif d'identifier les bandes de fréquences qui pourraient permettre d'accueillir du haut débit pour la sécurité publique. Il y a un certain nombre d'acteurs, parmi ceux qui participent à ces réunions, qui pensent que le 400 MHz est une bonne alternative. Il y en a d'autres qui pensent que le 700 MHz est une autre alternative.

Un expert du ministère de l'Intérieur a tenu à nous apporter une vision utilisateur et fonctionnelle par rapport à ce débat. Il confirme que l'interopérabilité va bien au-delà du choix d'une fréquence commune, puisque cela supposerait aussi un système totalement normalisé, pour éviter de développer différemment des portions de systèmes relevant initialement du même standard. Mais le vrai problème est avant tout d'ordre fonctionnel, estime cet expert. Il s'agit de savoir qui doit parler avec qui et avec quels droits. Ainsi, au sein de la Police, il n'est pas question que la Police judiciaire écoute ce que disent les renseignements intérieurs. Les uns et les autres ne doivent pas entendre ce que disent les agents de la sécurité publique... Il y a interopérabilité, mais il y a aussi à l'autre extrémité des mécanismes très avancés de cloisonnement. Il y a un postulat consistant à dire qu'il faut plus d'interopérabilité, mais quand on va dans le détail, la réponse et le besoin interopérable réel sont loin d'être aussi évidents. Il y a effectivement

des solutions d'interopérabilité aux frontières. Par exemple, la Gendarmerie nationale a pu partager un réseau privé avec la police allemande lors du Sommet de l'OTAN à Strasbourg en 2009[35]. Ces solutions reposent sur des centres de coopération policière et douanière qui intègrent nativement tous les systèmes de communication des uns et des autres. Il existe aussi des solutions pragmatiques de valises d'interopérabilité qui font des ponts entre communication de groupe et réseau hétérogènes. Elles sont mises à disposition aux frontières françaises avec des pays européens, mais elles ne sont pas nécessairement toujours utilisées, regrette cet expert. Selon lui, la problématique d'interopérabilité est réelle, mais dans l'ensemble du spectre des besoins utilisateur et notamment par rapport à cette vision du réseau à moyen-long terme avec un fort accroissement pressenti des besoins en services de données, le besoin d'interopérabilité ne fait pas partie des priorités. Le souci est avant tout d'apporter de nouveaux services qui amènent une plus-value à la fois sur la conduite des opérations, sur le volet tactique et sur le terrain, et qui permettent également le prolongement de l'espace de travail habituel en situation de mobilité (bureau mobile).

En outre, dans le domaine de la protection civile, la Commission a appelé notre attention sur les conclusions du Conseil relatives à l'approche intégrée pour une communication plus efficiente en matière de risque, de situation d'urgence et de crise, adoptées en 2011 sous présidence polonaise[36,37].

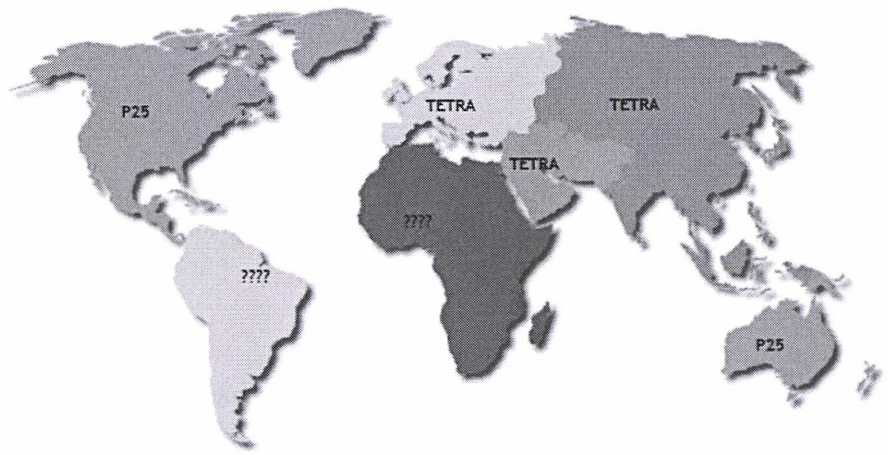
Le Conseil appelle les États membres à prendre des mesures pour assurer une approche intégrée de la communication des risques, d'urgence et de crise ; à développer davantage la prise de conscience des situations de risque et d'urgence en s'appuyant sur des technologies modernes ; à rechercher des solutions afin que suffisamment de spectre soit mis à disposition pour la sécurité publique, la protection civile et les secours : à prendre en compte le besoin d'une approche coordonnée en matière de spectre radio et de technologie. Le Conseil demande aussi à la Commission de promouvoir l'intégration des technologies émergentes dans le domaine de la communication en matière de risque, de situation d'urgence et de crise, en initiant des actions de recherche et développement, des expérimentations, leur mise en œuvre et leur évaluation ; et de faire le point pour la fin 2013 sur l'utilisation des technologies modernes d'information et les canaux d'information interactifs tels que les réseaux sociaux, dans le cadre des communications en situation d'urgence et de crise.

2.4.3 Reste du monde

Selon IMS Research[38,39], la technologie TETRA, en tant que norme de l'ETSI s'appuyant sur des bandes de fréquences harmonisées, est devenue la technologie dominante en Europe. Il y a environ 8 ans, le marché mondial de la radio professionnelle mobile s'est ouvert aux technologies numériques, avec les technologies TETRA en concurrence avec la norme P25 et une gamme de technologies propriétaires telles que TETRAPOL, EDACs et OpenSky.

[35] TETRAPOL helps the French Gendarmerie, key touch magazine p.33, 3/2010
[36] Draft Council conclusions on an integrated approach to more effective risk, emergency and crisis communication
[37] Draft Council conclusions on an integrated approach to more effective risk, emergency and crisis communication – corrigendum
[38] IMS Research est spécialisé dans les études de marché et de conseil pour l'industrie électronique mondiale
[39] The market for TETRA - now and in the Future (Presentation IMS Research, 2009)

Réseaux des forces de sécurité et de secours dans le monde



Asie et Moyen-Orient

Au cours des dernières années, on a constaté l'émergence de la technologie TETRA comme technologie numérique préférée par les utilisateurs de radio mobile professionnelle en Asie et au Moyen-Orient. Ainsi, en 2008, un réseau partagé TETRA a été déployé pour assurer la sécurité des jeux olympiques de Pékin. EADS secure networks a participé en fournissant ses dernières technologies. Cet événement a servi de vitrine pour promouvoir ces équipements. Par ailleurs, en Chine, la technologie TETRA est largement mise en œuvre par les forces de sécurité et de secours (forces de police à Pékin, Shanghai, Shenzhen, Zhuhai, Chengdu, Tianjin; contrôle aux frontières, police de Hongkong). Sur ce marché, IMS research anticipe une croissance annuelle moyenne de 40% sur la période 2008-2013. TETRA est également utilisé par les militaires chinois (Armée de l'air, la flotte du Nord, la région militaire de LanZhou).

Les grands équipementiers coopèrent avec des entreprises locales pour concevoir et produire les systèmes et terminaux TETRA pour le marché chinois. Ainsi, Motorola a implanté à Chengdu un centre de R&D et de développement de logiciels employant plus de 400 personnes. Le britannique Sepura coopère avec Tianjin 712 et Hisense pour produire des terminaux TETRA. Cette production locale est destinée à réduire les coûts et à s'adapter au mieux aux besoins du marché chinois. Depuis 2008, la firme HYT, basée à Shenzhen, coopère avec EADS pour développer des produits TETRA[40]. Au Moyen-Orient, des progrès similaires ont été observés avec l'arrivée de ces technologies pour des opérations militaires et de renseignement.

Russie

En Russie, le ministère pour l'information et les communications a également esquissé un plan pluriannuel pour déployer des réseaux TETRA pour les forces de sécurité et de secours ainsi que dans les transports.

[40] Partenariat entre EADS et HYT - Discours du Consul général de France à Canton – 16 Octobre 2008

Afrique et Amérique du Sud

L'Afrique et l'Amérique du Sud restent largement à conquérir, étant donné que la majorité des équipements installés doivent migrer vers le numérique. Cependant, le faible coût des équipements TETRA a conduit plusieurs métropoles à s'équiper en réseau TETRA dans ces régions, suggérant ainsi que TETRA pourrait y émerger comme technologie dominante au cours des cinq prochaines années. À noter, toutefois, que la technologie TETRAPOL est déjà mise en œuvre au Brésil[41]. Cette technologie est fournie par Cassidian à la police fédérale brésilienne depuis 2006[42] et équipe IRIS, le réseau Mexicain mis en œuvre dans les 32 états composant le pays[43].
La technologie P25 est la plus répandue en Amérique du Nord et en Australie, où la topographie et la densité de population sont comparables.

États-Unis et Canada : les premiers réseaux à très haut débit

L'évolution de la situation aux USA nous a été citée à plusieurs reprises comme un élément particulièrement intéressant de réflexion concernant l'avenir des réseaux européens. Huit ans après les recommandations de la commission tirant les enseignements de la gestion des événements du 11 septembre 2001 (voir retour d'expérience § 2.6), le Congrès américain a finalement adopté le 17 février 2012 une disposition législative[44] visant à créer un grand réseau à très haut débit, interopérable à l'échelle des USA. Elle garantit financièrement le lancement du projet en allouant une dotation initiale de 7 milliards de dollars.
Cette initiative, largement supportée par l'administration Obama, intervient dans le cadre du plan national sur le haut débit (NBP)[45] et met en œuvre un mécanisme novateur de partage des ressources en termes d'infrastructures qui devrait occasionner de substantielles économies tout en garantissant un haut niveau de robustesse. Les organismes de sécurité pourront notamment tirer parti du déploiement des réseaux commerciaux sans fil de quatrième génération (très haut débit mobile), afin de réduire significativement le coût global de la construction de leur réseau tout en garantissant l'interopérabilité et en renforçant sa résilience.
Ce nouveau réseau fonctionnera sur du spectre dédié, malgré une tentative infructueuse de partage des fréquences avec les opérateurs commerciaux[46]. Ce choix suscite déjà certaines critiques compte tenu de la rareté de la ressource en fréquences[47,48]. Verizon a récemment été pris de remords, en exprimant le souhait de partager le spectre avec le exploitants PPDR[49].

Le modèle américain a aussi été défini en réaction au modèle actuel fragmenté et à tendance monopolistique (Motorola), commente un équipementier. Par construction, il s'adresse à une communauté d'utilisateurs plus large que les « first responders ». Il prône l'utilisation d'une technologie (LTE) et de bandes de fréquences proches afin de limiter les coûts d'accès à la technologie et de déploiement. À la suite de l'échec des enchères pour le bloc D sur le modèle d'un partenariat privé/public, le spectre va rester à usage unique et dédié des forces de sécurité et autres professionnels. Certaines limitations de ce modèle sont en train d'apparaître dans les organismes de standardisation du LTE. À titre d'exemple, cet équipementier nous a cité le besoin en couverture via des terminaux haute puissance dans des zones où la couverture commerciale est inexistante, donc les sites radio ne seront jamais présents (à cause de la géographie des États-Unis).

---

[41] EADS: DS déploie le réseau Tetrapol IP au Brésil (Cercle finance, 16 septembre 2010)
[42] EADS in Brasil
[43] Cassidian – Brochure « solutions intégrées pour les services de secours et d'urgence » (Septembre 2010)
[44] Middle Class Tax Relief and Job Creation Act of 2012 H.R. 3630, Title VI – Public safety communications and electromagnetic spectrum auctions
[45] National Broadband Plan : connecting America – broadband and public safety
[46] FCC, Auction 73,700 MHz Band, 2008
[47] How politics inflame the 'spectrum crisis' (CNET News 16 février 2012)
[48] AT&T to end 2G service, offers free 3G phone upgrades
[49] Verizon's McAdam, in Keynote Address, Advocates for Shared Spectrum by Public and Private Sectors (The Sacramento Bee, 9 mai 2012)

Selon lui, le partage du reste des infrastructures fixes reste discutable ; en effet, quel organisme de sécurité acceptera d'être contraint par un opérateur commercial, s'interroge-t-il ? Quel opérateur commercial acceptera d'être contraint pour accueillir un relativement faible nombre d'utilisateurs exigeants sans que son (ses) concurrents ne soit (soient) soumis aux mêmes contraintes ?

Enfin, cet équipementier considère néanmoins qu'il est très important de regarder en détail ce qui se passe aux Etats-Unis pour en tirer le maximum d'expérience. Il va falloir trier entre les bénéfices tirés de l'utilisation d'éléments d'infrastructure partagée (liaisons, site, ... – ce qui est déjà fait par Telefonica en Espagne pour le réseau Sirdee par exemple) de ceux tirés de l'utilisation d'une technologie radio à basse puissance (de même niveau que les réseaux commerciaux) qui permet de diminuer légèrement le prix des terminaux tout en augmentant massivement le coût de l'infrastructure radio.

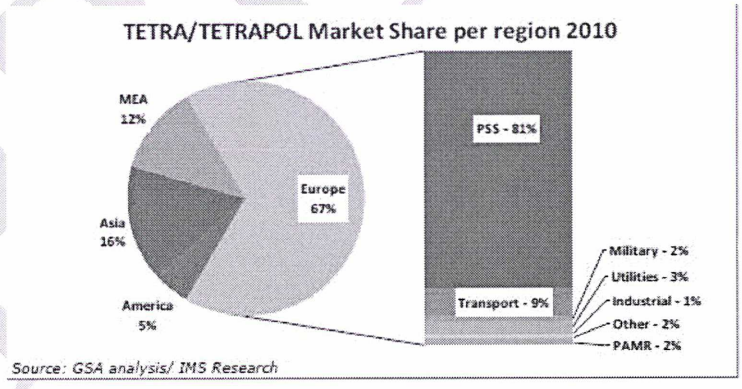
À noter enfin, l'approbation récente de la norme TETRA par les autorités américaine et canadienne.

Après cet état des lieux en France en Europe et dans le monde, examinons la question sous l'angle économique en nous intéressant tout d'abord à l'évolution du marché des utilisateurs de radio professionnelle mobile.

2.5 Le marché des utilisateurs de radio professionnelle mobile : un marché en forte croissance

2.5.1 Un marché dominé par les forces de sécurité et de secours

Au cours des 10 dernières années, le marché s'est essentiellement concentré sur les forces de sécurité et de secours, qui représentent plus de 80% du marché pour les technologies TETRA et TETRAPOL (voir figure ci-dessous).



Dans le secteur des transports, qui représente 9% du marché, l'avènement du numérique offre de nouvelles fonctionnalités non disponibles en analogique. Par exemple, la géolocalisation des bus permet l'information en temps réel des passagers sur les heures d'arrivées. Il est anticipé une croissance moyenne annuelle de 20% dans le secteur des transports. La technologie TETRA connaît un succès grandissant auprès des organismes de transport publics, avec un marché représentant le second plus important marché mondial pour TETRA. En particulier, les métros et aéroports s'équipent de plus en plus de ces technologies avec des contrats allant de 100 jusqu'à 6000 utilisateurs. Il ne faut toutefois pas oublier qu'en Europe, les transports ferroviaires ont

adopté le standard GSM-Rail dérivé de la norme européenne GSM afin d'ériger un vaste réseau paneuropéen interopérable.

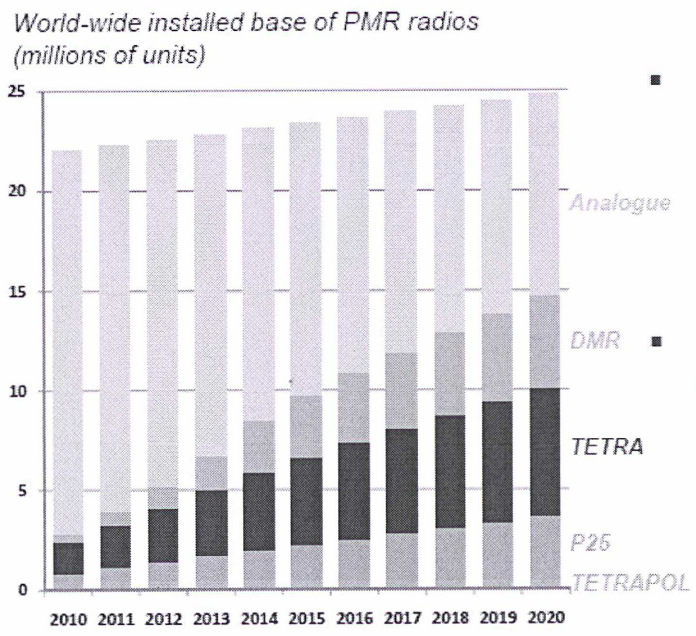
Les industries de réseaux représentent 3% des utilisateurs de ces technologies. La capacité de sécuriser la transmission de données a généré une forte impulsion au marché des énergéticiens où la télésurveillance et le contrôle-commande constituent des applications vitales. Pour ce secteur confronté à diverses menaces, notamment de sabotage ou d'attaques terroristes, la communication sécurisée des données est essentielle.

Dans le secteur de l'énergie, les commandes de terminaux TETRA devraient croître significativement. Actuellement, les principaux secteurs de croissance concernent le secteur pétrolier et gazier, où les radios peuvent être utilisées en zones d'atmosphère explosive (ATEX). Selon un analyste, le volume devrait doubler au cours des cinq prochaines années[50]. On constate également, auprès des énergéticiens, la migration des technologies analogiques ou cellulaires commerciales vers TETRA, du fait d'enjeux de sécurité et d'exigences de fonctionnalités similaires à celles des forces de sécurité et de secours.
Des applications typiques sur ces marchés concernent la gestion de crise, les systèmes de contrôle-commande (SCADA), la télémétrie, la détection à distance de pannes, etc...Le déploiement futur de réseaux intelligents d'énergie (smart grids) devrait largement faire appel à ces moyens de communication sécurisés.

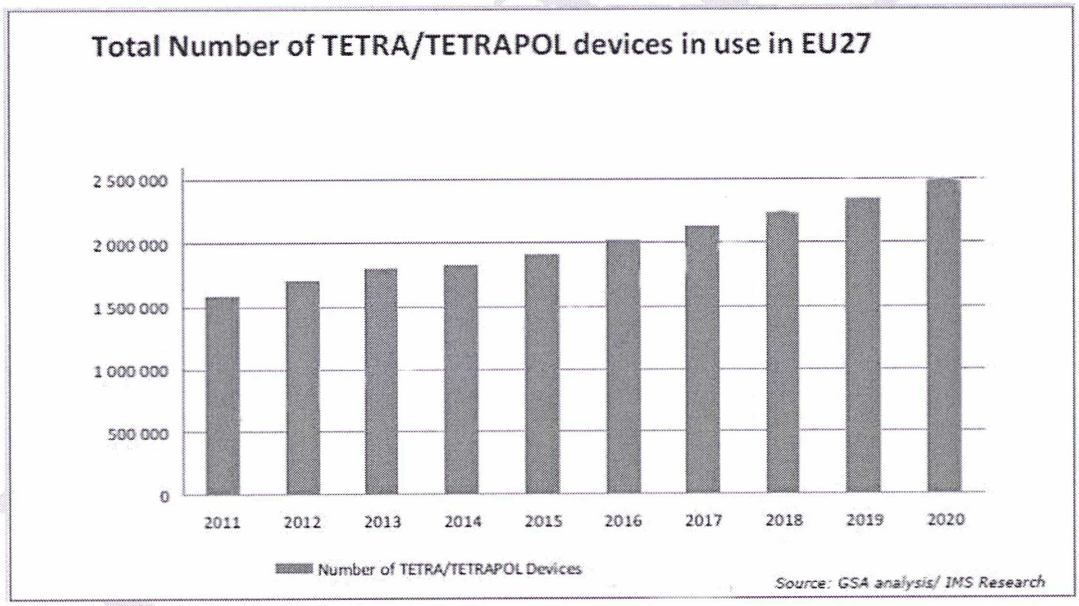
2.5.2 Un marché de niche

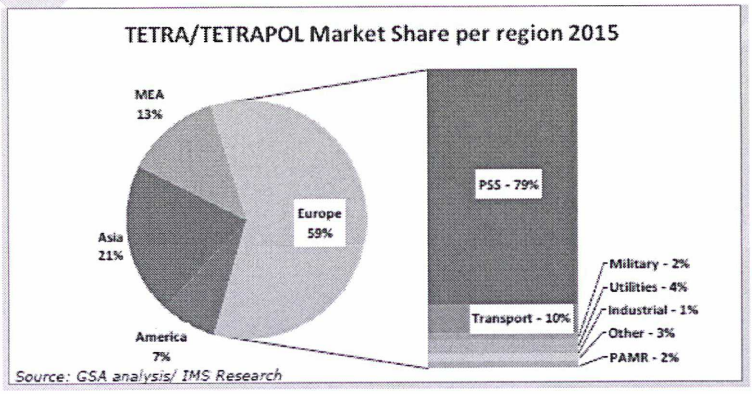
Le segment des utilisateurs de radio PMR représente aujourd'hui un marché de niche. Au plan mondial, une étude estime que la base installée comprend moins de 5 millions de terminaux, alors qu'on estimait en 2010 à cinq milliards le nombre de cartes SIM en circulation dans le monde[51]. Selon IMS Research, il y aurait environ 1,7 million de terminaux TETRA ou TETRAPOL en service au sein de l'Europe des 27, ce qui représente la proportion la plus importante dans le monde pour ces technologies. La situation devrait rester relativement stable au cours des prochaines années (voir figure ci-dessous). En France, on dénombre environ 170 000 utilisateurs au quotidien de terminaux par les forces de sécurité et de secours, contre 60 millions d'utilisateurs de cartes SIM commerciales. Ce point, estime un équipementier, indique qu'une approche au moins au niveau européen est nécessaire, car le niveau national n'est plus pertinent pour le marché de la radio PMR.

[50] Safety First, as Hazardous Working Zones Choose TETRA ATEX – Communiqué IMS Research, 18 avril 2012
[51] Cinq milliards de cartes SIM en circulation dans le monde, Les Echos n° 20719 du 15 Juillet 2010, page 13



Source: Independent research for Sepura Plc





2.5.3 Perspectives : un marché en forte croissance tiré par le numérique

Selon IMS Research[52], le marché mondial de la radio professionnelle mobile devrait croître dans les 5 prochaines années, y compris en Europe, malgré la crise économique. Ainsi, entre 2010 et 2015, le taux de croissance annuel moyen des flottes de terminaux devrait avoisiner 6%, témoignant de la dynamique du marché PMR dans cette région. Le marché PMR fait l'objet d'une reconsolidation alors que les nouvelles technologies, l'évolution de la législation et des exigences fonctionnelles nouvelles commencent à façonner l'avenir de ce secteur. En Europe, les fournisseurs d'équipements ont dû s'adapter à ces nouveaux défis et continuent de proposer de nouveaux produits ou des mises à jour (solutions numériques).

Migration vers le numérique

Après plusieurs décennies de domination, le marché de la radio mobile analogique atteint des limites au plan des innovations et entre en phase de déclin au fur et à mesure que les utilisateurs migrent vers des technologies numériques. Les équipements analogiques font probablement l'objet de l'un des derniers cycles de développement, alors que les fabricants concentrent à présent leur recherche et développement sur les équipements numériques, avec un marché de l'analogique qui n'est désormais porté que par des remplacements. L'analogique, qui permet l'établissement instantanées des communications en phonie et à faible coût, continue cependant d'apporter des réponses au marché des utilisateurs non concernés par des applications critiques.

Toutefois, la radio analogique souffre d'une autonomie de batterie limitée, d'une dégradation de la qualité de voix en limite de couverture et ne permet pas l'utilisation d'applications intégrées pour la transmission de données. Elle présente également des faiblesses liées à la sécurité des transmissions qui est nécessaire à certains utilisateurs, même s'ils ne font pas partie d'organismes de sécurité. Les évolutions technologiques dans le segment commercial ont entraîné la demande pour des applications avancées liées à la transmission de données dans l'industrie de la radio mobile. Il y avait un besoin de solution numérique structurée et standardisée pouvant satisfaire aux demandes du marché, mais sans conduire aux coûts des systèmes les plus avancés conçus pour les besoins des organismes de sécurité. La radio mobile digitale (DMR) présente désormais un certain nombre d'avantages par rapport aux systèmes analogiques, à des coûts qui ne sont pas très différents.

Les technologies numériques apportent au marché les solutions et fonctionnalités attendues et il est prévu une croissance significative des technologies digitales au cours des 10 prochaines années. TETRA, la technologie européenne dominante, est à présent considérée comme mature. Cependant, il reste de substantielles opportunités de marché pour la modernisation des parcs d'équipements et pour l'augmentation des capacités des réseaux existants en termes d'accroissement du nombre d'utilisateurs, voire pour le déploiement de nouveaux réseaux dans certains pays européens.

La prochaine étape pour le marché européen concerne les services avancés à très haut débit. Concernant les technologies numériques, Motorola est leader en Europe. EADS, Sepura et Selex sont les autres acteurs les plus importants.

[52] Digital, Broadband to Drive PMR Market Demand - Thomas Lynch – IMS research (Octobre 2011)

Les dernières données d'IMS Research confirment qu'en Europe, la migration vers le numérique va non seulement se poursuivre, mais également accélérer son rythme dans les cinq prochaines années. Il est prévu que le parc d'équipement numérique en radio numérique s'accroisse de 25% fin 2010 pour atteindre 50% fin 2015, et cette tendance devrait se poursuivre. Il s'agit du plus important taux de migration de toutes les régions, y compris l'Amérique du Nord, où le déploiement du numérique a également été important.

Très haut débit

Les forces de sécurité et de secours, les transports, les industries de réseaux et d'autres secteurs d'importance vitale ont manifesté au cours des dernières années un intérêt considérable pour la transmission de données. Nombreux sont les utilisateurs, dans ces secteurs, ayant commencé à intégrer des applications liées aux données dans leurs activités au quotidien. Les technologies commerciales offrent des débits cent fois plus élevés que les derniers réseaux de radio mobile professionnelle. Ces réseaux à très haut débit ont la capacité de transformer le fonctionnement actuel de ces organismes via des applications à très larges bandes telles que la vidéo en temps réel.

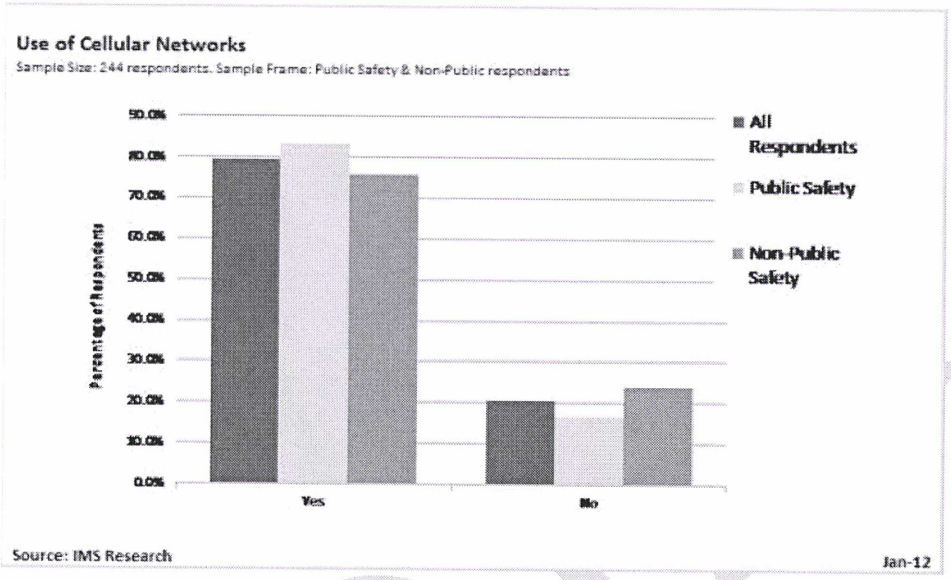
Cette situation suscite de nombreux débats au sein de l'industrie européenne de la PMR, afin de décider quelle solution sera retenue pour le très haut débit. La technologie Long Term Evolution (LTE) apparaît comme la solution favorite. Elle offre trois intérêt majeur pour les utilisateurs PPDR et les opérateurs d'importance vitale : un débit élevé, une interopérabilité native, l'instantanéité d'établissement des communications (faible latence). Le LTE a été retenu aux USA pour fournir aux organismes de sécurité des solutions très haut débit utilisées parallèlement aux applications en bande étroite (Technologie Project 25 ou P25). En Europe, il subsiste plusieurs obstacles, incluant les enjeux liés à l'harmonisation du spectre et des allocations de spectres spécifiques au marché de la radio mobile professionnelle. D'autres technologies existent, telles que la technologie TETRA enhanced data service (TEDS), mais ces systèmes sont plutôt considérés comme des solutions de moyen terme, car ils n'offrent pas de débits et largeurs de bande comparable au très haut débit.

IMS Research considère que les attentes des utilisateurs finaux à propos de la transmission des données vont accélérer l'évolution du marché vers les technologies numériques. IMS Research estime que, malgré l'avènement de la technologie LTE, les besoins des marchés traditionnels de la PMR ne conduiront pas à une rupture totale et qu'une solution hybride LTE/PMR évoluera à mesure que les standards PMR s'adapteront. De manière ultime, le succès d'une solution très haut débit pour le marché PMR européen dépendra de la capacité des régulateurs et gouvernements à allouer du spectre aux utilisateurs d'applications critiques. En outre, alors qu'un second dividende numérique est envisagé, l'harmonisation du spectre au plan européen s'avère être un facteur déterminant pour le succès du déploiement de solutions à très haut débit au cours de la prochaine décennie.

Transmission de données

Les équipementiers PMR cherchent à intégrer de plus en plus d'applications pour la transmission de données. Jusqu'à présent, le type d'application offert était très limité, l'utilisation principale de ces réseaux demeurant la voix. Traditionnellement, peu d'options étaient proposées aux utilisateurs finaux : les réseaux analogiques étant incapables d'offrir des services liés aux données, tandis que les technologies digitales les plus avancées étant trop onéreuses pour justifier le besoin et le bénéfice additionnel de l'usage de données par les utilisateurs – exception faite des organismes ayant des activités liées à la sécurité. Aussi, certains utilisateurs finaux en Europe ont fait le choix de migrer vers les réseaux cellulaires commerciaux comme second mode de

communication pour leur besoins de transmission de données. Selon une récente étude d'IMS Research, près de deux tiers des organismes utilisant des réseaux privés bas débit complètent déjà leurs moyens de communication par des terminaux de type smartphones cellulaires commerciaux[53]. Ainsi en France, la Gendarmerie nationale a opté pour une double dotation : ses agents sont équipés en terminaux du réseau dédié RUBIS et en terminaux permettant d'accéder au réseau d'un opérateur commercial.



Toutefois, la radio professionnelle mobile numérique offre une gamme significative de fonctionnalités, telles que la protection du travailleur isolé (dispositif homme-mort), géolocalisation, messagerie, appels de groupe, etc., présentant un niveau élevé de fiabilité et de sécurité demandé par les utilisateurs finaux. C'est pourquoi, à la suite de l'approche à court terme consistant à emprunter les réseaux cellulaires commerciaux pour satisfaire aux besoins de transmission de données, IMS Research prédit que les réseaux privés basés sur les technologies bandes étroites et LTE seront largement utilisés.

2.5.4 L'avenir du marché européen

Comme indiqué ci-dessus, l'avenir du marché européen de la PMR se présente favorablement. Les technologies numériques en particulier vont soutenir cette évolution, et le marché européen deviendra, s'il ne l'est pas déjà, un marché cible pour des entreprises extracommunautaires ainsi que pour les fournisseurs clés actuels.

Les applications liées aux données sont cruciales pour le succès des technologies numériques et pour le très haut débit. Le besoin d'application vidéo à très haut débit conduira au développement du très haut débit mais, pour IMS Research, le déploiement des réseaux privés LTE sera limité dans les cinq prochaines années et connaîtra un regain d'activité vers la fin de la décennie.

La migration vers le numérique, la demande concernant les données, de nouvelles méthodes de travail et l'amélioration de l'efficience constituent autant de facteurs qui feront évoluer le marché européen au cours des cinq prochaines années, in fine au bénéfice des équipementiers et des utilisateurs finaux.

[53] LMR Users Shaping the Future of Broadband PMR/LMR Data – Enquête IMS Research auprès de 261 organismes utilisant des réseaux PMR aux Etats-Unis et en Europe - Février 2012

2.5.5 Les enjeux financiers du très haut débit

Considéré comme le standard de facto pour les communications des services de sécurité et de secours très haut débit, le LTE connaît un intérêt croissant au sein de l'industrie de la sécurité. Il en résulte que les services de sécurité et de secours, et les fournisseurs investissent massivement dans les réseaux LTE avec plus de 11 attributions de contrats commerciaux (en mars 2012) et plusieurs expérimentations importantes au plan international.
Alors que ces premiers investissements s'annoncent prometteurs, il reste un certain nombre d'enjeux importants devant être pris en compte tels que l'allocation de spectre, le financement du déploiement d'infrastructures LTE dédiés à la sécurité et aux services d'urgence, la gestion des priorités pour les utilisateurs des services de sécurité et de secours empruntant les réseaux commerciaux et l'interopérabilité avec les réseaux bas débit existants tels que TETRA, APCO 25 ou TETRAPOL.

Selon une récente étude, le taux de croissance annuel moyen pour les réseaux LTE destinés aux services de sécurité et de secours est estimé à 90% au cours des cinq prochaines années, atteignant 6 milliards de dollars en 2016 contre 240 millions de dollars en 2011[54].

Ces revenus seront générés principalement par les opérateurs de ces réseaux, puis par les intégrateurs et gestionnaires de services, ce qui représente une opportunité lucrative pour les équipementiers et intégrateurs de système dans la construction, la détention et l'exploitation de ces réseaux. L'Europe restera en retrait derrière les États-Unis, le Moyen-Orient, l'Asie-Pacifique et l'Amérique latine dans l'adoption de la technologie LTE, du fait des contraintes réglementaires en matière de gestion du spectre.

2.5.6 L'augmentation des dépenses de communication des énergéticiens

Les dépenses des énergéticiens américains en équipements et services de télécommunication pourraient atteindre au moins 3.2 Md$ cette année, selon une étude publiée par le Utilities Telecom Council (UTC)[55]. Ce niveau de dépense en matière d'équipement de communication représente une augmentation de 21% par rapport aux 2.64 Md$ estimés pour 2009 et près de 3% par rapport aux 3.1 Md$ de dépenses en 2010. Les communications sans fil représentent le secteur en plus forte croissance chez les énergéticiens. Selon l'étude, les dépenses en matière de communications sans fil par rapport au total des dépenses pourraient doubler au cours des 5 prochaines années, passant de 28% du total des dépenses de télécommunication en 2011 à 50% à l'horizon de 2016.

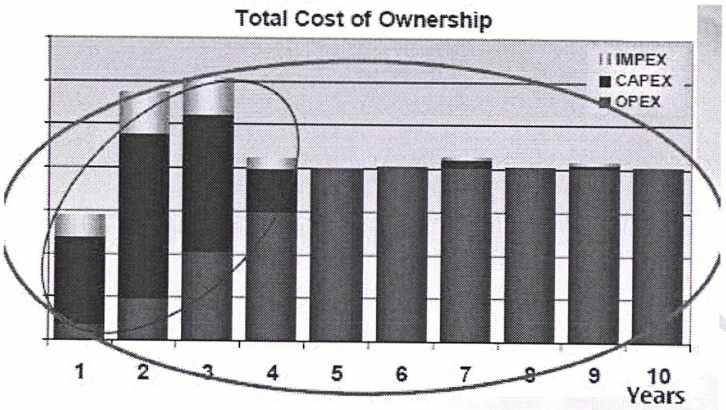
2.5.7 Quelques ordres de grandeur sur les coûts d'un réseau dédié

Dans l'absolu, une grande prudence s'impose, dès lors que l'on entend évaluer des coûts qui peuvent différer grandement d'un réseau à un autre suivant les fonctionnalités propres à chaque réseau. Néanmoins il est possible dégager quelques tendances et ordres de grandeurs pour fixer les idées.

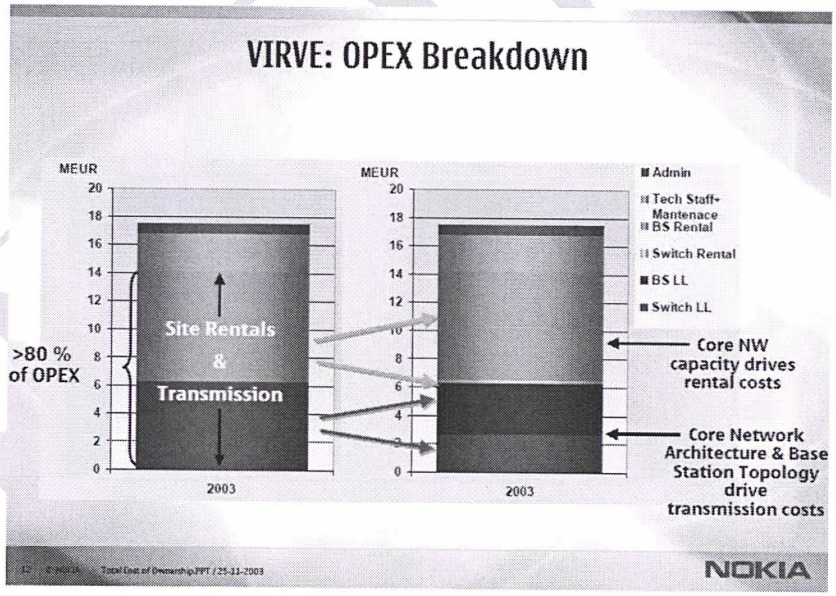
Dans les réseaux dédiés, les coûts sont essentiellement de nature fixe. Les principaux éléments de coût d'une infrastructure de réseau sont les dépenses d'investissement (CAPEX), les coûts de construction (IMPEX), et les dépenses de fonctionnement (OPEX).
Selon une étude comparative de l'équipementier Nokia datée de 2003[56], les dépenses de fonctionnement représenteraient typiquement de 50 à 80% du coût total d'un réseau sur 10 ans.

---

[54] Public Safety LTE: A Global Assessment of Market Size, Technology, Vendor Trends and Spectrum Allocation 2012 - 2016 - Mind Commerce LLC, March 2012
[55] Utilities Telecom Market Spending Forecast - Septembre 2011
[56] Measuring and managing the total cost of ownership for Tetra networks (Nokia, 2003)



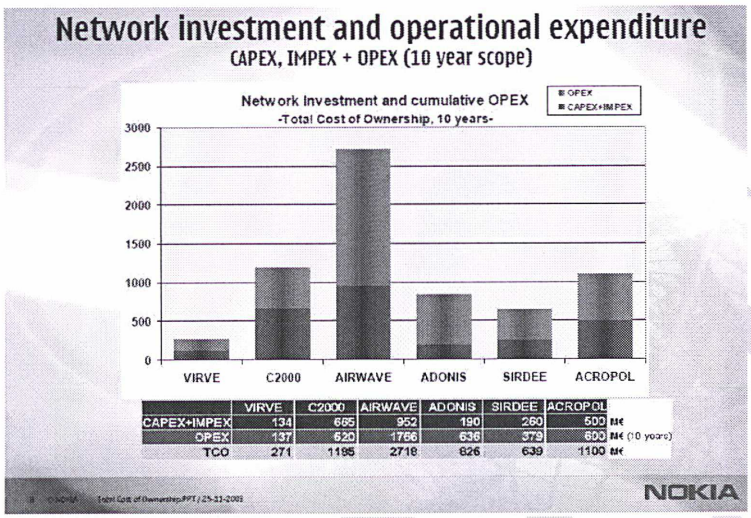
Les dépenses d'investissement et de construction du réseau couvrent les dépenses d'implémentation, les coûts d'acquisition des centres de contrôle-commande, des commutateurs, des stations de bases, et du système de gestion du réseau.
L'OPEX peut lui-même se décomposer en dépenses de maintenance et de personnels, d'énergie, et de location de sites ou de liaisons. Le coût des locations a un impact important sur les coûts de fonctionnement et est largement déterminé par l'architecture du réseau. À titre d'illustration, 80% des dépenses de fonctionnement du réseau finlandais VIRVE (TETRA) concernaient les locations de liaisons et de sites (1200 stations de base), selon Nokia, qui a installé ce réseau[57].



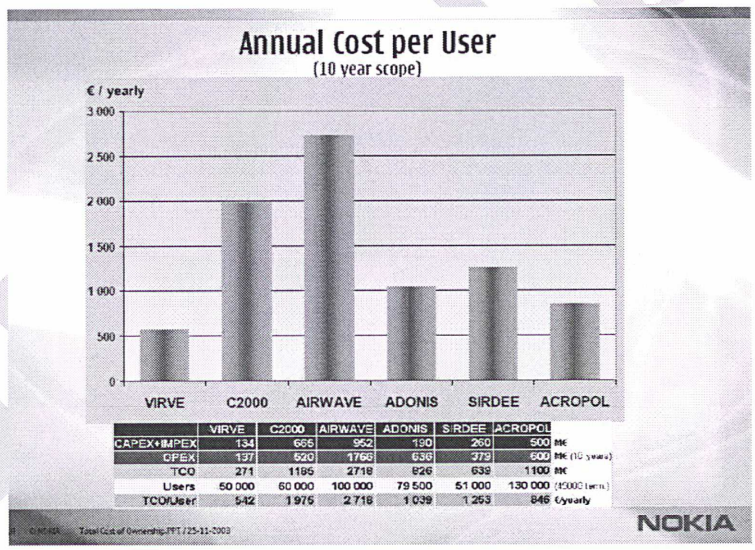
L'étude précitée présente une comparaison de la ventilation des coûts pour plusieurs réseaux PPDR européens, dont ceux du réseau ACROPOL (TETRAPOL) de la police nationale. Cette étude rappelle que les dépenses initiales d'investissement et d'implémentation du réseau ACROPOL s'élevaient alors à 500 M€, pour 390 stations de base et 130 000 utilisateurs. Les dépenses de fonctionnement devaient s'élever à 600 M€ sur dix ans, soit 38€/utilisateur/mois. Le coût total de possession s'établissait ainsi à 1100 M€ sur dix ans, soit 70€/utilisateur/mois, l'un

[57] Finnish public safety network VIRVE inaugurates two high-security Nokia TETRA features (Communiqué Nokia, 11 décembre 2003)

des coûts unitaires les plus faibles parmi les réseaux étudiés. En comparaison, le réseau britannique AIRWAVE (TETRA) revient à 226€/utilisateur/mois. Cette bonne performance résulte notamment d'une technologie TETRAPOL plus économe que TETRA en nombre de stations de base à couverture équivalente, ainsi que par un plus grand nombre d'utilisateurs.



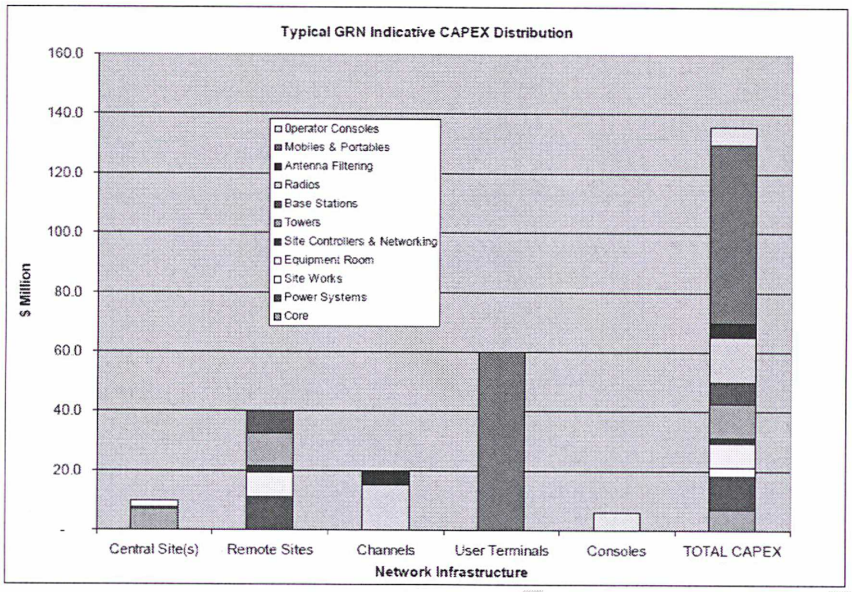
	VIRVE	C2000	AIRWAVE	ADONIS	SIRDEE	ACROPOL	
CAPEX+IMPEX	134	665	952	190	260	500	M€
OPEX	137	520	1766	636	379	600	M€ (10 years)
TCO	271	1185	2718	826	639	1100	M€



	VIRVE	C2000	AIRWAVE	ADONIS	SIRDEE	ACROPOL	
CAPEX+IMPEX	134	666	952	190	260	500	M€
OPEX	137	520	1766	636	379	600	M€ (10 years)
TCO	271	1185	2718	826	639	1100	M€
Users	50 000	60 000	100 000	79 500	51 000	130 000	(15000 terms)
TCO/User	542	1975	2 718	1 039	1 253	846	€/yearly

À ces coûts, il convient toutefois d'ajouter ceux des terminaux. À cet égard, un expert a appelé notre attention sur le poids des terminaux spécifiques utilisés jusqu'à présent par les forces de sécurité et de secours (cf. mode direct), qui représente une large part du coût complet du réseau dédié. Ainsi, dans la réponse à une consultation concernant la détermination des coûts du réseau mobile gouvernemental GRN (P25) en Nouvelle Galle du Sud (Australie)[58], Motorola met en évidence que le coût d'acquisition des terminaux mobiles et portables s'élève à près de 45% du coût total d'investissement du réseau. L'ordre de grandeur du coût d'acquisition d'un terminal se situe autour du millier d'euros. Toutefois, ce montant doit aussi être mis en regard de sa robustesse de conception et de sa durée d'utilisation pouvant atteindre plus de 10 ans.

[58] Pricing NSW Government mobile radio services (Motorola, 21 Avril 2011)



2.5.8 Les coûts de déploiement et de fonctionnement des réseaux français

Un rapport de la Cour des comptes a fait le point en 2011 sur les coûts de déploiement et de fonctionnement des réseaux utilisés par les forces de sécurité et de secours en France[59]. Selon, ce rapport, hors préfecture de police (100 ETP), les effectifs de soutien des deux réseaux sont estimés à 140 ETP pour l'INPT et 130 ETP pour RUBIS (35 au niveau national, 94 au niveau local). Les dépenses de personnels sont donc du même ordre : environ 5 M€ (ETP valorisés à 37 600 € / an, hors CAS pensions).

Le total des dépenses consacrées depuis 1994 au développement et à l'entretien de RUBIS était de 773 M€ au 31 décembre 2010, incluant le déploiement initial (448 M€), les nouveaux investissements (76 M€) et le fonctionnement (249 M€). Relativement stables ces dernières années, les dépenses annuelles de fonctionnement (hors dépenses de personnels) se sont élevés à 11,5 M€ en 2010, dont 3,5 M€ pour le maintien en condition opérationnelle et 7 M€ pour l'infrastructure (service « points hauts »).

Le total des dépenses consacrées au développement et à l'entretien d'ACROPOL depuis 1993 était de 1155 M€ au 31 décembre 2010. Également assez stables, les dépenses annuelles de fonctionnement (hors dépenses de personnels) ont atteint 108 M€ en 2010, dont 55 M€ au titre de la redevance annuelle versée à EADS, 45,5 M€ de fonctionnement et 7,5 M€ pour le maintien en condition opérationnelle du réseau, des terminaux et des faisceaux hertziens. Depuis 2009, près de la moitié de ces dépenses (43 M€) est mise à la charge de l'INPT.

Le projet ANTARES (voir § 2.4.1) a coûté environ 80 M€, dont plus de 52 M€ de renforcement de l'infrastructure. La différence (28 M€) a financé des études de conception (préalables à tout nouveau site) et le pilotage du projet. La direction de la sécurité civile (DSC) du Ministère chargé de l'intérieur est le maître d'ouvrage, la DSIC le maître d'œuvre et *EADS Cassidian* le maître d'œuvre délégué.

Les dépenses de fonctionnement (hors personnels) de l'INPT étaient en 2010 de 52,8 M€, couvrant la maintenance du système (17,3 M€), payée à *EADS Cassidian* en exécution d'un contrat pluriannuel (2004-2013) ; la maintenance des environnements techniques des relais (3,8 M€) ; les abonnements aux liaisons louées (18,5 M€) ; l'entretien (location de site, fourniture d'énergie) des « points hauts » (10,5 M€) ; diverses autres dépenses (2,7 M€)[60].

[59] La mutualisation entre la Police et la Gendarmerie nationale, Cour des comptes, tome 2 (Octobre 2011)
[60] Acquisition et migration d'une nouvelle version système, maintenance des faisceaux hertziens, etc.

Selon les prévisions, le budget de l'INPT devrait être d'environ 56 M€ par an de 2011 à 2013, mais les dépenses futures d'investissement sont incertaines ; elles dépendront, d'une part, des décisions de la DSC quant aux compléments de couverture demandés par les SDIS (Le coût des compléments de couverture nécessaires est estimé à 15 M€, mais dépendra des besoins et des moyens budgétaires de la Direction de la sécurité civile) et, d'autre part, de la volonté commune des utilisateurs de l'INPT de faire des investissements de nature à diminuer les coûts récurrents de l'INPT.

2.5.9 Un rapport de 15 à 20 en termes d'investissement dans un réseau commercial ouvert au public par rapport à un réseau dédié

Une autre comparaison utile pour fixer les idées est celle du montant des investissements entre un réseau dédié et les réseaux commerciaux ouverts au public. Interrogé à ce sujet, un consultant a indiqué que « *ce qu'a investi Bouygues télécom, c'est près de 15-20 milliards d'euros pour la construction du réseau. Et c'est un minimum, par rapport à ce qu'ont pu investir Orange-France Telecom et SFR* ». Un rapport parlementaire de 2007[61] reprenant des données de l'Autorité de régulation des communications électroniques et des postes (ARCEP) estime en effet à 28 milliards d'euros le montant cumulé de l'investissement (CAPEX, incluant le coût des licences UMTS) des trois principaux opérateurs mobiles français entre 1996 et 2006.

INVESTISSEMENT DES TROIS OPÉRATEURS MOBILES (1996-2006)

	Capex[1]	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006
SFR	en milliards d'euros	0,4	0,7	1,3	1,3	0,9	0,7	0,8	0,8	0,9	1,0	1,1
	en % du CA	53%	47%	48%	35%	21%	14%	13%	12%	13%	12%	12%
Orange	en milliards d'euros	0,6	0,8	1,5*	1,4*	0,6	0,6	0,9	0,9	0,9	0,9	1,0
	en % du CA	45%*	40%*	43%*	31%*	11%	10%	12%	12%	11%	10%	10%
Bouygues	en milliards d'euros	0,2	0,6	1,0	0,9	1,1	0,7	1,1	0,5	0,6	0,6	0,6
	en % du CA	643%	311%	163%	66%	53%	28%	37%	15%	16%	13%	13%
Total mobiles		1,3	2,1	3,8	3,6	2,6	2,0	2,8	2,2	2,4	2,5	2,7

Source : ARCEP

Dans la perspective des choix d'investissement concernant les futurs réseaux haut débit pour les forces de sécurité et de secours, la question des coûts méritera d'être approfondie. A cet égard, plusieurs études détaillées qui peuvent être utile d'un point de vue méthodologique, ont été publiées aux États-Unis à l'occasion des débats concernant leur futur réseau PPDR à très haut débit[62,63,64].

2.5.10 Les partenariats publics-privés (PPP), une alternative au financement des réseaux dans un contexte d'austérité budgétaire ?

Aux États-Unis, le Super Committee chargé de proposer 1500 milliards de dollars d'économie de dépenses publiques à l'horizon de 2021 a fait l'objet d'un lobbying intense afin que des crédits puissent être maintenus pour financer le futur réseau PPDR à très haut débit.

De nombreux réseaux dédiés ont été financés par un PPP, comme c'est le cas en France pour déploiement final de l'INPT. Dans son rapport, la Cour des comptes rappelle que l'État a conclu en 2004 avec EADS [en partenariat avec la banque BNP] un marché pour louer, pendant neuf ans, le droit d'usage d'une partie du réseau ACROPOL moyennant le paiement d'une redevance fixe

[61] « DIX ANS APRÈS, LA RÉGULATION À L'ÈRE NUMÉRIQUE » , Rapport d'information n° 350 (2006-2007) de M. Bruno RETAILLEAU, fait au nom de la commission des affaires économiques, déposé le 27 juin 2007

[62] Quantifying the Costs of a Nationwide Broadband Public Safety Wireless Network (Carnegie Mellon University, 9 janvier 2008)

[63] The public safety Network a new model for capacity, performance and cost (FCC, Juin 2010)

[64] A BROADBAND NETWORK COST MODEL (FCC, Mai 2010)

annuelle et de diverses dépenses complémentaires (dépenses de fonctionnement et de maintien en condition opérationnelle). Ce marché comporte une option d'achat du réseau par l'État pour un euro symbolique à son expiration, à la fin de 2012. A partir de 2013, le coût de fonctionnement du réseau ACROPOL devrait donc être allégé du montant de la redevance (55 M€).

Au Royaume-Uni, le réseau Airwave a été financé par un PPP, comme en Allemagne où Alcatel-Lucent exploitera pour 10 ans le nouveau réseau dédié numérique BOSNET en cours de déploiement[65]. En Nouvelle-Zélande, il est question d'un PPP concernant l'augmentation de la couverture du réseau existant[66].

Dans le domaine des opérateurs d'importance vitale, le plus gros PPP en France est celui signé avec RFF qui finance son réseau GSM-R en partenariat avec l'opérateur de télécom SFR, le spécialiste du des travaux publics Vinci et l'assureur Axa. Il s'agit du premier projet PPP de RFF, signé en 2010. Ce projet de télécommunications est mis en œuvre grâce à un contrat de partenariat (CP) de 15 ans, pour une valeur d'investissement d'environ 1 milliard d'euros. RFF est l'une des principales autorités ayant recours au PPP en France.
Toujours dans le secteur ferroviaire, Adif, le gestionnaire d'infrastructure ferroviaire espagnol, a attribué au consortium emmené par Alstom un contrat d'environ 280 millions d'euros pour la fourniture, l'installation et la maintenance sur 20 ans des systèmes de signalisation et de télécommunication de la ligne à grande vitesse qui reliera Albacete et Alicante[67].

Les partenariats public-privé (ci-après « PPP ») diffèrent des modes classiques de commande publique à plusieurs titres. Dans le cadre d'un PPP, le secteur public et le secteur privé collaborent pour réaliser des projets d'infrastructures publiques. La justification du recours à un PPP plutôt qu'aux autres modes de commande publique repose sur l'idée généralement acceptée selon laquelle un partage optimal des risques entre les partenaires public et privé engendre un bilan coûts/avantages (critère dit de l'efficience ou de la « value for money ») plus favorable pour le secteur public et, in fine, pour la société.

Dans un marché public traditionnel, le gouvernement supporte généralement tous les risques associés au projet. Dans le cadre d'un PPP, les risques et responsabilités sont supportés par les parties qui sont les mieux à même de les gérer. Par exemple, les risques associés à la construction, aux coûts, au calendrier et à la livraison du projet sont typiquement portés par le secteur privé dans le cadre d'un PPP. Le PPP encourage également à l'innovation, à l'abaissement des coûts tout au long du cycle de vie du projet, et offre généralement une qualité de service supérieure pour le public.
Les avantages clés pour un PPP incluent (i) le bénéfice pour le secteur public d'une garantie sur la date de livraison et les coûts du projet, (ii) le transfert du secteur public vers le partenaire privé de plusieurs risques clés, (iii) la prévisibilité des budgets sur le long terme, et (iv) la définition et le contrôle de la disponibilité de la structure de paiement par le secteur public et le respect de normes et d'exigences minimales en l'absence desquelles il peut être mis un terme aux accords de concession, avec des conséquences financières significatives pour le secteur privé. Les PPP peuvent être intégralement financés par le secteur privé (à la fois par des dépenses en capital ou par la dette), tout en prenant en compte les financements publics pouvant être disponibles.

[65] Alcatel-Lucent to operate the digital radio communication system for all German security authorities and organizations (Communiqué de presse Alcatel-Lucent du 22 mars 2010)
[66] Govt mulls digital radio communications network, Stuff.co.nz, 17 juillet 2012
[67] Alstom fournira le système de signalisation de la ligne à grande vitesse espagnole entre Albacete et Alicante – Communiqué du 11 janvier 2012

Les PPP sont toutefois plus complexes que les modes dits « classiques » de commande publique. Ils requièrent une préparation et une planification détaillées, ainsi qu'une gestion adaptée de la phase de passation du contrat permettant de stimuler la concurrence entre les candidats.

Le développement des PPP en France a soulevé un certain nombre de critiques, en particulier des architectes et des PME. Cette critique est en grande partie alimentée par la domination de facto de grandes entreprises (majors). Les difficultés rencontrées sur quelques projets de PPP (par exemple, le Centre hospitalier Sud-Francilien), ont renforcé ces critiques.

Selon la Mission d'appui aux partenariats publics-privés, bien que la pratique française du PPP soit encore relativement jeune, les projets de PPP semblent avoir été majoritairement livrés conformément aux attentes[68].

La procédure d'attribution des PPP est régie par plusieurs textes qui ont une origine européenne[69], nationale[70], ou sectorielle.

L'utilisation d'un CP pour un projet est principalement encadrée par l'ordonnance sur les PPP. Une autorité adjudicatrice peut opter pour un CP si au moins l'une des trois conditions suivantes est remplie :
- le projet est complexe (la complexité se pose en particulier lorsque l'autorité n'est pas en mesure de définir « seule et à l'avance » les moyens techniques, financiers ou juridiques les plus adaptés au projet)
- le projet est urgent
- le Contrat de Partenariat apparaît à l'issue d'une analyse comparative comme présentant un avantage économique au regard d'autres modes d'acquisition (critère dit « du bilan »).

Concernant ce dernier point, un équipementier nous a rappelé qu'un modèle PPP avait été initié aux USA dans le cadre du spectre identifié dans la bande des 700 MHz, appelé le bloc D, mis aux enchères en 2007. L'État américain a demandé aux opérateurs de se manifester sur ce bloc de fréquences de 2x5 MHz, en imposant un certain nombre de conditions, en particulier la préemption des ressources radio pour servir les forces de sécurité en cas de besoin. Le gouvernement américain avait émis un prix de réserve ; au cours des enchères, ce prix de réserve n'a jamais été atteint. Les opérateurs ont fait leur calcul financier et ils se sont rendus compte que ce n'était pas financièrement rentable pour eux.

Pour un expert du ministère chargé de l'intérieur, les frais financiers associés à un PPP peuvent être conséquents. Un établissement financier se rémunère assez logiquement en contrepartie des montants avancés. Sur la durée, le PPP peut aussi se révéler n'être pas si attractif, et présenter également une certaine rigidité. Les contraintes budgétaires se traduisent par beaucoup d'à-coups. On peut avoir des années relativement fastes, suivies de périodes de disette plus fortes, plus marquées et, lorsqu'on est engagé sur un PPP, la marge de manœuvre est automatiquement répercutée sur les secteurs qui ne sont pas liés par un PPP. Les responsables du programme au sens de la loi organique relative aux lois de finance (LOLF) peuvent se considérer un peu dépouillés de leurs prérogatives au sens LOLF. Mais c'est une solution possible, potentiellement parmi d'autres, estime cet expert.

[68] Cadre institutionnel & Unités de PPP, monographie de la Mission d'appui aux partenariats publics-privés - avril 2012
[69] La Directive 2004/18 de Mars 2004 concernant les travaux publics, l'équipement et les contrats de service, et la directive 2004/17 de Mars 2004 concernant les marches publics dans les secteurs de l'eau, l'énergie, le transport, et les services postaux.
[70] Ordonnance 2004-559 du 17 Juin 2004 et les lois de 2008 et 2009 qui l'ont modifiée et complétée.

On responsabilise quand même celui qui a engagé l'investissement : c'est le bon côté des choses, indique-t-on chez RFF. Le PPP a mis de la rigueur dans la gestion du projet GSM-R. Les pénalités sont lourdes en cas de manquements aux obligations, ce qui pousse les partenaires à faire preuve d'un plus grand professionnalisme.

Cela peut être une voie à creuser pour le futur, conclut un équipementier.

À noter que les futures émissions obligataires de l'UE, ou projects bonds[71], pourront permettre la mise en place de partenariats publics-privés pour le financement d'investissements prioritaires (énergie, transport, technologies de l'information et de la communication). Il vaudrait la peine d'examiner l'éligibilité des futurs projets de réseaux PPDR à ce nouveau type de financement, afin d'accélérer leur déploiement et leur interopérabilité au plan européen.

2.6 Retour d'expérience : un bilan contrasté

Dans le cadre de ce mémoire, nous avons souhaité faire le point sur le retour d'expérience du fonctionnement des réseaux utilisés par les forces de sécurité et de secours et des opérateurs d'importance vitale. Nous avons ainsi passé en revue un certain nombre d'événements pour lesquels nous nous sommes intéressés au comportement de ces réseaux et de leurs utilisateurs au plan technique, organisationnel et humain. Cet examen s'intéresse au comportement en fonctionnement de routine, lors d'événements programmés (manifestations publiques) ou de situations imprévues (catastrophes naturelles, industrielles ou d'origine humaine).

Malgré certaines situations où les réseaux sécurisés ont parfaitement fonctionné selon les équipementiers, il ressort de notre analyse un bilan plutôt contrasté. En effet, nous retenons de cette analyse les principaux constats suivants :

- La réactivité des équipementiers de réseaux dédiés (Séisme en Nouvelle Zélande en Février 2011) ;
- La mobilisation des équipementiers et opérateurs pour renforcer la résilience des réseaux dédiés à l'occasion de grandes manifestations programmées (réunions du G8/G20) et pour intervenir en cas de problème ;
- La survivabilité élevée des réseaux de communication des opérateurs d'importance vitale (Ouragan Katrina en 2005, inondations du Var en 2010) ;
- La vulnérabilité aux phénomènes naturels extrêmes des réseaux dédiés, aussi bien que des réseaux commerciaux (Ouragan Katrina en 2005 aux USA, tempêtes « Klaus » en 2009, « Xynthia » et inondations dans le Var en 2010, tempête « Dagmar » en 2011, séisme et Tsunami au Japon en Mars 2011), avec 80% de défaillances liées à des pertes d'alimentation électrique ;
- Des difficultés de gestion des fortes concentrations locales d'utilisateurs, entraînant la congestion voire la paralysie des réseaux (manifestations anti-CPE de 2006, carnaval de Notting Hill en 2007 au Royaume-Uni, Crash d'un avion de la Turkish Airline aux Pays-Bas en Février 2009) ;
- Des difficultés d'interopérabilité lors d'une catastrophe qui impactent la gestion de crise (attentats du 11 septembre 2001, ouragan Katrina aux USA en 2005) ;
- Le rôle des facteurs organisationnels et humains dans la gestion des communications et l'utilisation des équipements (Crash de l'avion de la Turkish Airline aux Pays-Bas en Février

[71] Le project bond n'a aucun impact sur la dette publique, il s'agit d'obligations émises par des sociétés créées dans le seul but de construire et exploiter un ouvrage, mais bénéficiant d'un « rehaussement de crédit » de la part de la Commission européenne et de la Banque européenne d'investissement.

2009, catastrophe ferroviaire d'Åsta, controverse sur l'utilisation des messages de statut au Royaume-Uni, attentats du 11 septembre 2001) ;

- Le manque de formation et de préparation à la gestion des crises (Ouragan Katrina, Crash de l'avion de la Turkish Airline aux Pays-Bas) ;
- Le risque de défaillance de mode commun (défaillance d'un composant électronique, et mise à jour périodique d'un logiciel d'exploitation du réseau C2000 au Pays-Bas) ;
- Des difficultés concernant la continuité des communications à l'intérieur des édifices (tunnel Mont blanc, métro de Londres) ;
- Des coûts d'utilisation parfois élevés (Réseaux Airwave, Ramage, réseaux multiples utilisés par les SAMU) ;
- Le problème de la confidentialité des communications couvertes par le secret médical (SAMU) ;
- Un investissement hâtif et un manque de préparation à l'origine de dysfonctionnements (Police de New Dehli lors de Jeux de Commonwealth en 2010) ;
- Un temps de déploiement long des réseaux (réseau Nødnett en Norvège, réseau RAMAGE à EDF) ;
- L'opposition des populations à l'implantation de nouveaux sites d'antennes (Airwave, Nødnett, Bosnet).

Ce bilan doit amener les opérateurs de réseaux de sécurité à la vigilance notamment concernant la résilience de leurs infrastructures, la formation des utilisateurs et l'ergonomie des équipements.

Dans la partie suivante, nous présentons plus en détail les événements étudiés. Ils sont classés chronologiquement, en événements survenus lors du fonctionnement en routine, lors de manifestations programmées et d'événements non programmés.

2.6.1 Fonctionnement au quotidien

Airwave et l'utilisation controversée de certaines fonctionnalités (Royaume-Uni)

Airwave Solutions Ltd a conçu, construit et exploite à présent le réseau numérique dédié PPDR britannique. Ce réseau est utilisé par la police, les pompiers et les services de secours (ambulances) – ainsi que par d'autres services d'urgence et de secours publics incluant le ministère de la défense, l'agence chargée des autoroutes, les gardes-côtes, le service des douanes et la police des transports. Le réseau Airwave fait partie de l'infrastructure nationale d'importance vitale et est conçu pour demeurer en fonctionnement lors d'événements majeurs pouvant entraîner la saturation ou le dysfonctionnement des réseaux mobiles et fixes de téléphonie ouverts au public.

Airwave est né du besoin de disposer d'une plateforme nationale de communication commune à tous les services d'urgence. En effet, des difficultés inacceptables de communication ont été mises en exergue dans de nombreux rapports à la suite d'événements majeurs, tels que la catastrophe ferroviaire de Clapham en 1988, ou antérieurement, lors de l'incendie de King's Cross.

En effet, certains services n'utilisaient pas de système dédié et dépendaient des réseaux radio mobiles ouverts au public, limitant les communications à un faible nombre de personnes dans une zone géographique donnée, et ne permettant pas des communications instantanées, résilientes et avec la nécessaire fiabilité.
Les principales priorités étaient d'améliorer la couverture, la fiabilité et la sécurité pour les services d'urgence. Au-delà de cet objectif, il s'agissait de disposer d'une technologie de

communication permettant d'insuffler de nouvelles modalités de travail pour les services de sécurité publics et d'urgence, afin d'améliorer leur efficience et d'être interopérable là où cela s'avère nécessaire.

Jusqu'au déploiement d'Airwave, toutes les unités de police, de pompiers ou de secours médical et les autres services de sécurité publique acquéraient et géraient leurs propres moyens de communication. Il en a résulté une centaine de systèmes disparates, variant largement en qualité et n'offrant guère de possibilité d'interopérabilité.

Airwave Solutions est détenu par la banque d'investissement australienne Macquarie, qui l'a rachetée en 2007 à la firme de téléphonie mobile O2.
Le déploiement de l'infrastructure a démarré en 2000, après que British Telecom (BT) a remporté un marché public de 2,5 milliards de livres pour fournir un service de radio numérique sécurisé destiné à remplacer l'ancien réseau analogique des services de secours. À la suite de la scission de BT, Airwave fut transféré à O2, une entité alors indépendante. Alors que les forces de sécurité font l'objet de restrictions budgétaires importantes, la société exploitant le réseau sur lequel communiquent tous les services de sécurité connaît une augmentation massive de ses profits. Les profits d'Airwave Solutions ont même dépassé ceux du géant des communications mobile Vodafone.
En 2010, le résultat avant impôt d'Airwave s'élevait à 170 millions de Livres, en augmentation de 26% sur les 12 mois précédents. Cela représente près de 45% des 380 millions de Livres de chiffre d'affaire de la société.

Le déploiement du nouveau système de communication commun à toutes les forces de police d'Angleterre, d'Écosse et du pays de Galles a été achevé en 2005. Depuis, la base d'abonnés d'Airwave s'est accrue significativement. Des contrats ont été conclus avec les services d'incendie et de secours médicaux qui devaient migrer vers le réseau avant la fin 2010. De plus, des services tels que l'administration pénitentiaire, le service des douanes, le métro de Londres et de nombreuses autorités locales ont commencé à utiliser Airwave.

En 2010, la presse a fait état d'une polémique concernant les coûts excessifs des communications en phonie d'Airwave. Selon les médias, les officiers de police auraient alors reçu l'ordre d'envoyer des messages texte plutôt que de communiquer en phonie, en raison des coûts élevés de communication imposés par la firme possédant le réseau.[72]

Le coût des abonnements exercerait une pression forte sur le budget de la police. Selon des officiers dans une unité rurale, les pénalités imposées par l'opérateur s'élèveraient à £2 par seconde dès que le nombre d'appels dépasserait une limite pré-déterminée.
Les policiers auraient donc été invités à communiquer davantage par messages courts afin de réaliser des économies. Selon la Police, l'abonnement mensuel inclut un prix fixe pour la fourniture du service, incluant un volume prédéfini de trafic, ainsi qu'un coût variable s'appliquant en cas de dépassement de ce volume.

Aussi, dans une tentative de réduction des coûts, tous les officiers de police britannique auraient été sensibilisés à l'utilisation des messages textes qui reviennent moins cher. Certains responsables de la police auraient condamné cette évolution, évoquant les risques pour la sécurité des officiers et du public.

[72] Police told to send text messages because it is too expensive to speak on their radios, Daylymail MailOnline, 14 Novembre 2010

Les utilisateurs disposent en effet de 16 codes numériques correspondant à des touches sur leurs terminaux. En saisissant une combinaison prédéfinie de codes, ils peuvent rendre compte de leur localisation, émettre une alerte, indiquer qu'ils procèdent à une arrestation, qu'ils effectuent une pause ou qu'ils retournent à leur commissariat. L'information est transmise automatiquement à l'ordinateur de leur centre de contrôle.
En cas d'urgence, ils peuvent demander de l'aide de façon normale. Mais en routine, ils auraient été invités à privilégier l'emploi de ces messages dits de statut.
Toutefois, certains critiquent l'usage des messages de statut, une procédure qui ferait perdre du temps, distrairait les officiers et les rendrait moins sensibles aux dangers potentiels lorsqu'ils saisissent les codes sur leurs terminaux.

Pour Airwave Solutions « toutes les forces de sécurité ne prennent pas l'entière mesure des services offerts par le réseau Airwave. Les officiers et les équipes des centres de contrôle-commande utilisent souvent uniquement les fonctions radio de base. En utilisant les fonctionnalités telles que les messages de statut, ils peuvent bénéficier d'une efficacité accrue. »

Au Pays-Bas, des problèmes récurrents de fiabilité du réseau C2000 (TETRA)

Le réseau partagé entre la police, les pompiers et les services de secours soulève des interrogations récurrentes concernant sa fiabilité, notamment lors de maintenances ou de mises à jour périodiques de logiciels d'exploitation[73]. Un tel dysfonctionnement s'est produit au mois d'avril 2012 dans la région de La Haye, perturbant les communications entre police, pompiers et services de secours médicaux[74]. Les interruptions de trafic durent de 5 à 30 minutes. Ces pannes affectent l'ensemble du territoire[75]. En juillet 2011, une panne générique de plusieurs heures était survenue à Rotterdam. Selon la presse, ces pannes à répétitions suscitent le mécontentement des élus et des utilisateurs, qui peuvent mettre leur vie en danger. L'exploitant devait résoudre le problème avec les équipementiers[76,77]. Le réseau a également été affecté par la foudre[78]. En février 2012, lors de l'attaque informatique du réseau de l'opérateur mobile KPN, C2000 n'avait pas été impacté[79].

Des utilisateurs insatisfaits au SAMU

En France, les Services d'Aide Médicale Urgente (SAMU) ont un rôle essentiel dans l'accès au système de soins et dans la prise en charge des demandes des soins non programmés. La loi du 13 août 2004 relative à la modernisation de la sécurité civile impose la migration des systèmes de radiocommunication des SAMU vers le réseau numérique ANTARES, interopérable avec les radiocommunications des services de sécurité civile (police et services départementaux d'incendie et de secours – SDIS). Cette migration doit se réaliser pour les SAMU en parallèle du déploiement du système pour les SDIS.
Les échanges entre les centres de réception et de régulation des appels d'urgence (CRRA 15) et les moyens mobiles médicaux et sanitaires déployés pour intervention sur le terrain constituent un des éléments essentiels de l'activité des SAMU. Ces échanges entre le CRRA et les unités mobiles, notamment les unités du SMUR, des sapeurs-pompiers et des transporteurs sanitaires, s'appuient sur des équipements de transmission radioélectriques qui apportent les capacités d'échanges en situation de mobilité.

---

[73] La panne géante du 6 juillet 2012 ayant affecté en France le réseau mobile d'Orange a également été occasionnée par une mise à jour logicielle pouvant avoir une origine liée au facteurs organisationnels et humains. Une panne similaire était survenue en 2004.
[74] Storing C2000 regio Haaglanden, De Telegraaf, 2 Avril 2012
[75] C2000 hapert in hele land, De Telegraaf, 30 Juillet 2011
[76] C2000 nog steeds een ramp, De Telegraaf, 24 Octobre 2011
[77] KPN network causes communication problems for C2000, Tetra applications
[78] C2000 Tetra network should be better secured, Tetra applications
[79] KPN server hacked – C2000 TETRA network never in danger, Tetra applications, Février 2012

A la suite du décret co-signé par le ministère de la santé, les SAMU adhèrent à l'INPT via le réseau ANTARES de la sécurité civile. 2000 utilisateurs sont concernés. Cependant, il nous a été indiqué au ministère de la Santé que cette solution ne donne actuellement pas entière satisfaction. Fonctionnellement, l'INPT ne répond pas aux besoins quotidiens des SAMU, pour le ministère. Les utilisateurs sont confrontés à des problèmes d'interopérabilité lors de déplacements interdépartementaux. De plus, l'INPT ne permet actuellement pas la transmission de données souhaitées par les urgentistes. De fait, chaque SAMU développe ses propres outils en utilisant les réseaux 3G commerciaux. Concernant l'utilisation des réseaux commerciaux, un rapport de l'observatoire régional des urgences de Midi-Pyrénées[80] pointait les limites des solutions opérées : l'inconvénient majeur de s'appuyer sur des réseaux opérés est qu'ils n'apportent ni priorisation des communications d'urgence, ni maîtrise des infrastructures (niveau de sécurisation inconnu, saturation possible des ressources radio).
Ces dispositions ne permettent pas de garantir le niveau du service radio en cas de crise ou de situation exceptionnelle, estiment les auteurs. Bien que la confidentialité des communications constitue un avantage en matière de transmission de données médicales, le mode de fonctionnement (communication point à point, absence de communication et de fonctions de groupe, appel par numérotation non immédiat) n'est pas spécifiquement adapté aux échanges d'un service d'urgence.
Dans ces conditions, le ministère nous a fait part de ses interrogations sur la gestion d'une crise majeure. Les SAMU souhaiteraient disposer de fréquences supplémentaires de manière à garantir la confidentialité des données médicales.
En terme de coût, la contribution forfaitaire du ministère chargé de la santé (aux frais de fonctionnement) s'élève annuellement hors investissement à 600 k€ et sera réévaluée en 2014 (soit environ 300€/terminal/an). Ce montant a été arrêté en se basant sur la contribution demandée aux SDIS. Le ministère continue cependant d'assurer le financement en parallèle du réseau RISC en Ile-de-France et PSN II hors région, utilisé sur la bande des 150 MHz par de nombreux ambulanciers qui ne sont pas autorisés sur le réseau ANTARES pour des raisons de sécurité.

2.6.2 Événements lors de manifestations programmées

Paralysie du réseau Acropol lors des manifestations anti-CPE (Paris, Mars 2006)

Pour encadrer les manifestations contre le contrat de première embauche (CPE), les autorités avaient mobilisé d'importantes forces de sécurité en mars 2006. Un expert nous a appris qu'à cette occasion, un défaut de coordination a conduit à augmenter au dernier moment le nombre d'utilisateurs enregistrés sur le réseau Acropol en Ile-de-France au-delà de ses capacités maximales d'hébergement. Cette situation a entraîné une panne géante qui a paralysé le réseau. L'intervention rapide de l'équipementier a permis de rétablir la situation. Des incidents similaires ont affecté le réseau PPDR Airwave au Royaume-Uni (voir ci-dessous).

Brouillage de l'INPT (Sommet de l'OTAN Strasbourg-Kehl, Avril 2009)

Des systèmes de contre-mesures électroniques peuvent être mis en œuvre pour assurer la sécurité de manifestations. Ainsi, les médias on fait état du brouillage des réseaux mobiles lors du mariage de Kate Middleton et du Prince William[81]. Selon des experts du groupe FM49, les services de sécurité américains utiliseraient fréquemment ces moyens, notamment pour assurer la sécurité des déplacements des convois présidentiels[82]. Mais ces brouillages impactent également les réseaux

[80] Rapport d'étude : SAMU et radiocommunications (Observatoire régional des urgences de Midi Pyrénées, Msys, 29 septembre 2008)
[81] Signal jamming technology will be deployed at Westminster Abbey to avoid disruptions to the royal wedding, Techweekeurope, 28 avril 2011
[82] PPDR needs for dedicated communications (operationnal situations) CEPT/FM 49, document de travail, 11 Mai 2012

dédiés. Un expert nous a ainsi indiqué que, lors du sommet de l'OTAN à Strasbourg en 2008, l'INPT aurait été affectée par la bulle de sécurité entourant Airforce One à son atterrissage à Strasbourg.

Police de New-Dehli : un investissement hâtif (Jeux du Commonwealth de 2010)

En Septembre 2008, le gouvernement local de Dehli décidait d'implanter un réseau TETRA en vue de garantir la sécurité des jeux du Commonwealth de 2010, notamment sur la base de l'expérience des jeux Olympiques de pékin en 2008. Le contrat d'un montant de 1 milliard de roupies (environ 15 M€) a été attribué au consortium HCL Infosystems Ltd – Motorola pour une période de 87 mois couvrant non seulement les jeux, mais également une période ultérieure de 7 années.

Le rapport d'audit sur les jeux du Commonwealth[83] a conclu que l'investissement dans ce réseau et le remplacement du réseau existant étaient peu judicieux compte tenu de l'absence de l'évaluation préalable des besoins de la police de Dehli (le principal utilisateur) et d'autres utilisateurs publics. Ce réseau n'était pas interopérable avec d'autres réseaux. Le déploiement du réseau ne fut achevé que quelques semaines avant le début des jeux, ce qui laissa peu de temps aux utilisateurs pour se familiariser avec les équipements. De plus, l'utilisation du réseau n'a pas pu être stabilisée au cours des jeux. La Police de Dehli s'est plainte de la mauvaise qualité des communications à l'intérieur des bâtiments et dans les espaces confinés ; cela nécessita le recours aux moyens de communication du réseau existant. L'audit a également relevé un certain flou autour du remplacement de 11000 terminaux existants par 3657 terminaux TETRA loués pour la période postérieure aux jeux (2168 – 2365 Roupies/mois), alors que les fonctionnalités utilisées ne sont, selon le rapport, que celles de simple téléphones mobiles.

D'autres difficultés de fonctionnement du réseau Airwave ont été soulevées par les utilisateurs

Malgré les améliorations apportées par Airwave, les organisations professionnelles ont fait part, lors d'une audition parlementaire en 2008[84], de leurs préoccupations concernant l'aptitude du réseau à gérer des événements de grande ampleur tels que les futurs jeux olympiques de 2012.

En 2007, lors du Notting Hill Carnival, le réseau Airwave n'aurait pas été en mesure de gérer localement une forte concentration d'utilisateurs. Il reste également d'importants problèmes concernant les communications des services d'urgence dans le métro. Cela a été mis en lumière lors de la tragédie de King's Cross en 1987, et ce problème ne semblait toujours pas entièrement résolu. Si Airwave peut être utilisé sur certaines lignes de métro, le déploiement reste partiel et a pris beaucoup trop de temps. 75% du métro et des tunnels sont couverts en 2008.

Selon certains experts, le volume de trafic en phonie a atteint les limites des ressources en spectre allouées au système dans certaines zones, en particulier à Londres. Cela suggère que le système Airwave sera inadéquat pour satisfaire de futurs besoins des forces de police, particulièrement dans des zones de population denses où les besoins d'information sont susceptibles d'excéder les capacités du réseau TETRA.

Airwave dispose de capacité limitées de bande passante (étroite) et de transmission de données. L'équipement existant est capable de véhiculer davantage de trafic, mais cela nécessite davantage de spectre. Selon une organisation professionnelle de la police, le réseau n'a pas fonctionné correctement lors de son déploiement initial et des problèmes persistent en termes de couverture et de fiabilité[85]. Une inspection en 2010 du Health and safety executive (HSE) auprès du service ambulancier Londonien (LAS) a révélé un dysfonctionnement des communications radio lors de

[83] Audit report on XIXth Commonwealth Games 2010, Report of Comptroller and Auditor General of India, Août 2011
[84] Policing in the 21st Century, House of Commons, Home Affairs Committee, 10 Novembre 2008
[85] Radio failures prompt safety concerns (Police magazine, Juin 2008)

phénomènes pluvieux intenses ainsi que le non fonctionnement du bouton d'appel d'urgence[86]. La presse évoque également un dysfonctionnement du réseau survenu lors des émeutes au mois d'août 2011[87,88], information démentie ultérieurement par l'opérateur d'Airwave[89] et les responsables de la police[90]. Le réseau a connu cette année de nouvelles perturbations en Écosse, à la suite de coupures de courant[91]. L'implantation de nouveaux sites d'antennes suscite par ailleurs des contestations du public[92].
Malgré ces critiques, Airwave a remporté récemment un marché public de 39 millions de Livres pour construire une extension au réseau existant à Londres et une seconde infrastructure de communication dédiée distincte (Apollo), à l'occasion des jeux olympiques et paralympiques de Londres de 2012. Du spectre additionnel a été attribué temporairement afin d'augmenter les capacités du réseau. Le renforcement du réseau a fait l'objet d'un programme d'essai intensif[93]. Le réseau semble s'être bien comporté lors des célébrations du jubilé de diamant de la reine Elizabeth II [94], ce qui est plutôt de bon augure à l'approche de l'ouverture des jeux, d'autant que le réseau public mobile O2 a connu une panne géante quelques jours après celle d'Orange en France[95].

Sommets du G8 à Deauville (Juin 2011) et du G20 de Cannes (Novembre 2011)

Le sommet G8 de Deauville a mobilisé d'importants effectifs de la police, de la Gendarmerie, des armées et de la sécurité civile. Selon un communiqué de Cassisian[96], « *10 000 utilisateurs ont ainsi bénéficié d'un puissant système de radiocommunications sécurisé sur le lieu du sommet. Pour cela, Cassidian a densifié le réseau INPT en doublant certains équipements afin de le rendre encore plus résilient en cas de crise.*
Le réseau RUBIS, quant à lui, a vu ses capacités renforcées, y compris sur la façade maritime, avec son extension OPERA, pour répondre aux besoins accrus d'échanges liés à la mobilisation de plus de 4000 gendarmes et 1700 militaires. La gendarmerie française a également déployé lors de ce sommet un réseau tactique constitué d'un système Milicor®, baptisé TOPAZE. Ce réseau a supporté l'essentiel de la manœuvre de sécurité, dans la mesure où il fédérait l'ensemble des communications des forces d'intervention (gendarmes mobiles et départementaux, patrouilles à cheval de la Garde républicaine et dispositif terrestre de protection de l'armée de terre). Outre la géolocalisation des unités de protection autour de l'aéroport de Deauville, TOPAZE a permis de projeter rapidement une bulle de communication sécurisée, densifiée et 100% disponible, exclusivement dédiée au sommet du G8 sur tous les sites sensibles : les lieux des réunions préparatoires, les lieux d'hébergement, les trajets empruntés par les chefs d'état ou encore les mouvements de foule.
Pendant toute la durée du sommet, les technologies fournies par Cassidian ont permis à l'ensemble des forces de l'ordre déployées sur place de travailler en toute confidentialité et d'assurer la protection des personnalités politiques de premier plan ainsi que celle des milliers de visiteurs et de résidents ».
Lors du sommet du G20 de Cannes en Novembre 2011, les technologies de communication hautement sécurisées de Cassidian ont à nouveau été mises en œuvre pour le maintien de la

[86] London ambulance radio system 'fails in heavy rain' (BBC News, 13 juillet 2010)
[87] Police were forced to use their own mobile phones during the August riots after their multi-billion pound radio system failed (Metro, 4 Décembre 2011)
[88] UK riots: police had to use their own mobiles (The telegraph, 4 Décembre 2011)
[89] Written evidence submitted by Airwave, HC 1456 Home Affairs Committee (Septembre 2011)
[90] Police say Airwave radio system didn't fail during riots (Publicservice 7 decembre 2011)
[91] Police radios disrupted by power cuts (Deadlinenews 4 avril 2012)
[92] Objections to plans for Tetra Goonhilly masts (Thisiscornwall, 14 juin 2012)
[93] Airwave tests 2012 Olympic PMR system at London gymnastics event (Wireless-mag, 11 janvier 2012)
[94] Airwave Network demonstrates interoperability during Jubilee celebrations (Wireless-mag, 25 juin 2012)
[95] O2 network outage raises Olympic service concerns (Reuters, 12 juillet 2012)
[96] Les technologies CASSIDIAN sécurisent avec succès le 37ème sommet du G8 en France, Communiqué EADS du 1er juin 2011

sécurité du site[97]. Il s'agissait d'assurer la protection de 20 chefs d'État et de gouvernement ainsi que des représentants de cinq pays invités et de 12 institutions internationales, comprenant au total plus de 6000 invités et environ 3000 journalistes accrédités. Au total, 12000 utilisateurs ont bénéficié du système hautement sécurisé lors du sommet. Dans cette perspective, Cassidian a adapté le réseau aux spécificités de ce type de sommets et a amélioré ses fonctionnalités pour la gestion d'une situation de crise. Outre la géolocalisation des unités en charge de la protection durant le sommet, TOPAZE a permis le déploiement rapide d'un système de communication sécurisé et densifié dédié au sommet du G20 assurant 100% de disponibilité du réseau dans tous les lieux sensibles.

Visite du Pape en Espagne (Septembre 2011)

Au cours des Journées mondiales de la jeunesse (JMJ), qui se sont tenues à Madrid en septembre 2011, les forces de police espagnoles se sont appuyées sur la technologie de Cassidian pour assurer le bon déroulement des activités et garantir la sécurité du pape et de plus d'1,5 million de visiteurs. Selon Cassidian[98], « *cette manifestation a sans doute été la mission la plus exigeante pour le réseau national de communications voix-données mobiles SIRDEE (Sistema de Radiocomunicaciones Digitales de Emergencia del Estado), étant donné la concentration de personnes à protéger. Cassidian a également participé activement à la maintenance du réseau SIRDEE et au support utilisateurs pour la Police nationale, la Garde civile, la Maison royale et le cabinet du Premier ministre. L'entreprise a par ailleurs assuré avec Telefónica un support d'urgence 24h/24.*

Le nombre d'utilisateurs du réseau SIRDEE a plus que doublé durant les périodes de pointe de la semaine des Journées mondiales de la jeunesse, sans impact négatif sur la performance réseau. Malgré une augmentation de plus de 166 % du nombre d'appels individuels et de 55 % des appels de groupe au cours des journées les plus chargées, les utilisateurs du systèmes Tetrapol ont bénéficié de l'entière disponibilité du réseau.

Plus de 10 000 agents des forces de sécurité ont assuré la sécurité du pape et des pèlerins. Outre la protection du pape et du public, les forces de police avaient la difficile mission d'assurer le maintien de l'ordre lors des manifestations anti-pape. Une salle de coordination spéciale, regroupant 40 agents de 13 organes de sécurité différents chargés de collecter les informations transmises par les forces déployées sur le terrain, avait été créée à cet effet. Les forces de sécurité se sont montrées très satisfaites du réseau SIRDEE et de l'excellente réactivité des services de communication dans une situation aussi délicate.

Les Journées de la jeunesse et la visite du pape viennent s'ajouter aux grandes manifestations sous haute sécurité qui ont requis une utilisation intensive du réseau SIRDEE pour garantir les communications hautement sécurisées lors de missions critiques. En dehors des diverses situations d'urgence telles que le séisme survenu en Espagne (voir ci-dessous) et les incendies sur Ibiza en début d'année, les forces de sécurité espagnoles se sont déjà appuyées sur le réseau SIRDEE lors du mariage royal du Prince d'Espagne en 2004.

2.6.3 Événement non programmés – Catastrophes

L'abandon du réseau RAMAGE d'EDF à la suite de la tempête de 1987 en Normandie

Un régulateur a évoqué les difficultés de fonctionnement du réseau RAMAGE d'EDF, rencontrées lors d'une tempête survenue en 1987 en Normandie, qui conduisirent ultérieurement à son abandon.

---

[97] CASSIDIAN's technology successfully secured the G20 summit in France (17 novembre 2011)

[98] CASSIDIAN a assuré la sécurité du pape lors de sa visite à Madrid à l'occasion des Journées mondiales de la jeunesse (Communiqué Cassidian du 12 septembre 2011)

Dans son ouvrage consacré à l'histoire des télécommunications au sein de l'entreprise[99], EDF rappelle avec force détails la genèse du réseau RAMAGE : au milieu des années 1970, EDF et GDF réfléchissent à la création d'un réseau radio unique, le réseau RAMAGE[100], permettant d'accompagner l'évolution de leurs réseaux de distribution et de transport et d'améliorer la sécurité des biens et des personnes en cas d'incident. C'est un réseau cellulaire qui est, en 1980, très en avance sur les idées qui prévalent en France sur les réseaux privés et même sur les réseaux radio publics. Les spécifications fonctionnelles sont rédigées par un groupe de travail multi-directions. Les terminaux RAMAGE doivent notamment permettre le raccordement automatique d'équipements de télé-conduite, l'appel de groupe, l'appel de détresse, le fonctionnement en mode direct en cas de panne du réseau. Des canaux sont attribués dans la bande des 70 MHz et 550 stations relais suffisent pour couvrir le territoire national.
Au sein du groupe de travail, certains estiment que l'on s'oriente vers un réseau trop sophistiqué et que les réseaux en place, légèrement modifiés, seraient suffisants. D'autres pensent que le réseau qui se prépare sera vite obsolète au plan technologique. Le déploiement du futur réseau est programmé entre 1986 et 1991. Au préalable, il est prévu une expérimentation en Normandie. L'appel d'offres est remporté par la société Télécommunications RadioTéléphonie (TRT), appartenant au groupe Philips. Les premiers équipements sont présentés en 1983.
Malheureusement, les essais initiaux de fonctionnement en charge sont décevants, de nombreuses fonctionnalités ne pouvant être assurées. La mise en service du réseau de Rouen en 1985 s'avère catastrophique du point de vue des utilisateurs, car la localisation d'un mobile sous le relais se fait mal et car les mises en communication sont lentes (de 20 secondes à 2 minutes alors que les spécifications prévoyaient 15 secondes). L'équipementier est sollicité pour remédier à ces difficultés. En même temps, la distribution constate que le mode d'exploitation des équipements de téléconduite du réseau électrique n'est pas compatible avec RAMAGE et nécessite des adaptations chronophages. Les tests sur le terrain des fonctionnalités sont reprogrammés en 1986. Parallèlement, le réseau est déployé au Havre et à Évreux.
En 1987, les trois réseaux de base sont en service, lorsqu'une forte tempête perturbe les réseaux électriques. Les équipes des centres de distribution fortement sollicités pour rétablir les réseaux électriques émettent de nombreuses récriminations. Les investigations révèlent que les relais ont été alimentés en permanence par le secteur ou par des groupes électrogènes et que les pylônes et antennes n'ont pas été endommagés. En revanche, certaines liaisons filaires d'infrastructures louées, réalisées en partie en aérien, ont été soumises à des séries de coupures brèves et répétitives perturbant fortement l'utilisation du réseau. Beaucoup d'utilisateurs ont été perturbés par les temps trop longs d'établissement des communications. Les utilisateurs les plus récents n'étaient pas très au fait de toutes les fonctionnalités utilisables comme l'appel de groupe. En outre, la plupart des télécommandes embarquées n'ont pu fonctionner correctement. Un régulateur ajoute que, quand EDF a dépêché ses équipes, il a fallu faire venir des postes radio d'autres régions. Lorsque ces terminaux sont arrivés, il n'a pas été possible de les connecter.
Cet épisode a marqué la fin de RAMAGE. La direction de la distribution (85% des utilisateurs) a rapidement conclu que ce type de réseau ne convenait pas bien aux besoins de ses agents en période d'incident sur le réseau électrique et qu'il était mal adapté aux transmissions de données liées à la conduite des réseaux électriques. De plus, les frais d'exploitation et d'entretien étaient considérés comme trop élevés. La plus grande part de ces frais provenaient notamment du coût des liaisons d'infrastructure louées.

La mise au point de RAMAGE a été longue. Entre-temps, l'environnement radio a changé. Les réseaux Radiocom 2000 et SFR apparaissent et, la littérature technique évoque déjà la

[99] Les télécommunications au cœur du système électrique français 1946 – 2000, EDF RTE, Editions TEC & DOC
[100] RAMAGE : sigle de réseau Radiophonique Mobile Automatique pour GDF et EDF

numérisation des futurs réseaux radio qui sera consacrée par la norme GSM pour les réseaux publics. EDF renonce à ce réseau en 1988.

Incendie du tunnel du Mont Blanc 1999 et continuité des communications dans les espaces confinés

Un consultant nous a indiqué que, depuis l'incendie du tunnel du Mont-Blanc en 1999, l'État a défini un nouveau référentiel en matière de sécurité dans les espaces confinés[101]. Ce référentiel comprend un volet radio qui préconise la mise en place de solutions permettant d'assurer la continuité des radiocommunications des services de secours dans ces espaces. Cette réglementation s'applique aux ouvrages routiers, ferroviaires ou fluviaux et à tous les espaces Recevant du Public (ERP). L'échéance pour la mise en conformité au regard de cette réglementation était le 11 février 2009 pour les ouvrages existants. Les nouveaux ouvrages doivent intégrer ces contraintes dans leur conception.

L'accident de train d'Åsta (Norvège, 2000)

Réseau Ferré de France a attiré notre attention sur l'accident de train d'Åsta, survenu le 4 janvier 2000. Un train en provenance de Trondheim a percuté un train local de Hamar sur la ligne de Røros. Cette collision entraîna une explosion suivie d'un incendie. 19 personnes furent tuées. L'absence de radio ou de système d'arrêt automatique à bord des trains sur la ligne de Røros a été un facteur contributif à l'accident d'Åsta. En effet, la seule manière de contacter les agents à bord des trains était d'utiliser le réseau de téléphonie mobile commercial Scanet ouvert au public. Or, les numéros de téléphones portables des agents de bord étaient erronés ou ne figuraient pas sur la liste des contacts du contrôleur de trafic le jour de l'accident. Au moment où le contrôleur de trafic à Hamar se rendit compte que les deux trains allaient se percuter, il n'a pas été en mesure de prévenir les conducteurs.
Alors que le fonctionnement du réseau de téléphonie mobile n'est pas en cause, cet accident appelle l'attention sur l'importance à accorder aux facteurs organisationnels et humains.
Scanet a été remplacé par la technologie GSM-Rail en 2007. Dans cette technologie, les communications sont établies à partir du numéro des trains (numérotation fonctionnelle), ce qui permet d'éviter toute confusion.
On notera également que le réseau GSM-R norvégien a fait l'objet en 2008 d'une évaluation initiale des risques à partir d'une approche socio-technique prenant en compte les facteurs organisationnels et humain[102]. Cette étude a permis d'améliorer la résilience du réseau.

Attentats terroristes contre les Etats-Unis, 11 septembre 2001

Les radiocommunications durant les attaques du 11 septembre 2001 ont joué un rôle déterminant dans la coordination des efforts de sauvetage entrepris par les pompiers de New-York, le département de police de New-York, le département de l'autorité de police portuaire et les services d'urgence médicale. Alors que les réseaux de communication des forces de sécurité avaient été modifiés pour prendre en compte le retour d'expérience des événements terroristes de 1993 au World Trade Center, les investigations concernant les radiocommunications ont révélé

[101] Décret n° 2006-106 du 3 février 2006 relatif à l'interopérabilité des réseaux de communication radioélectriques des services publics qui concourent aux missions de sécurité civile, circulaire interministérielle n° 2006-20 du 29 mars 2006 relative à la sécurité des tunnels routiers d'une longueur supérieure à 300 m, décret n° 2006-165 du 10 février 2006 relatif aux communications radioélectriques des services de secours en opération dans les ouvrages routiers, arrêté du 26 juin 2008 portant diverses dispositions relatives à la sécurité contre les risques d'incendie et de panique dans les établissements recevant du public, arrêté du 10 novembre 2008 portant définition des références techniques relatives à la continuité des radiocommunications dans les tunnels routiers, ferroviaires et fluviaux pour les services publics qui concourent aux missions de sécurité civile.
[102] Risk Assessment of Critical Communication Infrastructure in Railways in Norway, Stig O. Johnsen and Mona Veen, Norwegian University of Science and Technology, and JBV,OPM, Trondheim, Norway

que les systèmes de communication et les protocoles de chaque organisme ont été entravés par le manque d'interopérabilité, par l'endommagement ou le dysfonctionnement des infrastructures de réseau à la suite des attaques et par des intervenants des centres de contrôle-commande submergés par la gestion simultanée de plusieurs communications.
Sur le site du World Trade Center, la coordination des unités de pompiers de New-York a été fortement perturbée par le dysfonctionnement des moyens de communication : la commission nationale sur les attaques terroristes contre les États-Unis a souligné dans son rapport[103] que les interventions des pompiers ont été entravées par le mauvais fonctionnement de leurs radios à l'intérieur des tours incendiées ainsi que par la confusion concernant l'assignation des fréquences radios entre les différents personnels. Les canaux tactiques ont fait l'objet de saturation. Par ailleurs, des intervenants qui étaient en congés se sont rendus spontanément sur les lieux alors qu'ils ne disposaient pas de leur radio. Certains de ces intervenants ont pénétré dans les tours sans moyens de communication[104]. De plus, la commission a estimé que l'absence d'interopérabilité entre les moyens de communication des multiples organismes de sécurité et de secours intervenus sur le site du World Trade Center, au Pentagone, et au Somerset County (Pennsylvanie) a été un élément critique pour la gestion des événements. Cette difficulté rencontrée sur 3 sites différents a mis en évidence que la compatibilité des moyens de communication reste problématique, au niveau local, régional et fédéral. La commission a recommandé au Congrès d'adopter une disposition législative afin d'octroyer davantage de spectre pour les forces de sécurité et de secours et de résoudre la question de l'interopérabilité.

Explosion de l'usine AZF de Toulouse (Septembre 2001)

Avec l'explosion de l'usine AZF de Toulouse, le 21 septembre 2001, la France a subi l'un des accidents industriels les plus graves de son histoire. Cette usine d'engrais chimiques était en effet implantée dans la commune même de Toulouse (plus de 400 000 habitants en 2001), dans une zone industrielle située en lisière de rocade à proximité de nombreux quartiers d'habitation, d'un hôpital et d'un campus universitaire. L'explosion survenue un matin de semaine a entraîné la mort de 30 personnes et a causé plusieurs milliers de blessés. Des milliers de bâtiments ont été totalement ou partiellement détruits et toute la population de l'agglomération a été touchée directement ou indirectement. Par son ampleur et sa gravité, l'évènement répondait d'emblée à la définition que l'Organisation mondiale de la santé (OMS) donne d'une catastrophe (*disaster*), qu'elle soit d'origine industrielle ou naturelle : « Une catastrophe est un choc sévère, une rupture brutale, écologique et psychosociale, qui dépasse largement les possibilités de faire face de la communauté affectée » [OMS 2002].
L'explosion de Toulouse prend place dans ce contexte. Très vite après l'impact, le réseau de télécommunication est perdu, laissant isolés bien des intervenants essentiels ; les réseaux routiers sont largement affectés, empêchant parfois des hôpitaux de recevoir des blessés. Le professeur Christian Virenque est l'ancien chef du SAMU, désormais à la retraite. Lors du procès AZF, il a témoigné des difficultés de communication rencontrées par ses équipes. Avec des communications vite coupées et de trop nombreux blessés, il avoue que les secours ont été dépassés. « D'abord, nous avons été trahi par la télécommunication », explique-t-il. Mais surtout, « nous avons eu à faire à une catastrophe à moyens dépassés », c'est-à-dire une inadéquation entre les besoins et les moyens, poursuit-il. Des blessés ont dû attendre « plusieurs heures, voire plusieurs jours » avant d'être secourus[105].

[103] 9/11 Commission report pp. 280, 319-320, 397 (22 juillet 2004)
[104] Radio communications during the September 11 attacks, article Wikipedia
[105] Reprise du procès AZF : les secours dépassés (Interview France Info, 3 mars 2009)

Les télécommunications sont perturbées dans un rayon de 100 km, les lignes fixes et les réseaux de téléphones portables étant complètement saturés durant plusieurs heures après l'explosion[106]. A la suite d'un audit mené par le ministère de la Santé, les moyens de télécommunication ont été renforcés pour les Samu[107].
Du côté des opérateurs d'importance vitale, un responsable de RTE nous a indiqué que le dispatching de Toulouse continuait à disposer de ses moyens de télécommunications. Grâce à son réseau dédié, il demeurait relié au reste du monde alors que les autres moyens étaient inopérants.

Ouragan Katrina (USA, Août 2005)

L'ouragan Katrina, survenu lors de la saison cyclonique 2005 dans l'océan Atlantique Nord, est l'un des ouragans les plus puissants dans l'histoire des États-Unis. Environ 1836 personnes sont mortes victimes de l'ouragan et des très fortes inondations, faisant de Katrina l'ouragan le plus meurtrier depuis l'ouragan Mitch en 1998 ; les dégâts ont été estimés à plus de 81 milliards de dollars (2005). Cet ouragan est l'un des plus étendus (rayon de plus de 650 km). Il a atteint les côtes à proximité de La Nouvelle-Orléans et de Biloxi le 29 août 2005 vers 11 heures (heure locale) évitant partiellement la ville de La Nouvelle-Orléans en bifurquant au dernier moment vers l'Est. Son œil est large de 40 kilomètres et ses vents ont pu atteindre 280 km/h. Après le passage de l'ouragan, on trouva plusieurs États des États-Unis sous les eaux.
Cet ouragan a fortement sollicité la résilience des infrastructures de communication dans le secteur touché. La commission indépendante[108] chargée d'évaluer les conséquences de l'ouragan sur les réseaux de communication a observé que la plupart des infrastructures de la région avaient bien résisté à la pluie et aux vents violents, avec les dommages les plus importants constatés en zone côtière. Cependant, à la suite des inondations, la perte des alimentations électriques et des approvisionnements en carburants, l'absence de voies de communication redondantes et des coupures de lignes électriques, causées par inadvertance lors des travaux de remise en état, ont entraîné des dommages importants et étendus aux réseaux de télécommunication, engendrant de nouvelles coupures et prolongeant les délais de remise en service. Plus de 1000 stations de base étaient hors-service. La commission a également relevé :

- des instructions incohérentes données aux équipes chargées de remettre en état les infrastructures et à leurs sous-traitants concernant l'accès aux sites affectés ;
- l'accès limité aux sources d'énergie ou aux carburants ;
- le manque de systèmes de sauvegarde prépositionnés ;
- le manque de coordination entre les industriels des télécoms et les autorités locales, nationales ou fédérales ;
- l'utilisation limitée des moyens de communication prioritaires par les forces de sécurité et de secours tel que le Wireless priority service (WPS[109]) ou le telecommunication service priority (TSP[110]).

En ce qui concerne les réseaux de communication de sécurité utilisés par les forces de police, les pompiers ou les services de secours, l'ouragan Katrina a significativement affecté les fonctionnalités de ces réseaux normalement plus résilients que les infrastructures de communications commerciaux ouvertes au public. Par exemple, dans la région située autour de la Nouvelle-Orléans, plus de 2000 agents des forces de sécurité et de secours ont été contraints de communiquer en mode direct (en simplex, de poste à poste sans infrastructure relayée) en ne disposant que de 3 canaux de fréquences. En conséquence, le délai d'attente avant la prise de

[106] Explosion dans l'usine de fabrication d'engrais AZF Le 21 septembre 2001 Toulouse (Haute-Garonne) France – Fiche ARIA N°21329, Ministère chargé du développement durable – DGPR / SRT / BARPI N° 21329 ARIA, Septembre 2011
[107] AZF, une catastrophe utile ? (EspaceInfirmier.com 4 septembre 2009)
[108] Independent panel reviewing the impact of Huricane Katrina on communications networks (12 Juin 2006)
[109] Wireless priority service , US Department of Homeland security
[110] Telecommunication service priority, Federal communication commission, Public safety and homeland security bureau

parole pouvait prendre jusqu'à vingt minutes. Dans les zones les plus touchées, l'endommagement des infrastructures des réseaux de communication dédiés, ainsi que le manque d'interopérabilité, a sérieusement compliqué les interventions et a semé une forte confusion entre les responsables publics et les citoyens. En effet, l'Ouragan Katrina a remis en lumière le problème ancien d'interopérabilité entre les systèmes de communication des forces de sécurité et de secours fonctionnant dans des bandes de fréquences et avec des normes différentes.
La Commission a également souligné que le dysfonctionnement des moyens de communication des services de sécurité et de secours avait pour origine la planification, la coordination et la formation inadéquates aux technologies pouvant aider à restaurer les communications d'urgence. Ainsi, peu de services disposaient de pièces de rechange de composants clés afin de pouvoir effectuer des réparations rapides ou de systèmes redondant censés remplacer un équipement défaillant. Lorsque des moyens alternatifs de communication étaient disponibles, tels que les équipements satellitaires, le manque de formation et de connaissance des équipements, ainsi que le défaut de maintenance de ces équipements, a fortement limité l'utilisation de leurs fonctionnalités et les efforts de rétablissement de la situation. La commission souligne que les moyens de communication satellitaires, bien que pris d'assaut, ont été utilisables et ont fonctionné sur l'ensemble des zones sinistrées. 20000 terminaux satellitaires ont été déployés dans la région du Golfe. Par ailleurs, les services de secours ont semblé pâtir d'un défaut de planification concernant leurs moyens de communications d'urgence et d'un manque d'informations concernant les services et technologies permettant de satisfaire à leurs besoins critiques.
Enfin, la commission a rappelé que l'utilisation de réseaux de télécommunication pour diffuser au public de l'information relative aux situations d'urgence est de la plus haute importance. A cet égard, elle a relevé que les systèmes d'alerte d'urgence permettant de prévenir en avance les populations ou de diffuser de l'information n'ont apparemment pas été utilisés par les autorités au niveau des États et au niveau local. La commission a également stigmatisé les insuffisances concernant les moyens d'information des ressortissants étrangers ne parlant pas l'anglais et pour les personnes déficientes visuels ou auditifs.
À noter que, selon la commission, les moyens de communication des opérateurs d'énergie ont été particulièrement résilients et ont connu un taux de survivabilité élevé, s'expliquant (1) par la robustesse de leur conception devant permettre d'aider à la restauration des lignes électriques à la suite de tempêtes sévères, (2) par l'existence de systèmes de sauvegarde prépositionnés (batteries ou générateurs diesels), (3) par le fait que les liaisons de transmission sont redondantes et appartiennent aux exploitants et (4) car les personnels des exploitants sont chargés de la maintenance et des tests périodiques des matériels de sauvegarde.

Tempête Klaus (24-25 janvier 2009)

Selon un bilan des opérateurs de réseaux mobiles commerciaux ouverts au public[111], 350 000 clients mobiles SFR étaient privés de réseau après la tempête Klaus survenue le dernier week-end de janvier 2009 dans le Sud-Ouest de la France. Les coupures électriques dues à la tempête Klaus ce week-end-là ont provoqué beaucoup de dégâts, notamment dans les départements du Gers et des Landes. Privés d'électricité, les relais télécoms sont restés hors-service pendant plusieurs jours. Un tiers des clients affectés ont été rétablis 24h après la fin de la tempête. L'opérateur a mobilisé 600 personnes en vue d'un retour à la normale qui devait intervenir 4 jours après la fin de la tempête.
En attendant le retour de l'électricité, l'opérateur a utilisé des générateurs qui permettaient de faire fonctionner une partie des relais. Les autres opérateurs ont également été touchés. Ainsi, France Télécom a annoncé que 13 % de ses relais mobiles étaient encore hors service 2 jours après la fin

[111] Bilan des opérateurs télécom après la tempête (Degroupnew.com 27 janvier 2009)

de la tempête. L'opérateur a diligenté quelques mille techniciens sur place dès le dimanche 25 janvier et a installé cent trente groupes électrogènes dans les centraux les plus importants, afin de rétablir le téléphone pour un maximum de clients. Chez Bouygues Telecom, pas moins de 60 000 clients étaient encore touchés par le manque de réseau le 27 janvier.
Comme l'ensemble des réseaux de communication et de fourniture d'électricité, l'infrastructure nationale partageable des transmissions (INPT), a été affectée par la tempête. Toutefois, on apprend qu'aucun relais n'a été mis hors-service[112] ; seule une partie des artères louées à France Télécom a été endommagée, provoquant des dysfonctionnements et des interruptions de service. Dans le mois qui a suivi, la direction de la sécurité civile a tiré les conséquences de la tempête, ce qui l'a conduit à mettre en place un plan d'action visant à la sécurisation du réseau INPT.

Le centre de contrôle commande du réseau de sécurité C2000 dépassé par les événements lors du crash du Vol 1951 de la Turkish Airlines (Pays-Bas, Février 2009)

Le vol 1951 de la Turkish Airlines est un vol régulier de la compagnie aérienne nationale Turkish Airlines entre Istanbul et Amsterdam. Le Boeing 737-800 qui transportait 127 passagers et 7 membres d'équipage à bord s'est écrasé à proximité de l'aéroport d'Amsterdam-Schiphol le 25 février 2009, faisant 9 morts, 6 blessés dans un état critique et 25 blessés graves.

Cette catastrophe a eu lieu dans la région de Kennermerland, où vivent 500 000 habitants, et qui couvre la zone aéroportuaire de Schiphol, l'acierie Corus et la zone portuaire desservant Amsterdam. Près de 60 ambulances convergèrent vers les lieux de l'accident, ainsi que 600 à 700 intervenants des forces de sécurité et de secours.
Le fonctionnement du réseau sécurisé C2000 a été mis en cause lors de la gestion de cet événement. Selon le rapport d'enquête du Dutch Safety Board[113], de nombreux secouristes ont indiqué qu'il leur était impossible ou très difficile de communiquer via C2000, lorsque l'organisation d'urgence était opérationnelle sur le site environ 30 minutes après le crash.

En particulier, les urgentistes ont indiqué que les problèmes de communication avec C2000 ont perturbé les interventions concernant l'échange d'information sur le transport des victimes. En effet, le réseau a été congestionné à plusieurs reprises durant les premières heures suivant l'accident. Cette situation a fait croire à certains utilisateurs que le réseau était en panne. Certains utilisateurs se sont alors reportés sur le réseau GSM : du fait du nombre élevé de demandes de communication, les appels avaient été mis en attente et l'établissement immédiat des communications était impossible (voir figures ci-dessous). Suivant la période, le délai d'établissement des communications était compris entre 5 et 55 secondes, avec une majorité d'appels débouchant autour de 5 secondes d'attente. Selon l'opérateur du réseau de sécurité C2000, 8 stations de base ont supporté les communications. La majorité du trafic a été écoulé par la station de Halfweg.

[112] Sénat, séance du 3 décembre 2009 (compte rendu intégral des débats)
[113] Emergency assistance after Turkish Airlines aircraft accident, Haarlemmermeer, Juillet 2010

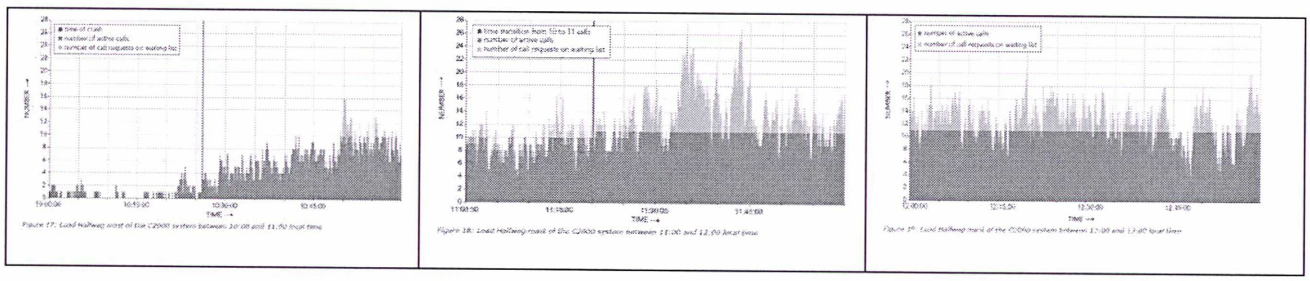


Figure : nombre de communications simultanées (bleu) et nombre de communications en attente (jaune) le 25 février 2009 entre 10h00 et 13h00 sur la station de base de Halfweg du réseau de sécurité C2000 (Pays-Bas), à la suite du crash du Vol 1951 de la Turkish Airlines

En outre, les opérateurs du centre de contrôle ont rapidement été dépassés par les événements, ne pouvant pas faire face à l'afflux des demandes de communication. Le rapport précité conclut que le dysfonctionnement du réseau sécurisé C2000 utilisé par les services d'urgence était dû à un défaut organisationnel et humain et non à une panne du réseau.

Tempête Xynthia (France, Février 2010)

Les bilans humains et matériels provoqués par la tempête Xynthia ont surpris par leur ampleur. Avec une cinquantaine de morts et des centaines de millions d'euros de dégâts, les départements de la Vendée (85) et des Charente-Maritime (17) ont été particulièrement meurtris au cours du dernier week-end de février 2010.

Aux côtés des secours mobilisés pour aider la population, France Télécom, SFR et ErDF ont dépêché dès le 1er mars des moyens et des équipes techniques pour réparer les réseaux de télécommunication et rétablir l'alimentation électrique le plus rapidement possible.

Par ailleurs, le réseau de téléphonie mobile d'Orange a été impacté en raison de la coupure de l'alimentation électrique de plus de 1 000 antennes relais. La couverture en téléphonie mobile est dégradée dans les mêmes régions mais également dans certains départements des régions Bourgogne, Champagne-Ardenne et Lorraine[114]. Plus de 2000 techniciens et spécialistes réseaux ont été mobilisés pour rétablir les communications. Orange a précisé, 48h après la tempête, que

[114] Communiqué de presse Orange du 1er mars 2010

« la situation est revenue à la normale, avec des taux de couverture à plus de 90 % dans toutes les régions ».

SFR indique pour sa part que les interventions de maintenance au cours du week-end ont permis de rétablir près des 2/3 des antennes relais mobiles impactées, 250 restant encore inactives[115]. SFR a non seulement renforcé ses équipes en charge de la maintenance de son réseau, mais aussi anticipé les éventuelles coupures d'alimentation électrique pouvant perturber le bon fonctionnement de ses équipements. Ainsi, près de 600 techniciens et ingénieurs ont été mobilisés depuis le début du week-end et plusieurs dizaines de groupes électrogènes ont également été acheminés sur les zones impactées.

Un rapport d'information du Sénat[116] rappelle que le réseau mobile français est constitué de 50 000 stations de base, qui couvrent chacune une cellule d'environ un kilomètre, reliées entre elles par des réseaux filaires. Le 27 février 2010, la tempête Xynthia a entraîné la mise hors service de 700 à 1.000 stations de base par opérateur dans quatre zones, soit une perte de service pour 700 000 à un million de clients. Le réseau a cependant été rétabli quatre jours après, alors qu'il avait fallu une semaine pour parvenir à ce résultat lors de la tempête Klaus en Gironde (2009), événement climatique de moindre ampleur. Cependant, seul un opérateur de téléphonie mobile a fonctionné correctement dans les heures et jours suivant la catastrophe, note le rapport.

La principale cause d'indisponibilité est due aux défauts d'électricité, la rupture de l'alimentation électrique représentant 80 à 85 % des incidents. Les stations de base disposent de batteries qui ont une autonomie de 2 à 3 heures, et des groupes électrogènes prennent le relais en cas de rupture du réseau électrique, ces groupes équipant des sites stratégiques. Il apparaît donc essentiel, selon le rapport, qu'une véritable coordination soit mise en place entre les opérateurs de téléphonie mobile et ERDF. Les opérateurs ne savent en effet absolument pas sur quels sites ERDF intervient en cas de crise, et ne peuvent donc implanter au mieux leurs groupes électrogènes.

A la suite de Xynthia, la direction de la sécurité civile a créé un groupe de travail rassemblant tous les opérateurs de réseaux – eau, télécommunications, électricité, hydrocarbures – afin de définir un plan ORSEC réseaux, soit les priorités de rétablissement du réseau.

Enfin, le rapport estime qu'une véritable concertation entre les services de secours et les opérateurs téléphoniques devrait être encouragée. Deux mondes semblent se côtoyer sans véritables recherches de synergies : d'une part, les fournisseurs des services de secours (EADS, Thales) et d'autre part, les opérateurs mobiles.

Un autre rapport de l'administration[117] pointe l'insuffisance de l'autonomie en énergie électrique du réseau INPT en CHARENTE-MARITIME : « *Si le S.D.S.I.S. de la VENDÉE n'a pas rencontré de problème particulier de transmissions radio, cela n'a pas été le cas de celui de la CHARENTE-MARITIME, qui a dû intervenir sur trois relais du réseau ANTARES pour en assurer l'alimentation électrique. Le S.D.I.S. a rencontré, à l'occasion de ce phénomène météorologique, les mêmes difficultés que celles déjà relevées lors de la tempête KLAUSS* ».

Du point de vue radioélectrique, le réseau ANTARES/ACROPOL n'a pas subi de dommage. Aucune rupture de faisceaux n'a été constatée sur les liaisons entre les différents relais, les concentrateurs secondaires et le concentrateur principal.

Bien que des batteries d'accumulateurs permettent de suppléer théoriquement pendant 18 heures au défaut d'alimentation en énergie, l'autonomie des relais n'a pas été suffisante pour faire face à la rupture de l'alimentation en énergie. En pratique, l'autonomie des relais serait plus proche d'une douzaine d'heures. Sur sollicitation du centre de supervision du réseau, le technicien radio du SDIS et un technicien du S.Z.S.I.C. de Bordeaux ont dû intervenir sur 3 relais pour installer des

---

[115] Les équipes de SFR mobilisées suite au passage de la tempête « Xynthia ». Des impacts réseaux essentiellement liés aux coupures électriques (Communiqué SFR du 1er mars 2010)

[116] Xynthia : une culture du risque pour éviter de nouveaux drames, Rapport d'information n° 647 (2009-2010) de M. Alain ANZIANI, fait au nom de la mission commune d'information sur les conséquences de la tempête Xynthia, déposé le 7 juillet 2010

[117] Tempête Xynthia : Retour d'expérience, évaluation et propositions d'action – rapport conjoint du Conseil général de l'environnement et du développement durable N° 00-7203-01, Inspection générale des finances 2010-M-29-02, inspection générale de l'administration 10-016-02, Inspection de la défense et de la sécurité civiles N°10-09, Mai 2010

groupes électrogènes sur les relais de Logèves, Ars en Ré et St-Pierre d'Oléron. Bien que les schelters disposent d'une prise électrique prévue pour le raccordement d'un groupe électrogène portable, pour que l'alimentation soit effective, les caractéristiques techniques du groupe doivent être suffisamment précises, notamment pour ce qui concerne la stabilité en fréquence et la tension de sortie.
Les puissances des groupes électrogènes à mettre en œuvre doivent être de l'ordre de 5 à 7 KW. À l'évidence, la consommation en énergie des relais est importante et ne peut être assurée par des dispositifs alternatifs de type panneau solaire. Dans le département de la Charente-Maritime, un panneau photovoltaïque correctement positionné produit une puissance moyenne annuelle de l'ordre de 13 W par m². Si 3 m² de panneaux permettent d'alimenter une installation radio simple, un schelter ANTARES, quant à lui, nécessiterait une surface de 100 m² pour rallonger l'autonomie de quelques heures.
À l'issue de cet évènement, il apparaît selon le rapport que :
- le réseau constituant l'infrastructure nationale partagée des transmissions (INPT) dispose d'une autonomie en énergie électrique insuffisante pour faire face à un phénomène météorologique exceptionnel ;
- le dispositif de supervision permet de détecter la perte d'énergie des relais ;
- la réalimentation des relais nécessite l'usage de groupes électrogène de qualités et de puissances suffisantes.
A défaut de dispositifs de secours automatiques, les opérations de réalimentation doivent être conduites par des techniciens compétents. »

Inondations du Var (15 et 16 juin 2010)

L'événement des 15 et 16 juin 2010 a été provoqué par des averses paroxystiques, d'un type commun à tout l'espace méditerranéen, constituant un phénomène rare par son intensité mais pas exceptionnel. Il a entraîné le décès de 23 personnes.
La mission d'enquête chargée de tirer les enseignements de cet événement[118] donne de nombreuses précisions sur l'état des moyens de communication.
Elle relève ainsi que l'organisation des secours a été affectée par la perte des réseaux de téléphonie fixe et mobile, ainsi que par l'inondation de points névralgiques du dispositif public de secours du SDIS, centre de secours principal de Draguignan. Néanmoins, les moyens engagés ont permis de sauver 2 450 personnes, dont 1 100 sauvetages au sol et 1 350 sauvetages aériens, 300 personnes ayant évité une mort certaine. La réactivité du commandement face à l'indisponibilité d'organes opérationnels majeurs a permis d'éviter des retards dans la mise en œuvre de moyens de secours nationaux et zonaux, notamment les hélicoptères. Par ailleurs, le bon fonctionnement des liaisons ACROPOL et ANTARES pendant toute la crise a été un élément déterminant.

La perte des liaisons téléphoniques fixes et mobiles : Tout au long de la crise, les liaisons téléphoniques fixe et mobile ont connu des perturbations très importantes. En soirée du 15 juin, donc au plus fort de la crise, les réseaux mobiles n'étaient plus exploitables. Des coupures intempestives étaient simultanément observées sur les liaisons de téléphonie fixe, puis le site France Télécom de Draguignan était déclaré hors service. Des pannes électriques provoquaient également des impacts sur le routeur RGT[119] de Draguignan.
L'ensemble des maires des communes ou adjoints rencontrés par la mission ont confirmé la quasi-impossibilité de communiquer par voie téléphonique, et ont rarement eu conscience de la possibilité d'adresser ou recevoir des SMS, qui semble avoir subsisté au moins en partie, comme en témoignent les échanges entre le directeur de cabinet et la sous-préfète de Draguignan.

---

[118] Retour d'expérience des inondations survenues dans le département du var les 15 et 16 juin 2010 – Rapport conjoint du Conseil général de l'environnement et du développement durable 007394-01 et de l'Inspection générale de l'administration 10-070-02 (Octobre 2010)
[119] Partie fixe du réseau du Ministère de l'Intérieur

Le réseau RIMBAUD[120] a été longtemps hors service car ses terminaux ont été noyés.

Le réseau téléphonique de la SNCF n'a jamais été coupé entre Nîmes et Alès malgré la destruction du pont de Ners. Il n'a cependant pas été utilisé par les autorités, qui ne savaient pas qu'il fonctionnait. Les réseaux de téléphone portable ont été aussi gravement perturbés : ils n'utilisent que partiellement la voie hertzienne et convergent tous vers des réseaux câblés. Tous les relais hertziens de la « région d'Alès » ont été foudroyés. Certains centraux spécialisés ont été inondés.

Le réseau satellitaire de télécommunication a fonctionné tant que les postes étaient alimentés en énergie. 2 des 3 postes de France Télécom n'étaient pas opérationnels.

Le réseau radio du SDIS a été saturé par les appels extérieurs via le CODIS, car en période de crise les standards sont liés.

L'émetteur radio de la direction départementale de la sécurité publique du Gard, situé au sous-sol, a été inondé par remontée de la nappe phréatique; les polices ont été privées de toute communication radio.

L'association des radioamateurs pour la sécurité civile (ADRASEC) a été mobilisée et a pu installer des liaisons radio en deux heures (voir encadré ci-après).

Les associations de départementales des radioamateurs au service de la sécurité civile (ADRASEC)

Ces associations régies par la loi du 1er juillet 1901 regroupent des radioamateurs motivés par la sauvegarde et qui se mettent volontairement, avec leur matériel et leur compétence, au service de la Sécurité Civile.

Chaque association est reconnue au sein d'une Fédération Nationale (la FNRASEC[121]) par la direction de la Sécurité Civile et par la Direction des Transmissions et de l'Informatique du Ministère de l'Intérieur, comme infrastructure mobile d'appoint utilisable lors d'opérations de secours se tenant à la disposition du Préfet (SIRACED-PC). La FNRASEC totalisait en 2009 un effectif compris entre 1500 et 1800 membres mobilisables en moins de 4 heures sur tout le territoire métropolitain et les DOM-COM.

Pour faciliter leur emploi, certains de ces personnels ont été placés en affectation individuelle de défense au sein de l'état-major départemental du SIRACED-PC (détachement transmission).

L'ADRASEC est gérée et activée par le SIRACED-PC et a pour mission de participer

- dans le cadre général des opérations de secours (Plan ORSEC, Plan Rouge, etc), au renforcement par des moyens spécifiques des liaisons établies par les secours publics, grâce à ses propres matériels.
- dans le cadre particulier du plan SATER (Plan Sauvetage – AéroTerrestre), à la recherche d'aéronefs accidentés ou présumés tels, par l'écoute et la localisation des signaux de détresse, grâce à leurs équipements spécifiques (radiogoniomètres).

De par leur disponibilité, leur compétence et leur dévouement, ces personnels contribuent, en étroite collaboration avec les fonctionnaires de SIRACED-PC et du SDTI (Service Départemental des Transmissions de l'Intérieur), à assurer la permanence des liaisons, pont vital pour le bon déroulement de toutes opérations mises en place pour la sauvegarde des populations.

[120] Pour "réseau interministériel de base uniformément durci". C'est le réseau téléphonique interministériel de défense
[121] Fédération nationale des radioamateurs au service de la sécurité civile (FNRASEC)

Bien que toujours considérée comme essentielle, en particulier par l'administration centrale, et notamment en cas d'avarie sur les relais de transmission, ce type d'intervention semble désormais passé au second plan, selon un rapport de l'administration[122]. Les possibilités d'interventions des ADRASEC devraient être mieux utilisées en cas de catastrophe et l'appui aux transmissions en situation de crise devrait faire l'objet d'un entraînement dans le cadre des exercices officiels. Lors de notre visite du centre opérationnel de gestion interministérielle des crises (COGIC) du Ministère chargé de l'Intérieur, nous avons pu visiter la station FNRASEC. Ses équipements permettent de contacter toutes les Préfectures du territoire Français.

Des services de secours affectés par l'inondation : Comme par le passé lors de crises semblables, des organes opérationnels majeurs se sont trouvés inondés, et se trouvaient effectivement en zone inondable. De plus, dans le Var, la mission a clairement établi que des responsables départementaux de la chaîne du secours n'avaient pas connaissance, antérieurement à la catastrophe, de l'inscription d'une partie de leurs installations en zone rouge du plan de prévention des risques d'inondation (PPRI) approuvé de Draguignan.
L'inondation du SDIS à Draguignan a impacté 160 véhicules dont 80 véhicules légers (VL). Pour mémoire, le SDIS 83 dispose de 1350 véhicules ; c'est donc plus de 10% de sa capacité qui s'est trouvée affectée. Le PC mobile a été touché et rendu indisponible, mais reste utilisable. 200 postes Antarès récemment livrés ont été perdus. Le CODIS, placé au 2e étage du SDIS, n'a pas été inondé mais rendu indisponible. Les moyens téléphoniques de transmission étaient, quoiqu'il en soit, rendus inutilisables du fait de l'indisponibilité de la sous-station électrique de Trans-en-Provence.

Le centre de secours principal de Draguignan, situé plus bas que le SDIS, a été également inondé comme à chaque crue importante, ce qui pose de manière évidente la question de sa relocalisation.

La réactivité du commandement face à l'indisponibilité d'organes opérationnels majeurs a permis d'éviter des retards dans la mise en œuvre de moyens de secours nationaux et zonaux, notamment les hélicoptères :

Le déplacement du poste de commandement opérationnel (PCO) : Face à la rupture des communications entre la sous-préfecture de Draguignan et le Centre opérationnel départemental (COD), et à l'indisponibilité des moyens mobiles de commandement, les autorités ont organisé le PCO successivement dans les locaux du centre de secours principal de Draguignan, puis dans ceux du centre commercial Carrefour « Salamandrier », dont la messagerie privée a été un temps

[122] Mission de contrôle des associations agréées de sécurité civile (Loi du 13 Août 2004 – Chapitre VI) - Rapport conjoint de l'Inspection générale de l'administration n°09-081-01 et de l'Inspection de la défense et de la sécurité civiles n°09-144 (Novembre 2009)

utilisée, enfin à l'Ecole d'application de l'artillerie (EAA) de Draguignan à partir du 16 juin. La sous-préfète de Draguignan a pu communiquer à partir du PCO par SMS avec le directeur de cabinet du préfet et ainsi solliciter, par exemple, le concours des hélicoptères.

La coordination de l'engagement aérien, notamment la communication entre fréquences civiles et militaires, a été mise en œuvre dans de bonnes conditions. Cette réussite est en partie attribuable à la présence de moyens militaires conséquents dans le Var, premier département militaire de France, moyens dont l'engagement a été directement sollicité par le préfet de département puis validé par la zone. Mais elle découle aussi du retour d'expérience de la tempête Xynthia, qui avait pointé un défaut de coordination des moyens aériens.

Le basculement des appels d'urgence : Face à l'indisponibilité des moyens de transmission du centre opérationnel départemental d'incendie et de secours (CODIS), et avec le concours de France Télécom, le basculement des communications du CODIS et des appels d'urgence sur les centres de gestion des interventions (CGI) du Luc et de Fréjus ont été assurés le 15 juin vers 19h18, ce qui a permis de fonctionner en mode dégradé avant la nuit. Toujours sur le plan téléphonique, trois valises INMARSAT supplémentaires ont pu être acheminées par la zone dans un délai de trois heures, ce qui est positif. Toutefois la mission considère que la dotation en valises du département du Var (deux dont une au standard de la préfecture) s'est révélée insuffisante.
Le contexte des risques dans ce département, ainsi que la faiblesse récurrente des réseaux de téléphonie mobile, justifierait que la sous-préfecture de Draguignan en soit dotée en permanence.
Faisant référence au retour d'expérience de la mission Xynthia, la mission s'est assurée auprès du responsable du service interministériel des services d'information et de communication de la préfecture (SISIC) que selon ce service, la maintenance de ces valises, ainsi que leur mise en œuvre par les membres du corps préfectoral, sont garanties en permanence.

La disponibilité de l'infrastructure nationale partagée des transmissions (INPT) : Le bon fonctionnement des liaisons ACROPOL et ANTARES pendant toute la crise a été un élément déterminant, dans le contexte de coupure des liaisons téléphoniques fixes et mobiles. La mission considère que des postes ANTARES devraient être mis à disposition du préfet et du sous-préfet d'arrondissement comme outils de gestion des crises. Quant au réseau RUBIS de la Gendarmerie nationale, il a subi une perturbation mais plus tardivement, le 17 juin. Il a été également signalé à la mission que le réseau radio du parc de l'équipement avait bien fonctionné, ce qui a facilité le travail de la direction chargée des routes au conseil général.

Séisme de Christchurch en Nouvelle Zélande (Février 2011)

Les réseaux terrestres et cellulaires ont tous deux été perturbés par un séisme dévastateur d'une magnitude de 6,3 qui a frappé la Nouvelle Zélande le 22 février 2011. Selon Cassidian, les forces de sécurité et de secours ont pu s'appuyer sur leur réseau dédié CORP25, qui est resté totalement opérationnel, pour la coordination des opérations de secours durant le séisme et lors de ses répliques[123]. L'épicentre du séisme se situait près de la ville de Christchurch, la seconde plus grande ville de Nouvelle-Zélande, totalisant une population de 386 000 habitants. Le séisme a endommagé des immeubles, des lignes électriques et la plupart des réseaux de communication. Dans les heures qui suivirent le séisme, les équipes de secours de tout le pays ont convergé vers Christchurch, contribuant à accroître le trafic sur le réseau CORP25 au-delà de la capacité souscrite. À la demande de l'intégrateur du réseau, Cassidian a pu porter en trois heures le nombre d'abonnés de 1700 à 2200. Deux jours plus tard, une nouvelle demande d'augmentation

[123] D'après key touch customer magazine 2/2011 p.21

des capacités pour 500 utilisateurs a pu être prise en compte en moins de vingt minutes par l'équipementier.

Le réseau CORP25 a été installé en 2008 pour la police de Nouvelle Zélande. Il gère 600 000 appels d'urgence par an et couvre actuellement trois principales régions - Wellington, Auckland et Canterbury, où est située la ville de Christchurch.
À noter que le gouvernement néo-zélandais a initié en 2010 une démarche visant à identifier les besoins futurs des services de sécurité et de secours et notamment à augmenter la couverture au-delà des trois régions précitées, à migrer leurs réseaux vers des technologies numériques et à assurer leur interopérabilité[124]. L'extension de ce réseau est toujours à l'étude[125].

Séisme et tsunami au Japon (11 Mars 2011)

Il n'a pas été possible d'obtenir d'informations très précises sur le fonctionnement des réseaux de communication utilisés par les forces de sécurité et de secours au Japon à la suite du séisme et du Tsunami de 2011. Concernant la gestion du volet nucléaire de la catastrophe, un rapport des autorités japonaises transmis à l'Agence internationale de l'énergie atomique (AIEA)[126] mentionne que sur le site, l'exploitant nucléaire TEPCO ne disposait plus de moyens de communication du fait de la perte des alimentations électriques externes. À l'extérieur du site, la police a transmis par son réseau radio aux gouvernements locaux les informations concernant l'évacuation des populations autour de la centrale nucléaire de Fukushima.
En ce qui concerne les autres réseaux de télécommunication, le Japon a publié un retour d'expérience sur l'impact de la catastrophe sur les réseaux de télécommunication commerciaux ouverts au public[127]. Ce retour d'expérience met en évidence qu'à la suite du tremblement de terre de grande ampleur du 11 mars 2011 (magnitude évaluée à 8,9 sur l'échelle ouverte de Richter), l'augmentation massive du nombre d'appels téléphoniques a causé la congestion des réseaux amenant les opérateurs commerciaux japonais à imposer des restrictions d'appels allant de 80-90% sur les lignes fixes à 70-95% sur les lignes mobiles. En revanche, les communications de données, tels que les SMS, n'ont été que peu ou pas concernées par des restrictions suivant les opérateurs, de sorte que ces communications ont mieux fonctionné que les appels téléphoniques, même si un certain délai d'acheminement des messages s'est avéré nécessaire[128].
Le tremblement de terre a entraîné un tsunami sur la côte Pacifique qui a causé des dommages considérables aux réseaux de télécommunication sur des zones très étendues, incluant la submersion des équipements à l'intérieur des bâtiments les abritant, la destruction de câbles enterrés, de câbles aériens et de stations de base. Du fait des coupures d'électricité, même les installations non directement touchées et équipées de batteries ou de diesels de secours ont rapidement été hors-service. Au total, 29000 stations de base ont été rendues inopérantes. Les dommages engendrés par ce séisme ont été plus importants et étendus qu'à l'occasion de précédents séismes. Toutefois, la restauration des infrastructures a pu globalement être achevée à la fin du mois d'avril 2011.
Le groupe de travail chargé de ce retour d'expérience a recommandé aux opérateurs d'augmenter la capacité de leurs réseaux afin de réduire les risques de congestion des appels téléphoniques à l'avenir. Le développement en cours des technologies de 4ème génération devrait contribuer à l'atteinte de cet objectif. D'autres pistes ont été suggérées, telles que la réduction de la durée des appels ou de la qualité audio des transmissions, avec à la clé des campagnes de sensibilisation des

[124] Whole of Government Plan for Public Protection and Disaster Relief Radio Communications - Emergency Telecommunications Services Steering Group (ETSSG), Avril 2010
[125] Govt mulls digital radio communications network, Stuff.co.nz, Business Day, 17 juillet 2012
[126] Report of Japanese Government to IAEA Ministerial Conference on Nuclear Safety - Accident at TEPCO's Fukushima Nuclear Power Stations Transmitted by Permanent Mission of Japan to IAEA, 7 Juin 2011, Chapitre V Response to the nuclear emergency
[127] Study group on maintaining communication capabilities during major natural disasters and other emergency situations (27 décembre 2011)
[128] State of Communication Damage and Congestion Caused by the Great East Japan Earthquake – reference material (Présentation - Juillet 2011)

usagers. Les difficultés d'acheminement des appels prioritaires rencontrés ont fait l'objet d'évaluation et les travaux devraient se poursuivre sur ce point, en particulier concernant la liste des organismes éligibles. En ce qui concerne les équipements de sauvegarde, les opérateurs commerciaux japonais se sont engagés à augmenter leur autonomie afin de la porter au minimum à 24 heures pour environ 2000 sites sur l'ensemble du territoire.

Séisme en Espagne (Mai 2011)

Les services de secours ont pu compter sur le réseau SIRDEE, a indiqué Cassidian, à la suite du séisme survenu à Lorca en mai 2011. Ce séisme d'une magnitude de 5,1 a causé des morts, des blessés et des dommages significatifs dans la région de Murcie, en Espagne. Selon l'équipementier[129] :

« Le réseau SIRDEE [...] a joué un rôle significatif dans l'organisation et la coordination des secours lors du tremblement de terre qui a ébranlé le sud de l'Espagne. Alors que les communications étaient très difficiles pour la population, en raison de l'encombrement des réseaux mobiles publics, toutes les communications par SIRDEE ont parfaitement fonctionné. Aucun problème n'a été constaté dans le réseau, et les utilisateurs ont pu s'appuyer sur SIRDEE et se concentrer sur leurs missions.

[...] Juste après le séisme, le nombre de professionnels de la sécurité publique intervenant dans le secteur a augmenté de telle manière que le nombre d'utilisateurs du réseau enregistrait une hausse de 264 %. Les communications groupées dans le réseau ont, quant à elles, triplé. Au lieu des 20 appels individuels par heure en temps normal, le système devait en traiter 128, soit une augmentation de 540 %. Le taux d'occupation des canaux est passé de 20 à 70 %, ce qui représente une hausse de 250 %.

Comme le souligne Telefonica, l'opérateur du réseau, malgré une augmentation considérable du nombre de terminaux connectés dans le secteur, SIRDEE a permis de continuer à assurer un service normal, à l'entière satisfaction des usagers. Les organismes utilisant SIRDEE ont indiqué qu'ils étaient entièrement satisfaits du niveau de service dans cette situation difficile.

Déployé depuis 2000, le réseau SIRDEE est le réseau national de communications voix-données mobiles basé sur la technologie de radiocommunication numérique sécurisée TETRAPOL de Cassidian. Outre les organismes relevant du ministère de l'Intérieur (la Guardia Civil et la police nationale), plusieurs autres utilisateurs ont adopté le réseau SIRDEE : la police routière, la famille royale, le cabinet du Premier ministre, l'unité militaire d'intervention d'urgence, la Marine nationale espagnole, la police autonome de la région Galice, la police municipale et les sapeurs-pompiers de Torrelavega, les services de protection civile de la région de Cantabrie, ainsi que les îles Baléares et la ville de Logroño ».

Attaque terroriste à Oslo et massacre d'Utøya (Norvège, Juillet 2011)

Le 22 juillet à 15h25, une bombe placée dans une voiture explosait au centre-ville devant des bâtiments du gouvernement norvégien. Immédiatement après, les forces de police, les pompiers et les services de secours médicaux se sont déployés en masse au centre-ville. Les victimes ont été évacuées vers les grands hôpitaux. Aux environs de 17h24, les centres d'appels d'urgence 110, 112 et 113 reçurent les premiers appels de détresse concernant la tuerie à Utøya. Un nouveau déploiement des forces de sécurité et de secours sur cette zone a été décidé afin d'évacuer les victimes dans les hôpitaux, de rechercher des blessés et disparus.

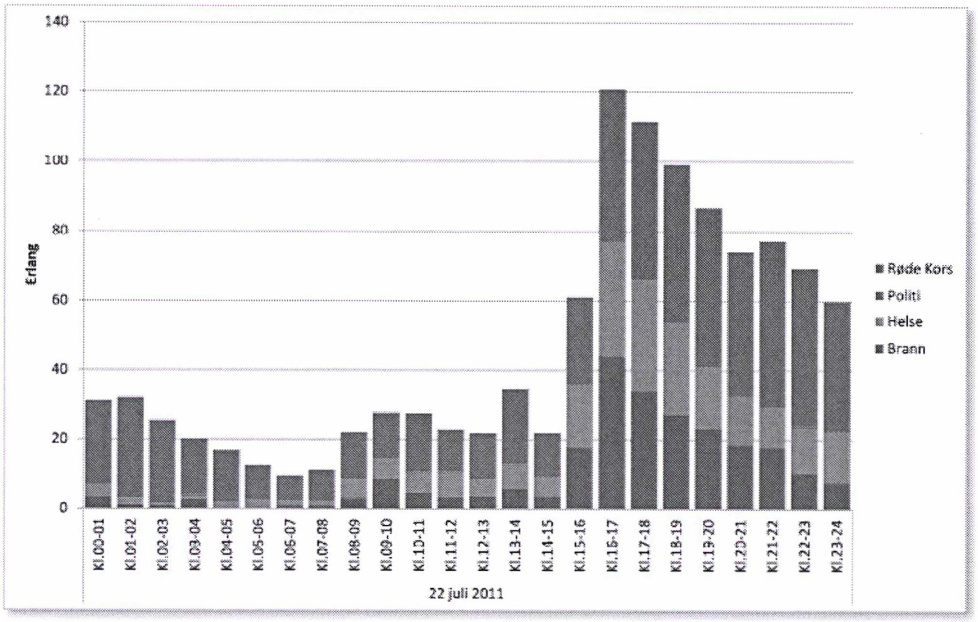
Selon les autorités, le réseau de sécurité a constitué un outil important pour coordonner les interventions de secours. Cependant, la presse a fait état de difficultés majeures de communication

[129] Séisme en Espagne : les services de secours ont pu compter sur le réseau SIRDEE de CASSIDIAN, Communiqué EADS du 28 juillet 2011

entre les services de sécurité et de secours lors de leur intervention à Utøya qui a conduit la police à utiliser des fax et e-mails[130].

En réponse, la direction des communications d'urgence (DNK[131]), qui détient et exploite le réseau PPDR Norvégien Nødnett (TETRA), a rendu public un retour d'expérience préliminaire[132] du fonctionnement de son réseau lors des attaques terroristes à Oslo et Utøya.

Ce réseau en cours de déploiement par l'équipementier Nokia Siemens Network (NSN) est alors opérationnel dans la partie Centre-Est du territoire, incluant les districts de Østfold, Follo, Romerike, Oslo, Asker et Bærum, ainsi qu'au sud de Buskerud. Il comprend 240 stations de base. Utøya situé au nord du district de Buskerud n'était pas couvert par le réseau. Aucun équipement du réseau n'a été endommagé et, selon DNK, le réseau a fonctionné normalement au cours de cet événement. DNK a bénéficié de l'assistance technique de NSN et de ses sous-traitants durant ces événements. Au centre-ville, près de 1000 terminaux Nødnett étaient en fonctionnement et moins de 300 à Sollihøgda. Le trafic global a plus que triplé après l'explosion dans le quartier des ministères. La figure ci-après présente la charge totale horaire du réseau le 22 juillet pour chaque entité utilisatrice (police, secours medical, pompiers, Croix-Rouge). Le graphique ci-après met en évidence une charge élevée à partir de 15h00 le 22 juillet qui a persisté jusqu'au 23 juillet.



Charge totale de trafic du réseau Nødnett le 22 juillet 2011
et répartition par entité utilisatrice (en Erlang[133])

[130] Politiet sendte faks under redningsarbeidet på Utøya, Bt.no 1er Août 2011

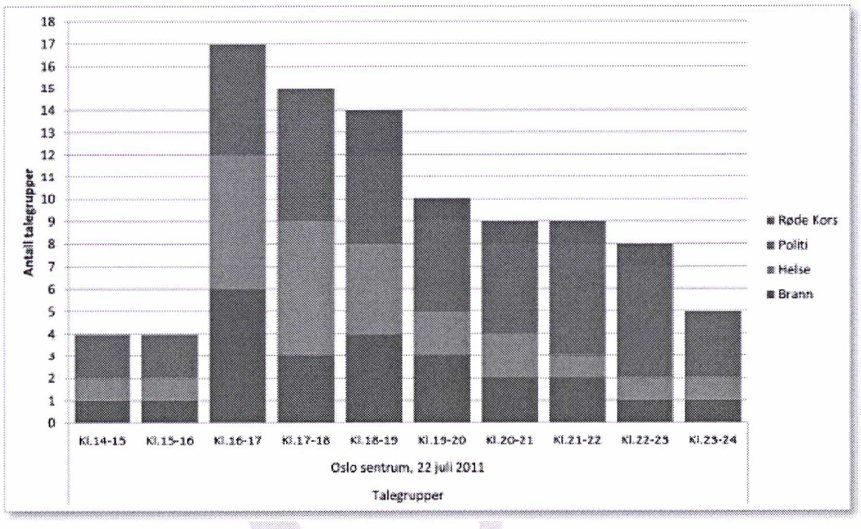
[131] DNK est responsable du développement du nouveau réseau de communication numériques pour les forces de sécurité et de secours en Norvège. Créée en 2007, cette entité dépend du ministère chargé de la Justice.

[132] Bruk av Nødnett 22. juli 2011, DNK Direktoratet for nødkommunikasjon, 8 novembre 2011

[133] Pour mesurer la charge de trafic au niveau des stations de base, il est parfois utilisé une unité de mesure standard appelée Erlang, employée dans les télécommunications et liée à l'utilisation de diverses ressources de communication au cours d'une unité standard de temps. L'erlang est une unité sans dimension qui mesure le nombre de sessions de communication et leur durée sur une période donnée. 1 erlang correspond à l'occupation maximale sur une ligne ne permettant qu'une communication téléphonique (par exemple sur une heure, 1 session de 3600 secondes ou 10 sessions de 360 secondes, ...).1 erlang correspond à une session téléphonique permanente sur la durée d'observation. 0,3 erlang correspond à 30 % de session téléphonique donc pour 1 h d'observation il y a 18 min de session téléphonique. 10 erlangs correspondent, par exemple, à une occupation de la ligne de 10 appels d'une heure simultanés sur une heure d'observation.

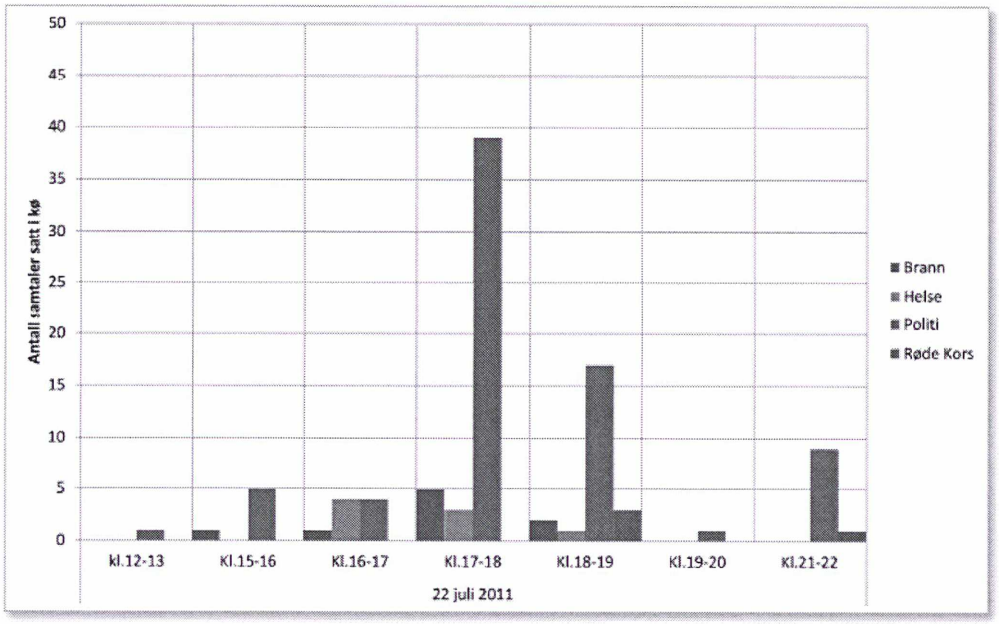
Pour DNK, les événements du 22 juillet ont démontré le caractère suffisant des capacités du réseau pour gérer une situation inhabituelle, même si la charge sur certaines stations de base individuelles a atteint parfois les limites de capacité pendant de courtes périodes.

Il n'a pas été rapporté de dysfonctionnement au niveau des équipements et les statistiques d'exploitation montrent qu'il y a eu peu de congestion du réseau en regard de l'importance du nombre d'appels. Selon les utilisateurs, Nødnett a fonctionné correctement. Cependant, il y a eu un tel trafic en groupe que certains utilisateurs ont dû patienter avant de pouvoir intervenir pour passer leurs messages. La figure ci-dessous présente l'évolution du nombre de groupes de conversation (conférences) simultanément actifs à Oslo le 22 juillet 2011. DNK précise que le bouton d'appel d'urgence a été activé à 8 reprises le 22 juillet au cours des communications de groupe afin de signaler des cas de blessés nécessitant une intervention urgente.



Nombre de groupe de conversation (conférences) simultanément actifs pendant plus d'une minute pour chaque tranche horaire, par entité utilisatrice dans une station de base au centre-ville d'Oslo le 22 juillet 2011

Par rapport au trafic total, peu d'appels ont été temporisés en raison de l'occupation des canaux. Cela n'a concerné que 0,5% du nombre total d'appels vers les stations de base en centre-ville. Sur une station de base au centre-ville proche du quartier des ministères, 4,2% des appels ont connu un délai d'attente avant d'aboutir dans les heures de trafic les plus intenses (voir figure ci-dessous). Le délai maximum d'attente était de 7 secondes et, dans 80% des cas, ce délai était de moins de 5 secondes), indique le rapport de DNK.



Nombre d'appels ayant abouti avec un délai supérieur à la normale le 22 juillet 2011

Enfin, alors que la classe politique s'est émue du délai de déploiement du réseau Nødnett [134], DNK a réaffirmé son souhait d'un achèvement rapide prévu en 2015. Motorola Solutions, sous-traitant de NSN, a été appelé à prendre la responsabilité de mener à terme les opérations. Le déploiement du réseau connaît en effet un important retard, notamment en raison de l'hostilité des populations concernant l'implantation d'antennes relais[135].

Tempête « Dagmar », Norvège, Décembre 2011

Plusieurs stations de base du réseau PPDR Norvégien Nødnett ont subi des coupures d'alimentation électrique lors de la tempête Dagmar en décembre 2011, indique l'exploitant du réseau DNK[136]. Des systèmes de sauvegarde permettent la poursuite du fonctionnement des équipements an cas de rupture des alimentations électriques. Certaines stations disposent d'une autonomie de 48 heures grâce à des groupes électrogènes diesels et des batteries, d'autres de 4 à 8 heures d'autonomie sur batterie.

Au cours des conditions météorologiques extrêmes rencontrées à Noël 2011, un certain nombre de stations de base situées dans la région centrale de Norvège ont été alimentées par leurs systèmes de sauvegarde. Pour certaines de ces stations, l'interruption du réseau électrique a été telle que les alimentations électriques de secours n'ont pas permis d'assurer la poursuite de leur fonctionnement. Cela a conduit à réduire la couverture du réseau dans certaines régions.

À la suite de ces conditions extrêmes, DNK évaluera la nécessité de nouvelles mesures pour renforcer la fiabilité du réseau. Une revue des procédures d'urgence sera également réalisée.

[134] Politikere frykter nødnettet ikke er klart i 2015 Nationen Nyheter, 21 Avril 2012
[135] Vernet skog forsinket nødnett-mast, Nationen Nyheter 4 Août 2011
[136] Enkelte basestasjoner i Nødnett ble rammet av strømutfall under ekstremværet «Dagmar», Communiqué DNK du 27 Décembre 2012

Possible piratage du contrôle-commande des trains, Nortwest Railway (Amtrak) (USA, Décembre 2011)

Selon plusieurs médias américains, l'administration américaine chargée de la sécurité des transports (The Transportation Security Administration (TSA)) aurait fait état, dans un mémo, du piratage du réseau informatique de la compagnie de chemins de fer Northwest (Amtrak) qui a perturbé les signaux de contrôle-commande des trains pendant deux jours en décembre 2011. L'attaque aurait été organisée à partir de l'étranger. Cette information a toutefois été démentie par l'association américaine des chemins de fer. Il n'est donc pas confirmé s'il s'agissait d'une cyber-attaque. Selon les médias, l'exploitant n'aurait pas souhaité communiquer sur cette affaire.

TROISIEME PARTIE

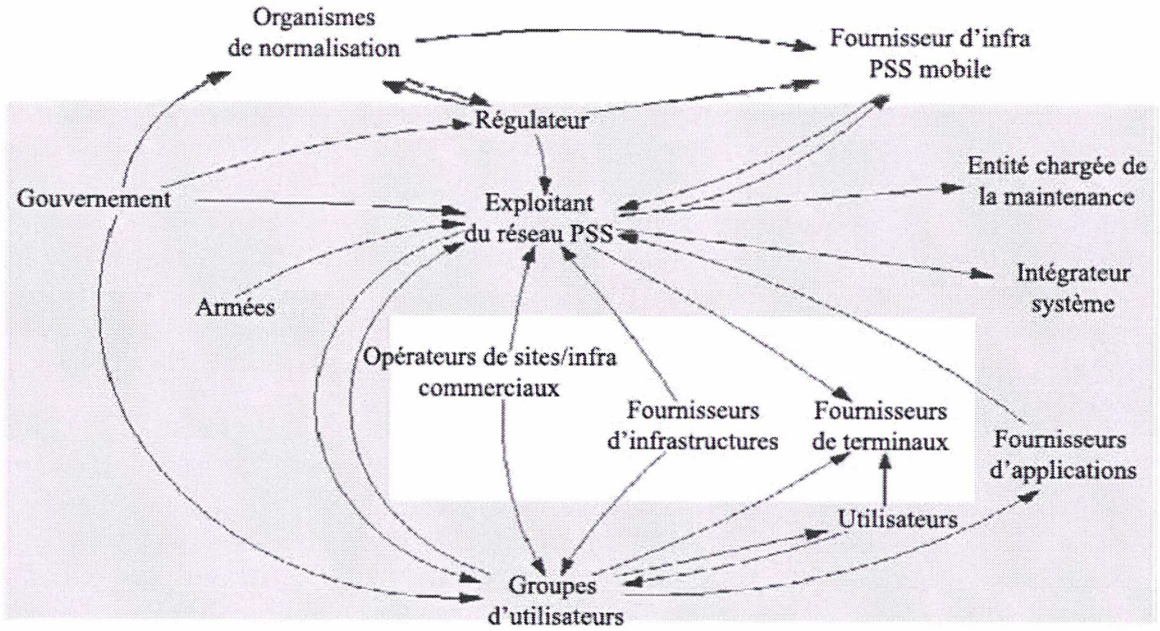
Analyse stratégique de l'évolution des réseaux PPDR

Dans cette partie, nous nous attachons à étudier les intérêts des parties prenantes principales avant d'examiner la structure concurrentielle de l'industrie concernée par le marché des réseaux de sécurité. Puis, à partir de l'analyse des forces de changement à l'œuvre aux plans économique, technologique et social, nous tenterons de dégager plusieurs axes stratégiques que nous confronterons à la position des parties prenantes.

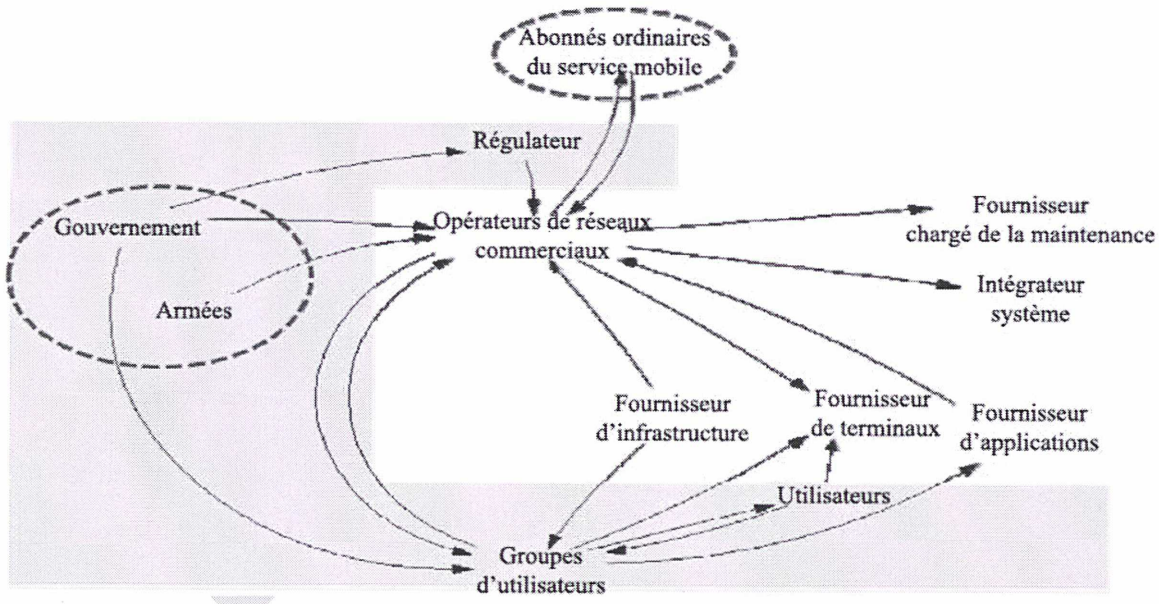
3.1 Parties prenantes principales

Dans la chaîne de valeur des réseaux mobiles PPDR, le détenteur du réseau est généralement l'administration en charge des services de sécurité et de secours, c'est-à-dire le gouvernement. Des organismes de normalisation tels que l'Institut européen des standards en matière de télécommunication (ETSI) sont chargés de définir les spécifications techniques. Le régulateur attribue des licences et le spectre de fréquences et intervient en matière de concurrence. Les utilisateurs (police, pompiers, armée, douanes, secours médical et d'urgence,...) utilisent le réseau mobile. L'opérateur du réseau est responsable de sa construction, de sa maintenance et de son exploitation technique. Les fournisseurs d'équipement du réseau, fabricants de terminaux, développeurs d'applications et intégrateurs sont chargés d'implémenter les fonctionnalités du réseau. Les opérateurs de réseaux cellulaires commerciaux ouverts au public peuvent également être impliqués ; ils peuvent fournir des services à très haut débit pour acheminer les communications administratives au travers de leurs réseaux commerciaux existants. Dans certains pays, des opérateurs privés louent des sites de transmission pour le réseau mobile PPDR. Si le service de communication mobile PPDR était basé sur l'utilisation de réseaux commerciaux, alors le rôle de l'opérateur en tant que partie prenante serait important.

La figure ci-après représente une chaîne de valeur où le réseau dédié PPDR appartient aux pouvoirs publics. Dans ce cas, les relations contractuelles avec le gouvernement sont assez étendues.



La figure suivante représente le cas où le service de communication est externalisé auprès d'un opérateur commercial de réseau mobile ouvert au public.



Dans ce cas, les liens contractuels sont établis essentiellement entre le gouvernement et l'opérateur commercial. Cette alternative n'est pas utilisée en Europe. Cela s'explique par le conflit entre deux acteurs : le gouvernement, qui a des exigences de disponibilité élevées en cas d'urgence, et les abonnés ordinaires au réseau qui verraient leurs droits d'accès limité en pareil cas.

3.2 Analyse des intérêts des parties prenantes principales

Dans cette partie, nous analysons les intérêts des parties prenantes principales et les alternatives qui s'offrent à elles.

Le Gouvernement souhaite acquérir un moyen de communication mobile pour ses services chargés de la sécurité et des secours, qui doit être sécurisé et disponible en toute circonstances. Il a le choix entre posséder et exploiter lui-même le réseau, posséder le réseau et externaliser son exploitation et sa maintenance, ou encore de faire intégralement appel aux services d'un opérateur commercial. Dans ce dernier cas, l'opérateur peut mettre à disposition un réseau dédié ou proposer l'utilisation du réseau ouvert au public.
Pour le décideur, la connaissance du comportement des réseaux commerciaux et des réseaux dédiés en situation d'urgence peut servir de guide dans le choix des solutions. De plus, il doit avoir conscience que les technologies dédiées (infrastructures et terminaux) sont peu évolutives et pâtissent de faibles volumes. La fiabilité du service doit être garantie, ce qui peut constituer un défi pour les opérateurs commerciaux. En outre, un changement d'opérateur peut générer certains risques.

Le régulateur est chargé d'allouer le spectre de fréquences et de délivrer les licences aux opérateurs de télécommunications en cherchant à atteindre l'objectif délicat d'un optimum sociétal (voir encadré). Les opérateurs commerciaux, ainsi que les opérateurs exploitant des réseaux utilisés par les services de secours et de sécurité ou ceux d'autres opérateurs d'importances vitales, peuvent être intéressés par les mêmes bandes de fréquence. Au plan européen, les décisions devraient être harmonisées, sans quoi il ne sera pas possible de générer des économies d'échelle.

La recherche de l'optimum sociétal, un débat complexe

A titre d'illustration, les autorités chargées de la gestion du spectre que nous avons rencontrées (ANFR[137] et ARCEP) considèrent, tout comme leur homologue américaine (Federal communication commission), que les services d'urgence ou de sécurité sont peu incités à utiliser le spectre de manière efficiente[138]. En effet, au contraire des entités commerciales, les utilisateurs des services publics d'urgence et de sécurité ne payent pas pour l'obtention de leur spectre qui fait l'objet d'attribution administrative. En réaction, les utilisateurs et exploitants évoquent souvent les externalités positives liées à l'existence de tels réseaux[139,140]. Mais ces externalités restent très difficiles à évaluer. De plus, les régulateurs considèrent que les flux de communication des services publics d'urgence et de sécurité sont généralement modestes, avec des pointes de trafic lors de crises. Si les services d'urgence et de sécurité doivent disposer de capacités suffisantes pour encaisser ces augmentations de flux lorsqu'elles surviennent, la réservation de fréquences dédiées aux services d'urgence et de sécurité pour supporter ces pics de trafic tend à neutraliser une ressource rare entre deux crises dont la survenue est par définition impossible à anticiper.

Au ministère Chargé de l'Intérieur, on considère qu'il n'y a pas en France ni en Europe d'utilisation dispendieuse du spectre alloués aux forces de sécurité et de secours. Les populations demandent que l'État soit précautionneux et sont de plus en plus exigeantes sur l'efficacité de leurs services de sécurité et de secours.

Les réseaux d'urgence et de sécurité sont dimensionnés pour tenir la charge en temps de crise : c'est leur raison d'être et l'objectif de leur définition, rappelle un équipementier. Selon lui, il serait intéressant de voir si le spectre Schengen [380-385 / 390-395] MHz utilisé par les services de sécurité est utilisé de façon plus efficace que le spectre [410 – 430] MHz et [450 – 470] MHz utilisé par des utilisateurs de type entreprise. La rationalisation liée à la mise en place d'un réseau dédié national a amené une efficacité qui n'existe ni aux USA où, pour des raisons légales, les affectations sont fragmentées, ni dans le monde PMR entreprises, où le spectre est alloué de façon totalement fragmentée. Pour le futur, estime cet

[137] Agence nationale des frequences radio
[138] The Public safety nationwide interoperable broadband network : a new model for capacity, performance and cost – FCC White paper, June 2010
[139] Industry Estimates 100,000 Jobs from Public Safety Communications Network (Telecommunications Industry Association (TIA) – Septembre 2011)
[140] Safety First - Reinvesting the Digital Dividend in Safeguarding Citizens, Wik Consult & Aegis engineering, Mai 2008

équipementier, il est important de revoir ces modes d'allocation spectrale dans le cadre de l'utilisation de nouvelles technologies très haut débit telles que le LTE, issu du monde commercial, afin d'utiliser la ressource spectrale de la manière la plus efficace possible. C'est l'un des grands chantiers ouverts aux USA sur l'allocation de la bande des 700 MHz aux différentes agences de sécurité publique. Il s'agit de rompre avec le paysage actuel fragmenté, typique de la situation hors Europe pour la sécurité publique. En Europe, la révision de la bande supérieure des 400 MHz (de 410 à 470 MHz) dans les années à venir devrait être un sujet de réflexion, estime cet équipementier. Il ne peut pas imaginer qu'en 2020 l'attribution des fréquences continue à être fragmentée, empêchant la mise à disposition de technologies très haut débit à efficacité spectrale beaucoup plus importantes.

L'exploitant d'un réseau dédié utilisé par les services de sécurité et de secours doit fournir des moyens de communication sécurisés et disponibles en toutes circonstances. Il souhaite disposer de spectre additionnel pour des applications futures en large bande et très haut débit (<1 GHz) et acquérir les infrastructures pouvant supporter ces nouveaux services.

Les exploitants de réseaux cellulaires commerciaux peuvent vouloir utiliser leur réseau existant et, au prix d'investissements additionnels et de coûts d'opération marginaux, proposer des services de communication mobile pour les services de sécurité et de secours. L'abonnement mensuel correspondant peut être plus élevé, comparativement aux abonnements des autres usagers. Toutefois, les revenus les plus importants proviennent du réseau ouvert au public. La capacité du réseau peut être insuffisante en situation d'urgence. Le renforcement de la sécurité du réseau afin d'augmenter son autonomie ou de réduire le délai d'intervention en cas de panne peut s'avérer prohibitifs, de même que le montant des pénalités de retard prévues par le contrat.

Le groupe d'utilisateurs (police, pompiers, secours médicaux, douanes,...) souhaite disposer d'un système de communication mobile fiable, sécurisé et disposant de fonctionnalités spécifiques répondant aux attentes des services de sécurité et de secours. Les utilisateurs souhaitent également bénéficier, dans la mesure du possible, des moyens de communication offrant des services analogues à ceux fournis par opérateurs mobiles commerciaux. Ces organismes utilisent par ailleurs de plus en plus les réseaux cellulaires commerciaux au moyen de leur propre téléphone cellulaire, ou de celui fourni par leur employeur.

Les fournisseurs d'équipements de réseau PPDR interviennent dans un marché de niche, où les marges sont légèrement supérieures à celles du marché des réseaux cellulaires traditionnels. Le développement des technologies à très haut débit ouvre de nouvelles opportunités. Les derniers grands réseaux TETRA en Europe seront livrés autour de 2015. Ces réseaux devront faire l'objet d'un maintien en conditions opérationnelles jusque vers la fin des années 2020. Certaines évolutions compatibles avec les technologies actuelles permettront d'améliorer leurs performances, et pourront constituer la solution économiquement la plus avantageuse en milieu rural. Les réseaux PPDR à très haut débit du futur seront très probablement conçus à partir des technologies LTE standard. De nombreux pays souhaitent doter leurs services de sécurité et de secours de tels réseaux. Ces technologies sont en cours de déploiement aux USA et en Asie. Il convient toutefois de rappeler que si, lors du déploiement initial des réseaux mobiles PPDR dédiés (TETRA, TETRAPOL), le marché semblait attractif, étendu et en forte croissance, il y a aujourd'hui une compréhension partagée des limites de ce marché. C'est la raison pour laquelle le marché des infrastructures de ces réseaux est actuellement dominé uniquement par deux

fournisseurs principaux (Cassidian et Motorola). Hormis le cas récent des Etats-Unis, le spectre pour les applications large bande et très haut débit n'est pas encore disponible partout.

Pour les fournisseurs d'équipement de réseau cellulaire, la prochaine étape sur le marché des communications mobiles PSS est celui de la transmission des données à très haut débit, pouvant être implémentée via la technologie LTE. Les évolutions futures des réseaux PSS passeront par deux étapes qui soulèvent deux questions : premièrement, comment satisfaire aux besoins de transmission de données à très haut débit ; deuxièmement, comment remplacer les réseaux PSS actuels d'ici la fin des années 2020. Dans le premier cas, les besoins pourront être satisfaits soit en utilisant des réseaux commerciaux, soit en construisant des réseaux dédiés large bande (type TETRA TEDS[141]) ou à très haut débit LTE. Dans un second temps, il s'agit d'implémenter les fonctionnalités des communications PSS en phonie dans une nouvelle technologie spécifique, pouvant être la technologie LTE. En effet, alors que la technologie LTE permet d'améliorer l'interopérabilité et d'augmenter le débit des transmissions de données, elle ne sera pas en mesure de supporter des services de phonie avant plusieurs années, voire dix ans ou plus. Si le déploiement de technologies large bande ou très haut débit ouvre de nouvelles opportunités, le volume de ces marchés restera faible comparé au marché des réseaux cellulaires.

Le volume de terminaux PSS est faible en comparaison de celui des terminaux de téléphones cellulaires fonctionnant sur les réseaux commerciaux ouverts au public. Trois fabricants se partagent pour l'essentiel le marché des terminaux TETRA (Motorola, Cassidian, Sepura) et TETRAPOL (Cassidian). Les fournisseurs de téléphones cellulaires n'ont pas montré un intérêt particulier sur le marché des terminaux PSS. La situation serait différente si la solution très haut débit s'appuyait sur des technologies commerciales. Le marché des terminaux TETRA et TETRAPOL est si réduit qu'il n'est pas attendu de changement majeur sur ces marchés. TEDS est aussi un marché de niche. Il est probable que les fournisseurs de matériels TETRA seront seuls présents sur ce marché. Les volumes sont plus faibles que ceux des terminaux TETRA, car l'utilisation de TEDS pourrait être limitée à l'environnement des véhicules. Si le très haut débit n'est utilisé que pour la transmission de données, les terminaux pourraient être très proches des produits grand public. La possibilité d'utiliser les plateformes des technologies cellulaires pourrait accélérer le développement des terminaux PSS et la croissance de ce marché. Cependant, les utilisateurs de ces terminaux exigent des équipements robustes, résistant à des conditions environnementales plus sévères (protection contre l'eau et les poussières) que les terminaux de téléphone cellulaires ordinaires. D'autres fonctionnalités spécifiques devraient être prises en compte, telles que le cryptage, la touche d'appel d'urgence…

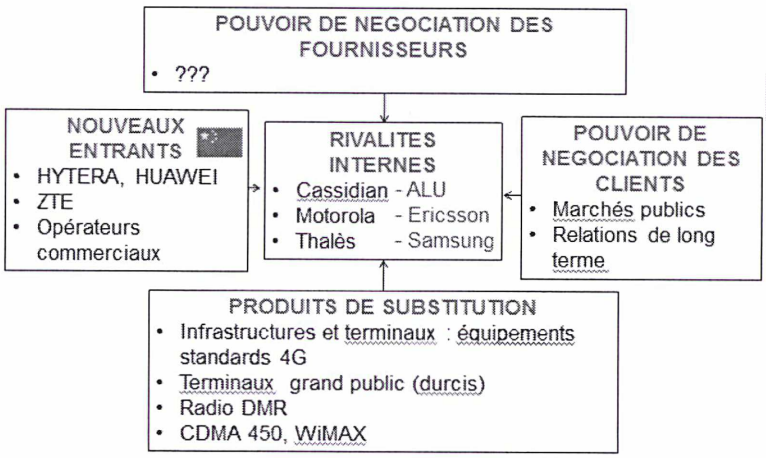
Du côté des développeurs, l'augmentation attendue des capacités de transmission offre une plus large sélection d'applications pour les réseaux PSS ainsi que l'utilisation d'applications développées pour les réseaux commerciaux.
Les réseaux actuels en bande étroite disposent de faibles capacités de transmission (quelques kilobits/s), ce qui limite le champ des applications. L'amélioration des performances en large bande (TETRA TEDS) permet des débits allant de 50 à 200kbits/s ce qui est suffisant pour la plupart des applications, à l'exception des vidéo-transmissions et de la navigation Web. Les réseaux à très haut débit offriront encore de nouvelles perspectives aux développeurs d'applications. Ces applications devraient pouvoir être utilisées sur tous les réseaux et partiellement sur les réseaux actuels.

[141] TETRA enhanced data service

3.3 Analyse de la structure concurrentielle de l'industrie : vers la fin de l'oligopole ?

Notre analyse de la structure concurrentielle de l'industrie s'appuie sur la grille proposée par Michael E. Porter[142]. Selon Porter, la profitabilité dépend de six facteurs : les concurrents actifs sur le même marché, de nouveaux entrants potentiels, l'émergence de technologies de substitution, le pouvoir de négociation avec les fournisseurs, et le pouvoir de négociation avec les clients. L'analyse des forces de Porter permet d'imaginer des scénarios d'évolution possibles du domaine et tenter de mettre l'entreprise en bonne position pour parer aux menaces et saisir les opportunités.

Structure concurrentielle de l'industrie



3.3.1 Les concurrents actifs sur le même marché

L'industrie de la radio mobile professionnelle concentre historiquement un nombre réduit d'acteurs : il s'agit principalement de Cassidian, Motorola et de Thalès. Leurs facteurs clés de succès ont longtemps reposé sur une offre d'équipements et d'infrastructures dédiées, utilisant du spectre dédié et répondant aux besoins spécifiques des utilisateurs notamment en termes de résilience augmentée.

3.3.2 L'émergence de technologies de substitution

En termes de produits de substitution, la technologie LTE standard devrait supplanter les normes de radio mobile professionnelles actuelles de l'avis de la plupart des experts.

Les industriels historiques se sont alliés récemment pour relever ce défi. La multiplication des alliances et des partenariats annoncés récemment laisse présager une modification de la structure concurrentielle existante.

Ainsi, Cassidian et Alcatel-Lucent ont annoncé au printemps 2012 le lancement d'une nouvelle solution 4G LTE baptisée « Evercor » pour renforcer la sécurité et les opérations des agences de sécurité publique, des opérateurs d'énergies et des sociétés de transport[143]. Evercor combine la technologie haut débit mobile 4G LTE d'Alcatel-Lucent avec les systèmes TETRA de Cassidian pour former la toute première solution de radiocommunications mobiles professionnelles 400 LTE intégrée de bout en bout pour la bande 380-470 MHz – la fréquence généralement réservée aux agences de sécurité publique et à d'autres services critiques dans de nombreux pays, en particulier

[142] Stratégie d'entreprise, pp.46-47 , Thierry Weil (Ecole des mines de Paris, 2008)
[143] Alcatel-Lucent et Cassidian dotent les systèmes de radiocommunications mobiles professionnelles (15 mai 2012)

en Europe. La solution prendra en charge les communications haut débit telles que la vidéo en temps réel pour compléter les systèmes radio existants. Grâce à elle, les sociétés de transport et les opérateurs d'énergies utilisant des communications TETRA pourront également bénéficier d'applications haut débit mobile.
On notera également l'extension du partenariat entre Cassidian et l'équipementier Coréen Asia Pacific Satellite communications Inc. (APSI) pour répondre aux besoins liés au transfert de données critiques dans un grand nombre de secteurs industriels[144]. Par ailleurs, nous avons noté l'acquisition du Groupe autrichien 3T par Sepura, qui permet désormais au britannique Sepura de pénétrer proactivement le marché des infrastructures et de l'intégration[145]. Sepura entend également se développer sur le segment des utilisateurs industriels.
Au même moment, Thales et Nokia Siemens Network (NSN) ont signé un protocole d'accord visant à développer une solution LTE concurrente de celle de Cassidian et d'Alcatel-Lucent. Les futurs produits seront initialement destinés aux marchés d'EMEA (Europe, Moyen-Orient et Afrique)[146].
Un peu plus tôt en 2010, Motorola Solutions leader mondial sur les solutions de communications PPDR s'était allié avec Ericsson, leader mondial dans le haut débit mobile, y compris LTE[147] ; Ericsson fera bénéficier Motorola d'économies d'échelle substantielles.
De même, Samsung Electronics et Thales ont signé un accord de partenariat portant sur le développement conjoint et la commercialisation d'une solution d'infrastructure et de terminaux mobiles. À travers ce partenariat, Thales et Samsung Electronics créent une offre supportant à la fois la norme 4G WiMax mobile, le standard 4G LTE (Long Term Evolution) et la norme TETRA, norme européenne de sécurité publique[148].

3.3.3 De nouveaux entrants potentiels

En termes de nouveaux entrants, les équipementiers chinois constituent une menace à surveiller tout particulièrement, notamment s'agissant de Huawei – également présent sur le marché de la radio mobile professionnelle. Totalement marginal au début des années 2000, Huawei est devenu en 2011, sans acquisition, deux fois plus gros que la combinaison des deux précédents champions mondiaux, Alcatel et Lucent. Mais de fortes barrières à l'entrée demeurent : l'Amérique n'en veut pas pour des raisons liées à la sécurité nationale149 et l'Europe s'en méfie150 ; la Commission européenne vient en effet d'initier des investigations concernant d'éventuelles aides d'État. En France, un rapport parlementaire[151] préconise l'interdiction des équipements chinois, pour des raisons liées à la sécurité nationale. Par ailleurs, Hytera, un autre acteur majeur de la radio professionnelle mobile, a racheté en 2011 la division TETRA de Rhode & Schwarz[152]. Hytera présentait ses dernières applications au salon Milipol à Paris en 2011[153] et a participé au forum radiocoms qui a eu lieu à Paris en avril 2012[154].

Les opérateurs commerciaux exploitant des réseaux ouverts au public étaient traditionnellement peu présents sur le marché de la radio professionnelle mobile. Cependant, des partenariats ont été conclus avec plusieurs très grands opérateurs commerciaux dans le cadre du déploiement des premiers réseaux LTE destinés aux forces de sécurité et de secours aux Etats-Unis. Ainsi,

---

[144] CASSIDIAN et APSI étendent leur coopération aux modems TEDS (16 mai 2012)
[145] Police radio maker Sepura targets private sector (16 mai 2012) – Le groupe britannique Sepura est un leader du marché dans les radios Tetra, avec environ 40 pour cent du marché mondial, au coude à coude avec Motorola Solutions Inc et en avance sur Cassidian.
[146] Thales et Nokia Siemens s'intéressent à leur tour aux réseaux publics de sécurité (21 mai 2012)
[147] Ericsson and Motorola Solutions enter alliance to provide LTE solutions for Public Safety (Septembre 2010)
[148] Thales et Samsung apportent la 4G aux téléphones mobiles du secteur public
[149] Huawei blocked from first responder network contract, US cites 'national security concerns' **(Octobre 2011)**
[150] L'UE pourrait enquêter sur des aides illégales à Huawei et ZTE **(1er juin 2012)**
[151] Rapport du sénateur Jean-Marie Bockel, Juillet 2012
[152] Hytera will take over TETRA specialist Rohde & Schwarz Professional Mobile Radio GmbH (26 juillet 2011)
[153] Hytera to present digital security products and innovative applications at Milipol Paris 2011
[154] Hytera au forum radiocoms 2012

Motorola prévoit de tirer parti des applications LTE à travers le réseau commercial de Verizon exploité en parallèle d'un réseau privé LTE et dans le cadre d'un accord d'itinérance lorsque le réseau privé n'est pas disponible[155].

De même, le géant AT&T s'est allié avec Harris Corporation pour développer les réseaux de 4ème génération pour les forces de sécurité et de secours et leur permettre l'itinérance sur ses propres réseaux, pour les zones géographiques non couvertes par le réseau dédié[156].

Par ailleurs, Ericsson a appelé notre attention sur sa solution Governement Home Network (GHN)[157] conçue sur le concept d'un opérateur de réseau mobile virtuel (MVNO) empruntant les réseaux commerciaux (voir encadré). Pour Ericsson, « *les réseaux de télécommunication "grand public" sont une infrastructure critique pour l'économie nationale* ». Si le concept du GHN paraît séduisant, l'équipementier n'a toutefois pas été en mesure de nous préciser où cette solution a déjà été mise en œuvre.

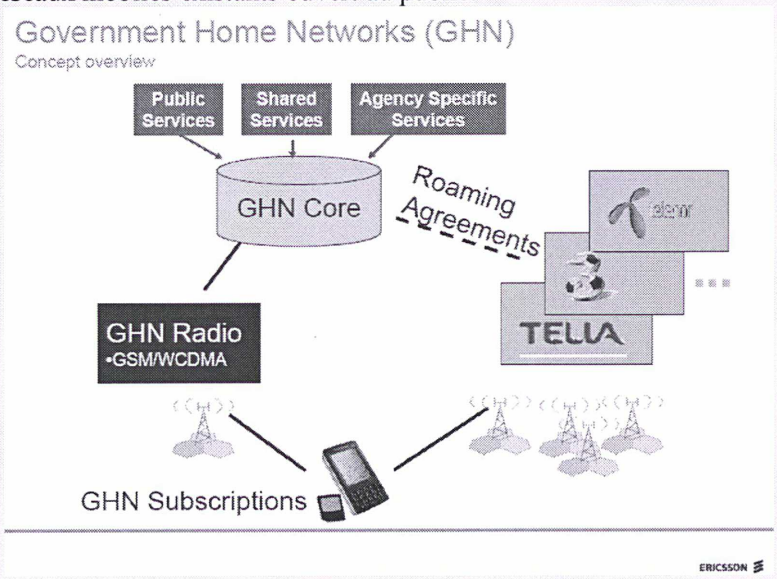
« *On veut bien être opérateur de l'État, on a cette culture* » réagit un opérateur français. Mais il estime nécessaire une juste compensation et qui ne doit pas être asymétrique. Il s'agit d'une question d'équité, estime cet opérateur. Selon lui, les opérateurs d'infrastructures (les couches dites basses) portent l'essentiel des obligations contrairement aux opérateurs des couches hautes. « *Nous ne sommes pas délocalisables, et nous ne souhaitons pas subir de distorsions de concurrence* ». À la clé, un véritable sujet de compétitivité par rapport à des opérateurs tels que Verizon estime-t-il.

Mais en termes d'incitation, un autre opérateur français rappelle que les opérateurs ont déjà bénéficié de points supplémentaires pour l'ouverture de leurs réseaux aux MVNO. Seraient-ils prêts à ouvrir à nouveau leur réseau à un opérateur bien particulier s'occupant de la sécurité intérieure, s'interroge-t-il ? Selon lui, les opérateurs commerciaux ne souhaitent pas voir les contraintes réglementaires augmenter. Dans certains pays, l'opérateur ferroviaire continue à opérer, comme la SSB-CFF en Suisse. En effet, Swisscom a refusé d'entrer sur ce marché à cause des exigences en termes de sécurité et de risque. Swisscom ne voulait pas endosser un tel niveau de responsabilité. Il reste que certains opérateurs sont capables de prendre de tels risques. Tout est fonction du besoin exprimé, estime cet opérateur.

[155] Motorola, Verizon establish public-safety LTE alliance **(23 février 2011)**
[156] Public Safety Agencies to Benefit From AT&T and Harris Corporation Alliance to Deliver Next-Generation LTE Solutions **(24 octobre 2011)**
[157] Ericsson Government Home Network

L'offre Governement Home Network (GHN) d'Ericsson

Government Home Network (GHN) est un concept d'un opérateur de réseau mobile virtuel (MVNO) s'appuyant sur les réseaux mobiles existants ouvert au public.



Pour Ericsson les principaux arguments en faveur d'une telle solution sont :

Utilisation des réseaux existants

GHN tire parti des couvertures et infrastructures de réseaux commerciaux ainsi que de tout réseau privé existant. Cette solution apporte une redondance entre plusieurs réseaux et permet l'itinérance au niveau national via les accords d'itinérance existant entre plusieurs opérateurs.

Utilisation des technologies commerciales

Les technologies commerciales sont utilisées par plusieurs milliards d'abonnés. Le marché évolue vers le haut débit. En termes d'économie d'échelle réalisables via l'utilisation des réseaux commerciaux, le coût est une fraction de celui induit par les solutions PMR traditionnelles. Le dynamisme commercial du 3GPP et l'utilisation de technologies standard sécurisent le développement de nouvelles fonctionnalités et des améliorations. L'exploitation d'une solution GHN permet la mise en place de gestion de priorité des appels.

Une couverture nationale dès le premier jour

La solution peut être rapidement déployée par la réutilisation des infrastructures existantes. Le temps de déploiement d'une solution GHN nationale peut être mesuré en semaines, comparativement à cinq voire dix ans pour un réseau PMR dédié.

La couverture GHN permet la transmission de données tout en garantissant son interopérabilité avec les réseaux PMR existants.

Exemple de scénario : incendie d'une raffinerie Le scénario est celui d'un incendie majeur affectant une raffinerie. Des dommages majeurs impactent l'environnement et les infrastructures, y compris les infrastructures locales de communication. Les services de secours et de sécurité arrivent sur place dans les 5 minutes pour maîtriser l'incident. Le réseau GHN permet de partager des images de l'incendie entre tous les intervenants. L'accès au GHN peut être étendu à la sécurité des raffineries et des équipes de secours du site utilisant l'infrastructure de communication commune via l'introduction de cartes SIM GHN dans leurs terminaux cellulaires personnels. Le profil d'abonnés pré-définis permet de garantir la sécurité des informations au niveau approprié entre les utilisateurs.	[redacted]

3.3.4 Le pouvoir de négociation avec les clients

L'essentiel de la négociation intervient dans le cadre de marchés publics. Le pouvoir de négociation est certes plus important avant la passation des marchés qu'à la suite de sa conclusion. Mais, pour la Cour des comptes américaine (GAO), les agences publiques ne sont pas en mesure d'exercer une pression importante sur les prix d'achat de leurs équipements ; il en résulte des dépenses excessives, en particulier du fait que toutes les entités se fournissent auprès des équipementiers indépendamment les unes des autres[158]. L'annonce du rapprochement entre les associations d'utilisateurs APCO et TETRA initiée aux États-Unis, pourrait favoriser l'émergence d'un marché global susceptible de générer de nouvelles économies d'échelle[159,160].

Par rapport aux nouveaux entrants potentiels, les équipementiers historiques peuvent s'appuyer sur toute une offre de services pour fidéliser leurs clients ; en particulier, ils peuvent proposer des adaptations afin d'augmenter localement la résilience du réseau en prévision d'événements planifiés. Certains équipementiers peuvent également mettre à disposition leur expertise en matière de sécurité, comme Cassidian qui vient de créer un nouveau département dans le domaine de la cybersécurité[161].

3.3.5 Le pouvoir de négociation avec les fournisseurs

??? voir avec ALU et Cassidian pour compléments

3.4 Forces de changement à l'œuvre

Les entretiens avec les parties prenantes et l'actualité du sujet dans le monde ont permis de préciser les forces de changement à l'œuvre ; celles qui affecteront les développements futurs des réseaux PSS ; celles qui sont les plus fortes ; celles qui génèrent le plus d'incertitudes. Ainsi avons-nous analysé l'influence (positive ou négative) que peuvent exercer les facteurs macro-environnementaux d'ordres politiques, économiques, sociales et technologiques sur le développement des réseaux de communication pour la sécurité et des secours.

---

[158] Various Challenges Likely to Slow Implementation of a Public Safety, US Government Accountability Office (Février 2012)
[159] APCO, TETRA association partner to support public-safety LTE research (Urgent communications, 15 mai 2012)
[160] Creating global market critical to public-safety broadband success (Urgent communications, 15 mai 2012)
[161] EADS Cassidian traque les pirates du Net (Le Parisien, 13 juin 2012)

3.4.1 Forces politiques

Au plan politique, le thème de l'insécurité avec ses corollaires liés au terrorisme et à l'extension de la criminalité dans le monde appellent au développement des moyens de communication des forces de sécurité et de secours. Une transparence accrue, la recherche de performance et de traçabilité des activités des forces de sécurité et de secours sont également au cœur des attentes. Enfin, la recherche de spectre additionnel de fréquence fait l'objet d'un lobbying intense auprès des politiques, notamment aux USA.

3.4.2 Forces économiques

Au plan économique, le financement des réseaux PSS constitue un défi pour de nombreux pays désireux de maintenir un certain équilibre budgétaire. Par ailleurs, s'agissant de questions touchant à l'utilisation de biens économiques publics, les gouvernements ont des attentes en matière de retour sur investissement. En outre, les décisions d'investissement concernant de futurs systèmes de communication PSS peuvent avoir un impact majeur sur les coûts de fonctionnement des réseaux mobiles PSS.

3.4.3 Forces technologiques et sociales

Au plan social, les jeunes générations poussent au développement des communications via Internet. Les populations ont des attentes importantes de la part des autorités. Les télécommunications, ainsi que le développement des réseaux de transport, d'énergie et d'eau, sont devenus indispensables à la société. Cela se traduit par l'accroissement du nombre d'organismes à prendre en considération dans la sphère des services de sécurité et de secours.

Au plan technologique, les performances des réseaux 3G apparaissent déjà bien supérieures sur certains aspects, comparées aux technologies PSS. Les connections internet permettent des capacités de communication plus étendues que celles dont disposent les services de sécurité, pouvant donner un avantage aux organisations criminelles. La 3G bénéficie également d'économies d'échelle importantes.
S'agissant du développement de nouvelles technologies pour les réseaux PSS, le WiMAX semble avoir perdu en intérêt. La technologie LTE a été plébiscitée aux USA pour servir de base à la conception du futur réseau PSS à très haut débit. Cela pourrait fortement influencer les choix technologiques à venir en Europe, en lien avec de futures décisions d'attribution de fréquences.
Par ailleurs, l'intelligence et l'augmentation des capacités de stockage des terminaux cellulaires va susciter des attentes de la part des utilisateurs professionnels et offre de nouvelles opportunités, tant en termes de traitement que de fonctionnement de nouvelles applications sur leurs terminaux. Les équipementiers rivalisent d'inventivité pour séduire les utilisateurs potentiels de ces nouvelles applications[162].
La recherche et développement en cours vise également à améliorer la sécurité des intervenants en intégrant divers capteurs dans leurs équipements. Tel est par exemple l'objet de travaux récents au CEA-LETI, en partenariat avec CASSIDIAN et le SDIS en région Rhône-Alpes (projet Demoloc).[163]
Le développement de techniques de compression des données réduira les exigences en matière de débit. En dépit de la qualité des algorithmes de chiffrement des systèmes actuels de communication, de nouvelles menaces devront être prises en compte en termes de sécurité.

---

[162] Voir par exemple la brochure "Barricaded suspect incident analysis. Enhancing critical incident response with public safety LTE", Motorola 2011 ou la vidéo de présentation du nouveau terminal LEX 700 de Motorola

[163] CEA-Leti and Partners Develop System to Monitor Public-Safety Personnel in Dangerous Situations. (Janvier 2011)

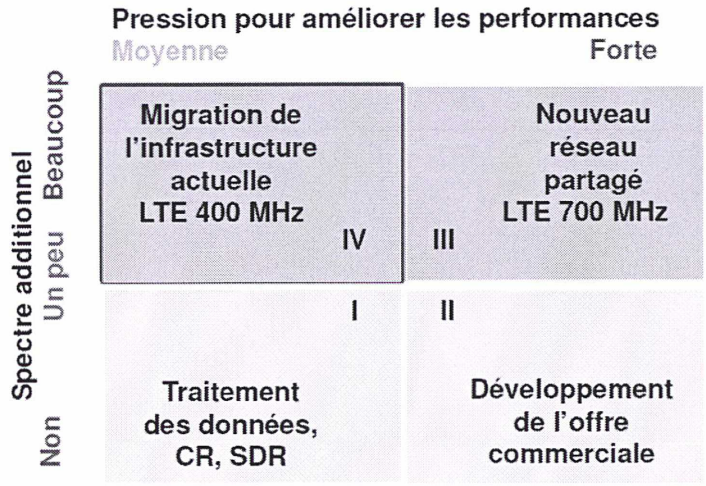
La charge de trafic d'un réseau PSS peut être élevée en situation de crise. Des outils plus performants sont nécessaires pour suivre le trafic et contrôler les accès en cas de surcharge du réseau.
L'exigence d'efficience dans l'utilisation du spectre peut être satisfaite par le biais de technologies d'accès dynamique au spectre et de la radio cognitive, qui soulèvent toutefois des interrogations s'agissant du contrôle des priorités d'accès.

Le marché des communications PSS constitue un défi pour les opérateurs commerciaux, car le service à offrir requiert des durées de fonctionnement des batteries de sauvegarde supérieures à celles spécifiées pour les réseaux cellulaires. Le délai d'intervention en cas de panne est également plus court et, d'une manière générale, les exigences de disponibilité sont plus élevées pour ces acteurs. Les enjeux listés peuvent représenter des coûts additionnels significatifs pour un opérateur commercial, coûts qu'il peut répercuter contractuellement via le tarif d'abonnement, mais qui devraient rester dans tous les cas inférieur aux charges d'investissement et d'exploitation d'un réseau dédié. À noter que les réseaux existants avec leurs réservations de spectre entraînent une certaine dépendance qui influe sur tout projet visant à les remplacer. Et à la question de la durée des batteries s'ajoute celle du risque de congestion des réseaux commerciaux en cas de crise.

Enfin, les utilisateurs finaux sont aussi des usagers des réseaux 3G, dont la couverture et la capacité croissent très rapidement avec les usages des services en 3G. La jeune génération des personnels des services de sécurité et d'urgence est habituée aux services 3G (et ultérieurement aux services 4G) et aux interfaces utilisateur sophistiquées qu'elle espère retrouver dans son travail. La voix (communications de groupe) constitue de loin le mode de communication le plus important dans les réseaux PSS, mais les transferts de données deviennent également importants. Le streaming vidéo est perçu comme un élément important pour améliorer la prise de conscience de l'environnement au cours d'interventions critiques. Les services attendent une couverture intérieure aussi bonne lors de l'utilisation de leur terminal professionnel que celle à laquelle ils sont habitués sur les réseaux GSM. Ceci impacte la sélection des technologies futures.

3.5 Deux incertitudes clés pour définir des stratégies possibles : l'obtention de nouvelles fréquences et la pression des avancées technologiques

Les principales tendances et incertitudes liées aux évolutions des réseaux PSS dépendent de la prédictibilité et de l'importance des forces à l'œuvre. Afin de définir les scénarios futurs, nous avons identifié deux incertitudes clés : l'obtention de nouvelles fréquences et la pression des avancées technologiques – qui permettent de définir quatre axes stratégiques.



3.5.1 Premier axe stratégique (I) : optimisation des performances des réseaux dédiés actuels par l'amélioration du traitement des données

Ce scénario est favorisé par la crise économique actuelle et la difficulté à trouver des moyens de financement pour des investissements majeurs dans les réseaux mobiles PSS. Dans le même temps, il n'y a pas suffisamment de confiance dans la disponibilité des réseaux commerciaux, ou encore le fait que les opérateurs commerciaux ne veulent pas réellement endosser de responsabilité en cas de défaut de disponibilité de leur réseau.

Ce scénario correspond plus ou moins à la situation actuelle (en Europe) : absence de disponibilité de spectre additionnel et pression modérée pour implémenter de nouvelles applications afin d'améliorer les performances. Les améliorations de performances de portée limitée peuvent être obtenues : (1) en utilisant les réseaux commerciaux pour véhiculer des communications non critiques ; (2) en prenant en compte les évolutions des standards actuels (par exemple TETRA TEDS), si les bandes de fréquences actuelles le permettent et (3) ; en améliorant l'utilisation des canaux de communication par le biais de techniques de compression permettant d'optimiser les volumes de données transmises, ou encore en développant des applications de radio cognitive (CR) ou de radio logicielle (SDR), qui ont notamment fait l'objet de travaux dans le cadre du 7ème PCRD (Projet EULER précité de la Commission européenne).

3.5.2 Deuxième axe stratégique (II) : développement des offres des opérateurs commerciaux (réseau virtuel MVNO, non critique)

Dans ce scénario, il y a de fortes incitations à prendre en compte de nouvelles applications ; des solutions de financement existent, mais c'est la disponibilité de spectre additionnel qui fait défaut. Dans ce cas, la seule solution est d'optimiser l'utilisation des fréquences actuelles. Cet objectif peut être atteint (1) en implémentant l'évolution des normes actuelles (TETRA TEDS) lorsque cela est possible et (2) en utilisant les réseaux commerciaux mobiles à très haut débit pour véhiculer les communications non critiques, sans sacrifier aux impératifs de disponibilité ni de sécurité. En Belgique, l'opérateur du réseau PPDR ASTRID a ainsi annoncé qu'il deviendra en 2013 un « Mobile Virtual Network Operator » (MVNO) qui offre des services par le biais du réseau de tiers[164]. Il a déclaré à cette occasion que « *acheter un spectre propre et développer à présent un nouveau réseau de données mobiles, cela n'a jamais été une option. Il n'y a pas de budget pour cela.* »[165]

[164] ASTRID veut le 3G pour la communication data – Communiqué ASTRID du 29 mars 2012
[165] Les services de secours utiliseront des réseaux 3G pour les données mobiles – Le Vif 13 mars 2012

Toutefois, la méfiance persistante dans la disponibilité des réseaux commerciaux en situation d'urgence ou concernant les risques liés à un changement d'opérateur peut constituer un frein à la concrétisation de ce scénario.
De ce point de vue, nous n'avons pas eu confirmation, auprès des autorités compétentes, de l'existence en France d'une organisation pour la gestion des priorités d'accès aux réseaux commerciaux. Nous recommandons la mise en place d'une telle organisation en France (voir encadré ci-après).

Vers un mécanisme de gestion des priorités d'appels pour les réseaux commerciaux ouverts au public et partagés avec les forces de sécurité et de secours
Certains opérateurs proposent des offres permettant au client, en échange d'un surcoût, d'avoir accès aux réseaux mobiles dans les heures de saturation, et sans coupure ou perte de débit[166]. Cet accès prioritaire au réseau est vivement dénoncé par des associations, dont l'UFC-Que Choisir en France. Cette dernière redoute que l'arrivée d'un tel type de service en France ne crée des abonnés de second plan.
Or, la mise en œuvre de la préemption doit pouvoir être maîtrisée en toutes circonstances par les services de sécurité et de secours. En outre, selon l'ANFR[167], il conviendrait d'actualiser le cadre législatif et réglementaire en vigueur actuellement, qui fixe des conditions non applicables aux services de sécurité et de secours dans les situations que l'on pourrait considérer de « pré-crise ».
Au plan juridique, le dispositif à mettre en place pourrait s'inspirer de celui en vigueur pour la gestion en France des délestages électriques[168]. En pratique, l'organisation pour l'enregistrement et le traitement des demandes d'accès des usagers prioritaires pourrait prendre exemple sur les organisations existant à l'étranger, aux États-Unis[169], au Canada[170] ou au Royaume-Uni[171]. L'UFC-Que Choisir considère qu'en situation d'urgence, l'intérêt général doit primer et nous a assuré que ce type d'organisation serait plus acceptable que les solutions payantes proposées par certains opérateurs commerciaux.
Afin de renforcer l'acceptabilité d'un tel mécanisme, les pouvoirs publics doivent en contrepartie fournir de l'information sur la crise. Le déploiement en France d'un nouveau système d'alerte et d'information du public (SAIP, voir § 2.4.1) utilisant les réseaux mobiles commerciaux peut contribuer à l'atteinte de cet objectif.

A noter qu'un mécanisme de gestion des priorités devrait également être envisagé sur la partie dédiée d'un réseau de sécurité comportant de nombreux utilisateurs. Le futur grand réseau à très haut débit américain prévoit une telle organisation.

3.5.3 Troisième axe stratégique (III) : création d'un réseau très haut débit partagé interopérable à l'échelle européenne et proposant des services avancés à partir de technologies standard en 700 MHz

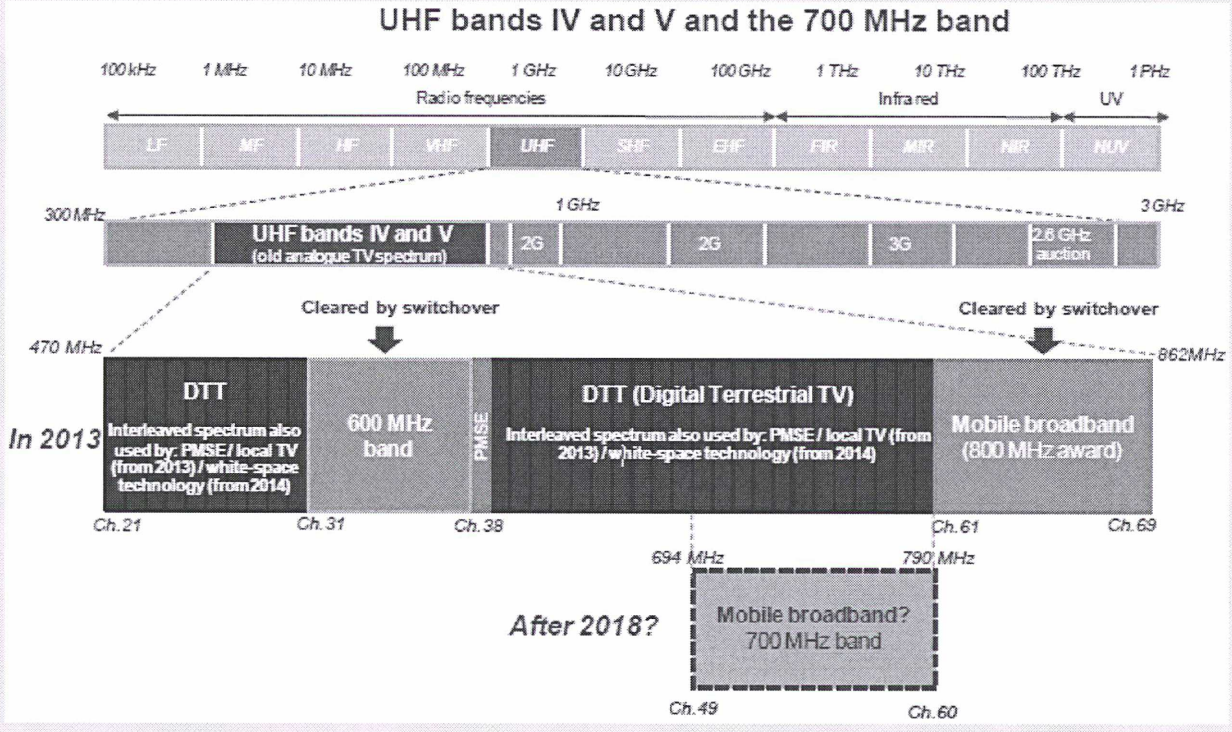
D'un point de vue conceptuel, il s'agit du scénario le plus séduisant ; nous l'avions mis en avant lors de notre consultation des parties prenantes dans le cadre de ce mémoire[172]. Dans ce scénario existe une forte pression pour prendre en compte de nouvelles applications. Il est favorisé par l'accroissement de la menace terroriste, de la criminalité ou de catastrophes naturelles, de sorte que du spectre additionnel est attribué, comme c'est le cas aux USA, au Canada et dans certains pays asiatiques, dans une bande de fréquences proche de celle attribuée aux opérateurs commerciaux.

[166] Vodafone teste un accès prioritaire payant à son réseau 3G+ (LeMondeInformatique du 20 novembre 2009)
[167] Rapport du groupe de travail du conseil d'administration de l'ANFR « Organisation et évolution de la gestion du spectre » (mars 2008)
[168] Arrêté du 5 juillet 1990 fixant les consignes générales de délestages sur les réseaux électriques
[169] Wireless Priority Service (WPS) aux USA
[170] Service prioritaire sans fil (SPSF) au Canada
[171] Privileged Access Schemes – MTPAS, FTPAS and Airwave au Royaume-Uni
[172] Quels réseaux de communication électronique pour la sécurité intérieure et les services d'importance vitale ? Note de synthèse - Vincent Jugé et David Krembel (Mars 2012)

Au plan technique, il s'agirait d'utiliser les mêmes technologies que les opérateurs commerciaux, de partager les infrastructures en procédant le cas échéant au renforcement de leur résilience et aux extensions de couverture nécessaires, de conclure des accords d'itinérance, voire de partager du spectre sous réserve de disposer d'un accès prioritaire en situation de crise.
Considérant le développement probable de services vocaux sur le réseau à large bande dans le long terme, il conviendra de proposer des évolutions au standard LTE, afin de prendre en compte les exigences des utilisateurs PPDR. Ce travail a débuté aux États-Unis et le groupe européens d'expert FM49 de la CEPT devrait prendre l'attache de l'organisme de normalisation compétent pour ce standard, le 3GPP LTE.
Dans ce scénario, nous faisons le pari de l'ouverture future de la bande de fréquence des 700 MHz à la téléphonie mobile en Europe, qui permettrait de bénéficier d'économies d'échelle au niveau mondial et du retour d'expérience de la création des réseaux PPDR Nord-américains. En effet, la conférence mondiale des radiocommunications de 2012 (CMR-12) a réfléchi à la possibilité de faire de nouvelles attributions de spectre au service mobile. Après avoir œuvré pour harmoniser l'utilisation de la bande 790-860 MHz (dite « bande 800 MHz ») pour les usages mobiles haut débit (dont le processus d'attribution aux opérateurs a été finalisé en décembre 2011 en France), c'est dans la bande 694-790 MHz (dite « bande des 700 MHz »), initialement réservée à la diffusion télévisuelle, que la CMR-12 propose de prélever des ressources. En effet, une telle évolution serait possible à la suite de l'introduction de technologies de compression plus efficaces pour la diffusion en télévision numérique terrestre (TNT), incluant les normes DVB-T2 et MPEG 4. Dès à présent, des travaux d'harmonisation de l'utilisation des fréquences dans cette bande vont être lancés et feront l'objet d'une évaluation lors de la prochaine conférence mondiale des radiocommunications CMR-15 de l'Union internationale des télécommunications (UTI), en 2015[173] (à noter que les États-Unis exploitent déjà la bande 700 MHz pour du data mobile à très haut débit LTE et WiMAX). Le recours à des technologies standards, s'il est favorable en termes d'économies d'échelle, nécessitera toutefois de prendre en compte de nouveaux enjeux de sécurité compte tenu de l'augmentation de la surface d'attaque qui en découle.
Une consultation récente au Royaume-Uni par le régulateur Ofcom a porté sur la stratégie d'emploi futur des bandes de fréquence UHF comprises entre 470 et 862 MHz, y compris l'opportunité d'un service mobile à très haut débit sur la bande 700 MHz tenant compte notamment des besoins PPDR[174]. À cette occasion, plusieurs équipementiers ont pris position favorablement (voir encadré sur cette consultation).

[173] La Conférence mondiale des radiocommunications fixe le cap pour demain (Union internationale des télécommunications, février 2012)
[174] Securing long term benefits from scarce spectrum resources – a strategy for UHF bands IV and V (470 – 862 MHz), pp. 49-50 (Consultation Ofcom, 29 Mars – 7 juin 2012)

Consultation du régulateur britannique Ofcom portant notamment sur l'opportunité de services en très haut débit mobile dans la bande des 700 MHz après 2018 et sur les besoins PPDR (29 mars – 7 juin 2012)



Position d'Ericsson

Ericsson estime que la façon la plus rentable de fournir le très haut débit aux forces de sécurité et de secours est de partager l'utilisation des réseaux commerciaux avec les garanties appropriées pour l'utilisation par les services d'urgence. La pratique de réduire les coûts en partageant les coûts élevés de l'utilisation intermittente du spectre par les services d'urgence a été lancée au Royaume-Uni en utilisant la technologie TETRA, où les coûts ont été répartis sur une large partie de la fonction publique avec une grande capacité d'être à la disposition des services d'urgence en cas de besoin. Le système américain de sécurité publique a cherché à imiter ce principe pour le haut débit en élargissant l'ensemble des utilisateurs encore davantage, en partageant les installations lorsqu'elles ne sont pas nécessaires pour les services d'urgence, en laissant le public en général utiliser les installations. Nous croyons que c'est la bonne approche logique à suivre pour le Royaume-Uni, indique l'équipementier. Suite à notre approche des services d'urgence, les capacités sont fournies à chaque fois et partout où la capacité publique nécessaire est disponible pour le partage. Si les marchés commerciaux ne fournissent pas une capacité suffisante, on peut s'attendre à ce que le service public puisse ajouter à la capacité des sites livrés dans le Programme d'infrastructure mobile.

L'utilisation du spectre commercial permet aux services d'urgence d'accéder à une large gamme de terminaux commerciaux et d'implémenter des applications spécialisées. L'attribution de spectre dédié pour les services d'urgence peut augmenter les coûts de ces services. Ainsi, nous recommandons que le spectre dans les bandes UHF 4 et 5 soit attribués uniquement lorsque l'utilisation du spectre commercial ou subventionné ne peut pas être un substitut approprié, estime Ericsson.

Position de Motorola UK Ltd

Au contraire, Motorola considère qu'il faut privilégier l'utilisation de spectre dédié. L'équipementier convient que la bande 700 MHz pourrait jouer un rôle important dans la satisfaction du besoin pour la croissance dans le haut débit mobile, en particulier dans le marché PPDR spécialisé. Cette bande est

particulièrement pertinente en raison de l'adoption du 700MHz aux États-Unis et au Canada pour les réseaux PPDR, ainsi que dans certains pays de la région Asie-Pacifique, et pourrait conduire à des économies d'échelle à travers le monde pour la fourniture d'équipements. Cette bande a toutes les caractéristiques nécessaires pour être un candidat idéal pour la bande du spectre PPDR européenne dédiée, à la fois pour des raisons techniques et économiques. Son intérêt serait de compléter l'utilisation de 380 à 400 MHz, où Airwave offre la technologie TETRA pour les services d'urgence à bande étroite. Le choix du 700 MHz permettrait de satisfaire la demande de services large bande en plus des services existants à bande étroite.

Il y a un besoin avéré de spectre pour les données à large bande pour les services d'urgence. Selon l'exigence de l'ETSI TR 102 628, le besoin serait de 10 +10 MHz. Il est probable que les services PPDR en Europe adopteront également la technologie LTE, comme aux États-Unis. Motorola estime qu'il est peu probable qu'un réseau commercial puisse satisfaire toutes les exigences en matière de sécurité et de résilience, ce qui implique de privilégier le choix d'un réseau privé et de spectre dédié comme la solution optimale. En raison de la petite échelle du marché, l'harmonisation du spectre dans toute l'Europe sera impérative pour ces réseaux, de même que le choix d'un spectre avec suffisamment de points communs avec le spectre adopté ailleurs dans le monde pour ces applications. En raison de l'adoption du 700 MHz aux États-Unis, au Canada et dans certaines parties de l'Asie, ce serait la bande de fréquence optimale pour les applications PPDR. Motorola demande instamment à l'Ofcom de soutenir l'activité de la CEPT FM PT49, qui s'efforce de trouver des fréquences pour une utilisation PPDR en-dessous de 1 GHz.

Position de Nokia Siemens Network (NSN)
Pour NSN, il ne devrait pas être alloué de spectre dédié aux services d'urgence dans la bande 700 MHz . Toutefois, en fonction du spectre libéré à la suite de dividendes numériques, les obligations des services PPDR pourraient être prises en compte dans un processus de licence ou de vente aux enchères, s'il y a un besoin national pour cela.
Selon NSN, on devrait étudier avec soin si les besoins de haut débit PPDR peuvent être satisfaits par la coopération avec des opérateurs commerciaux de LTE : il y a des possibilités pour donner aux utilisateurs PPDR des droits spéciaux pour l'utilisation de la capacité, ce qui contribuerait à couvrir les coûts de construction élevés des réseaux dédiés. Les communications les plus critiques pour la sécurité pourraient rester dans le réseau actuel (évolué) TETRA et le contenu à large bande pourrait être transmis via le réseau commercial.

Le réseau TETRA est un écosystème fermé et incapable de soutenir de nouvelles applications à large bande requises par les autorités PPDR. Le réseau TETRA britannique fournit une meilleure couverture que les réseaux mobiles commerciaux actuels en raison de son fonctionnement à 400 MHz et au-dessous dans la bande IV. Les services de base TETRA peuvent être complétés par les solutions commerciales de radio mobiles, surtout si elles sont autorisées à fonctionner dans la bande IV. Les obligations de couverture et la hiérarchisation peuvent être attachés à l'une des licences IV de la bande afin de s'assurer que tout service commercial dans la bande est apte à l'usage prévu pour les autorités PPDR.

Le quasi-doublement de la fréquence résultant de l'utilisation de la bande des 700 MHz imposerait cependant en Europe de renforcer la densité des antennes-relais des réseaux PPDR, afin de maintenir une bonne couverture. Compte tenu du montant des investissements, de la rareté de la ressource en points hauts, du délai de déploiement et des questions d'acceptabilité par le public de l'implantation de nouveaux sites, il conviendrait de s'interroger sur le développement de partenariats avec les opérateurs commerciaux, comme le prévoit déjà par exemple la nouvelle loi américaine en terme de partage d'infrastructure et d'accord d'itinérance[175] (voir figure ci-dessous, illustrant le cas du partage d'infrastructures). À noter que certains opérateurs commerciaux eux-mêmes envisagent désormais de partager leurs infrastructures en Europe, notamment afin de réduire les coûts élevés de déploiement de la 4G [176]. En France, l'ARCEP a déjà défini une

[175] Middle Class Tax Relief and Job Creation Act of 2012
[176] Le partage de réseau, une solution en vogue pour réduire les coûts (LesEchos.fr, 4 mai 2012)

doctrine concernant le partage des infrastructures dans la perspective du déploiement des réseaux de troisième génération[177]. Cette position décrit les scenarii de partage qui sont des possibilités offertes aux opérateurs qui le souhaitent. Cinq niveaux peuvent être envisagés, concernant respectivement les sites et éléments passifs, les antennes, les stations de base, les contrôleurs de réseaux radio et les cœurs de réseau.

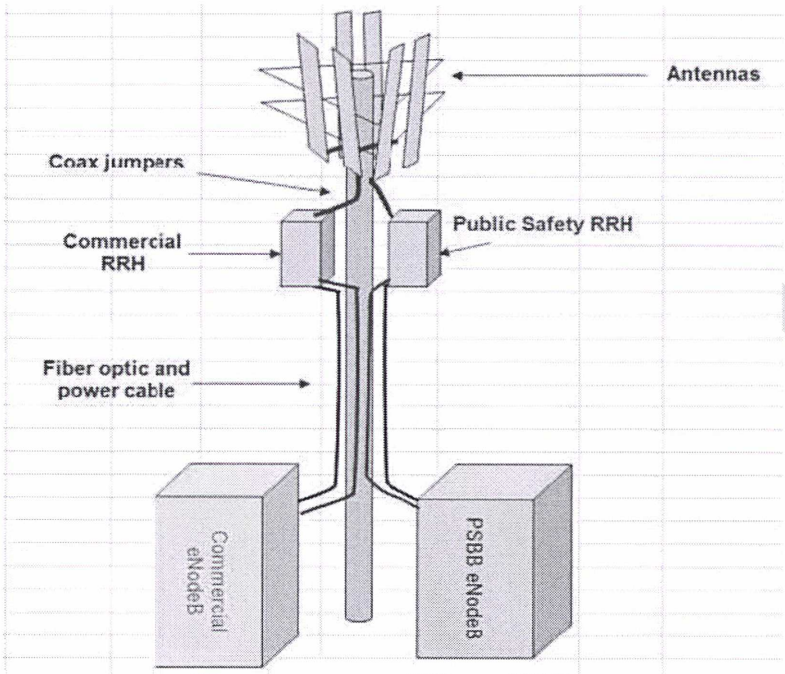


Fig. Illustration du partage d'infrastructure entre un opérateur commercial et PPDR (station de base haut débit), d'après *A broadband technical cost model OBI technical paper n°2, US Federal communication commission*

Certains niveaux, tels que le partage des sites et éléments passifs, sont encouragés. En revanche, l'ARCEP refuse tout partage des infrastructures (telles que le cœur de réseau) qui nécessiterait une mise en commun des fréquences entre opérateurs. En effet, la réglementation impose que les fréquences soient attribuées intuitu personæ, et donc incessibles. Il convient de s'interroger sur les adaptations à envisager dans la perspective de la réflexion engagée au sein de l'Union Européenne concernant le partage des fréquences[178]. En outre, il conviendrait d'examiner l'acceptabilité d'une telle doctrine par les autres affectataires de fréquence (Ministères chargés de l'intérieur et de la Défense).

Cependant, la persistance de difficultés budgétaires, et la volonté d'opérateurs commerciaux d'assurer une plus grande disponibilité de leur réseau peuvent limiter la portée de ce scénario. En outre, plusieurs experts ont appelé notre attention sur les limites de la transposition du modèle américain en Europe (absence d'une réelle gouvernance européenne dont la mise en place se heurte aux souverainetés nationales dans le domaine de la sécurité, absence d'opérateurs commerciaux ayant une taille critique à l'échelle européenne à même de conclure des accords de partenariat).

[177] Position de l'Autorité de régulation des télécommunications sur le partage d'infrastructures dans les réseaux mobiles de troisième génération (mise à jour de septembre 2008)
[178] Shared spectrum access (DG INFSo)

3.5.4 Quatrième axe stratégique (IV) : extension des réseaux dédiés actuels aux technologies LTE en 400 MHz

Ce scénario serait favorisé par l'attribution de nouvelles fréquences dans la bande 350-470 MHz. Dans ce scénario, il y a dans un premier temps une incitation plus mesurée à prendre en compte de nouvelles applications. À cet égard, les utilisateurs en France nous ont fait part de besoins initiaux modestes en spectre additionnel, de l'ordre de 1,4 MHz à 2x5 MHz pour la technologie LTE. Ce scénario présente l'avantage de pouvoir réutiliser un certain nombre d'éléments des infrastructures actuelles dimensionnées pour la bande 400 MHz (sites, points hauts, éléments passifs, liaisons...). De ce fait, il est privilégié par la communauté des utilisateurs PPDR en France et plus généralement en Europe, et apparaît comme étant assez probable. De plus, la pénétration à l'intérieur des bâtiments est meilleure que dans la bande des 700MHz. Certains équipementiers commencent à proposer une offre de terminaux LTE fonctionnant dans la bande 400 MHz. Un consultant nous a suggéré que la couverture très haut débit pourrait initialement se limiter aux zones urbaines. Ce scénario présente néanmoins des économies d'échelle moindres en ce qui concerne l'offre de terminaux et se heurte à la disponibilité du spectre. En effet, selon les experts, il n'existe pas de possibilité d'harmonisation au niveau européen en-dessous de 400MHz. Enfin, une solution satisfaisant tous les utilisateurs du spectre au-dessus de 400 MHz suppose une étroite concertation de toutes les parties prenantes, incluant les opérateurs d'importance vitale pour lesquels nous avons mis en évidence des enjeux industriels importants qui pourraient être remis en cause en cas de modification de leurs allocations actuelles de fréquence.

Discussion : vers un consensus sur la complémentarité des réseaux dédiés et opérés

Un équipementier confirme l'existence du débat sur la question des fréquences. Selon lui, il ne faut pas oublier de voir quelles sont les possibilités et qu'elles sont les difficultés pour aller dans ces bandes de fréquences. La bande des 400 MHz est déjà allouée au service de radio mobile professionnelle en Europe et en partie à la sécurité publique. Dans le cas français, les Ministères chargés de l'Intérieur et de la Défense ont déjà des allocations qui ont été accordées par l'ANFR. S'agissant de la bande des 700 MHz, c'est un spectre alloué en Europe aux radiodiffuseurs à la suite d'un premier dividende numérique. La question se pose donc de savoir si les radiodiffuseurs sont prêts à renoncer à ce spectre au profit d'autres utilisateurs intéressés, tels que la communauté des opérateurs commerciaux. Cette dernière a récemment publié une position par laquelle elle faisait état de la recherche de spectre supplémentaire. Il y a donc un vaste débat et il convient de mettre en perspective le poids de la sécurité publique par rapport aux autres acteurs économiques. Pour un équipementier, si des préférences sont exprimées en France, il ne faut pas oublier de replacer cela dans un contexte européen plus large.

Pour un expert du service des technologies et des systèmes d'information de la sécurité intérieure (Ministère de l'Intérieur, ST(SI)²), on se projette plutôt sur une solution de type I+II évoluant progressivement vers la solution IV, sans écarter le scénario III. Le choix potentiel n'est pas encore forcément validé, estime-t-il. Même s'il y a des réseaux dédiés, que ce soit en 400 MHz ou en 700 MHz, il n'y a pas de certitude que la capacité en débit suffise au besoin total des services d'urgence et de sécurité ; à plus forte raison, si le choix se porte sur un grand réseau unique – ce qui est la tendance – un réseau commun à l'ensemble des services de sécurité et d'urgence, avec une vision très large, étendue potentiellement à des opérateurs d'énergie, de transport, à la police municipale, au service des routes etc. Toutefois, plus il y aura d'utilisateurs du réseau par souci de

maîtrise de la contrainte budgétaire, moins le réseau unique aura de capacité à satisfaire tous les besoins, et donc le segment commercial conservera un caractère complémentaire probablement indispensable encore longtemps, estime cet expert.

L'Autorité de régulation des communications électroniques et des postes (ARCEP) rencontre régulièrement tous les utilisateurs de réseau de PMR dans le cadre de la gestion des fréquences. Pour l'ARCEP, ces utilisateurs ont un message relativement commun, qu'il s'agisse des opérateurs d'importance vitale, du ministère de l'équipement, ou de la santé, qui ne sont pas affectataires de fréquences : ils ont déjà un réseau et veulent l'utiliser au mieux ; ils sollicitent donc des fréquences supplémentaires par rapport à celles attribuées actuellement. La réponse de l'ARCEP est que la bande des 400 MHz est très majoritairement déjà utilisée pour ce type d'application et qu'elle n'est pas extensible. Il faut regarder collectivement comment répondre au problème de spectre additionnel. Cela ne peut pas être au sein de la bande des 400 MHz, estime l'ARCEP. Collectivement, dans cette bande, il n'y a pas de spectre additionnel, à moins de faire des choix entre utilisateurs plus prioritaires que d'autres et donc d'attribuer du spectre additionnel disponible dans des bandes plus hautes, potentiellement un peu moins utilisées.

Pour l'ANFR, il convient également d'évoquer le dimensionnement du réseau dans le temps et en fonction des budgets. Compte tenu de l'importance du délai de déploiement des réseaux dédiés, ne serait-il pas préférable de doter les utilisateurs de terminaux multi-bandes et multi-standards incorporant l'ensemble des applicatifs et applications qui seront utiles, s'interroge ce régulateur ? On utilisera des réseaux dédiés au fur et à mesure de leur mise en place, ainsi que des réseaux commerciaux chaque fois qu'il n'existera pas de couverture par un réseau dédié. C'est là qu'interviennent aussi les pouvoirs publics, et ce que fait par exemple l'Allemagne en imposant aux opérateurs commerciaux des couvertures dans des zones défavorisées telles que les zones rurales. Une telle solution présenterait de plus l'intérêt de prendre en compte la dimension européenne, estime ce régulateur, parce que l'Allemagne n'a pas encore achevé le déploiement de son nouveau réseau dédié.

Il y a des applications qui sont aujourd'hui considérées comme critiques (dites « mission critical ») et qui sont offertes par l'infrastructure existante dédiée. À côté de cela, estime un opérateur commercial, commencent à apparaître d'autres usages développés à partir d'une nouvelle technologie, le standard LTE, qui a notamment permis aux monde commercial d'accéder à des applications temps réel vidéo. À partir de là, les utilisateurs sont en train de définir des usages qui pourraient être apportés dans les activités PPDR ou PMR, où n'existe pas encore une vision très claire des besoins pour ce type d'applications, observe un expert. Avant de définir le scénario, il faut définir les applications « mission critical », estime un opérateur : s'agit-il d'applications dont on a besoin partout sur le territoire ou pas ? Sont-elles nécessaires en cas de catastrophe, lorsque l'infrastructure est endommagée ? En pareil cas, il faudrait pouvoir disposer de réseaux ad hoc temporaires pour lesquels des fréquences sont à définir. S'agissant de la question de la couverture des réseaux commerciaux, cet opérateur estime que le régulateur pourrait très bien définir de nouveaux engagements dans le cadre de leurs licences, afin de pallier les insuffisances en termes de couverture du territoire. Il y a plusieurs autres solutions qui mériteraient d'être examinées avant de statuer. Force est de constater que, à chaque fois, les avancées technologiques et les innovations bénéficient en premier lieu aux écosystèmes jouissant d'économies d'échelle, donc aux réseaux commerciaux. Les utilisateurs PPDR et PMR exploitant un réseau dédié, seront toujours confrontés avec un temps de retard à ce problème d'évolution technologique. Faut-il continuer sur cet enchaînement, ou privilégier l'utilisation des réseaux commerciaux, s'interroge cet opérateur ? Cela ramène à la question de la gestion des priorités en situation d'urgence. À cet égard, il semblerait que la position des opérateurs commerciaux commence à évoluer. Aux États-Unis, un

haut responsable de l'opérateur commercial Verizon a ainsi récemment défendu l'idée de partager du spectre avec les utilisateurs du secteur public[179].

Il est nécessaire de caractériser la crise et de s'interroger sur les besoins, considère pour sa part un expert du Conseil général de l'économie, de l'industrie, de l'énergie et des technologies (CGEIET). C'est précisément la démarche en cours actuellement au niveau européen. En effet, dans le cadre de la décision en matière de politique de gestion du spectre adoptée en février 2012 par l'Union européenne, le groupe FM49 de la CEPT analyse les besoins, définit des niveaux de criticité des applications permettant d'y répondre et en déduit le spectre nécessaire. Une matrice a été élaborée pour présenter cette analyse[180] ; elle est complétée par un catalogue descriptif.[181] Les travaux sont en cours.

De plus, selon cet expert, on pourrait très bien imaginer une organisation s'appuyant au quotidien sur des réseaux commerciaux et qui disposerait d'un réseau d'ultime secours. Il conviendra cependant de former les utilisateurs afin qu'ils soient à même de faire fonctionner le réseau d'ultime secours en situation d'urgence. Des exercices périodiques sont nécessaires pour tester les procédures d'utilisation. Cependant, dans l'absolu, ce réseau de secours sera peu utilisé, ce qui limite aussi la possibilité de détection précoce et la correction des dysfonctionnements. Par exemple, il a été constaté au moment de l'Ouragan Katrina que des terminaux satellites n'étaient pas chargés et que des utilisateurs ne savaient pas s'en servir, rappelle un équipementier : « *Je pense qu'il est important au niveau de l'équipe utilisateur que chaque agent ait le plus possible l'habitude d'utiliser le terminal qu'il met en œuvre en situation de crise* ». De plus, pour cet équipementier, il convient de s'interroger sur le partage des responsabilités en cas d'utilisation d'un réseau commercial et de défaillance de ce dernier, qui ne permettrait plus d'apporter de secours aux personnes.

Mais le retour d'expérience a fait apparaître un bilan plutôt contrasté. « Quand on parle disponibilité, ce n'est pas parce qu'un réseau est réputé être un réseau des forces de sécurité qu'il est nécessairement ou obligatoirement plus disponible qu'un réseau commercial. Là, il faut faire attention au langage parce qu'un réseau commercial, justement pour des raisons commerciales, fait l'objet d'un certain soin ; des moyens peuvent être accordés, le réseau est maillé et il peut être en fait beaucoup plus disponible » estime un responsable du CGEIET au vu de ce bilan.

Cette problématique se situe à la charnière entre des technologies et des usages, dont on voit bien que, dans la vie courante, ils évoluent avec une rapidité extraordinaire. Si l'on revisite l'usage que chacun d'entre nous faisait de son téléphone portable il y a seulement quinze ans, que l'on effectue la comparaison avec les possibilités actuelles, et que, dans le même temps, les pouvoirs publics doivent faire face à des décisions qui demain engageront l'Etat sur 15 à 20 ans, comment réagir, s'interroge une responsable du CGEIET ?

Pour Réseau de transport de l'électricité (RTE), il ne faut pas opposer réseau dédié et réseau opéré. Il faut utiliser les deux types de réseaux. Avoir son propre réseau dédié permet de garantir certaines sécurités en cas de crise. Mais, par ailleurs, personne n'a les moyens ni ne peut garantir un choix technologique pour 20 ou 30 ans. C'est la raison pour laquelle il est nécessaire de faire appel à des opérateurs ; il convient donc de trouver un juste équilibre entre une partie dédiée et une partie opérée. Dans certains cas, les moyens de communication opérés augmentent la résilience du réseau global. Pour un opérateur d'infrastructure vitale, le seul moyen d'augmenter la

[179] Verizon's McAdam, in Keynote Address, Advocates for Shared Spectrum by Public and Private Sectors (The Sacramento Bee, 9 mai 2012)
[180] FM 49 - Matrice sur les nouveaux usages - draft
[181] FM49 Catalogue - Matrix (juin 2012)

résilience, c'est de mutualiser les infrastructures. Il faut faire en sorte que les deux types de réseaux puissent coexister.

Les deux réseaux sont complémentaires, confirme un expert du ST(SI)². Le fait d'avoir une double dotation en radio PMR et dans le segment commercial amène naturellement de la résilience et de la complémentarité. Tel est le cas des agents de la Gendarmerie : certaines zones sont couvertes par le réseau RUBIS et non par ceux des opérateurs commerciaux, tandis que la réciproque est évidemment vraie.

Un autre équipementier partage également ce point de vue sur la mutualisation des réseaux. Il ajoute qu'imaginer le futur pour les 10 ou 20 prochaines années est l'un des défis majeurs que tentent de relever au quotidien les organismes de régulation. Ils font des paris au niveau mondial, pas forcément sur la technologie, mais sur le fait que du spectre sera nécessaire pour écouler un certain trafic permettant d'utiliser ou offrir des services à des utilisateurs particuliers comme la police, les forces de sécurité ou des opérateurs d'importance vitale. La technologie devra permettre d'utiliser ces ressources au mieux. S'il n'est pas possible d'avoir une certitude absolue sur les usages futurs, il est cependant certain que des ressources seront nécessaires pour être capable de supporter des applications critiques ou vitales. Au dernier salon Euro-Satory, des stands de la police nationale et de la Gendarmerie ont présenté des véhicules dotés d'applications orientées autour de la vidéo, de la surveillance, pour la transmission des données, et qui préfigurent ce que pourra être l'usage de demain. C'est un exemple possible ; cependant, la situation sera peut-être totalement différente dans quelques années. Mais il y aura toujours besoin d'avoir des ressources spectrales, certainement en partie dédiées, certainement une partie plus en commun avec un opérateur commercial à définir. La ressource spectrale est vraiment très stratégique.

Conclusion

Au terme de ce mémoire, nous souhaitons insister plus particulièrement sur trois points. En premier lieu, il convient de souligner le consensus qui se dégage au plan international concernant le choix d'une future technologie standard, telle que la norme LTE, pour les réseaux de communication utilisés par les forces de sécurité, de secours et les opérateurs d'importance vitale. Cette nouvelle technologie, qui se déploie par ailleurs sur les réseaux commerciaux ouverts au public, permettra d'augmenter considérablement les capacités de trafic, notamment par la transmission de données ; de réaliser des économies d'échelle ; d'améliorer l'interopérabilité. En cours de déploiement Amérique du Nord, en Asie et au Moyen-Orient, son retour d'expérience bénéficiera à l'Europe à l'horizon de 2020, accompagné d'économies d'échelle bien plus importantes que par le passé.

En second lieu, les nouveaux besoins et les usages suscités par l'introduction des nouvelles technologies supposent l'obtention de ressources spectrales additionnelles. Ce mémoire a souligné quelques-uns des enjeux économiques et industriels lié à la gestion du spectre. Si des efforts ont déjà été réalisés en France et en Europe en termes d'optimisation du spectre alloué à la sécurité publique, les nouvelles applications envisagées, leur doctrine d'emploi et leur traduction en bande passante restent encore à définir afin de permettre aux régulateurs d'être le mieux à même de répondre aux demandes des différentes parties prenantes.

Enfin, ce mémoire a souligné une évolution tendancielle à l'intégration progressive de différentes entités au sein de grands réseaux nationaux dédiés. Au-delà de cet acquis, les échanges avec l'ensemble des parties prenantes françaises ont abouti à une vision partagée sur l'intérêt des complémentarités avec les réseaux commerciaux ouverts au public, afin d'une part d'augmenter la

résilience globale des moyens de communication de sécurité et pour permettre, d'autre part, une transition progressive de ces réseaux vers la technologie LTE. Dans ce cadre, il appelle notamment l'attention sur la nécessité de mettre en place en France un mécanisme institutionnel de gestion des priorités d'appel au profit des forces de sécurité et de secours et des opérateurs d'importance vitale.

Annexes

Personnes consultées

ARDOUIN	Philippe	Chef de projet	Gaz Reseau Distribution France (GrDF)
ARVIDSSON	Viktor	Directeur de la stratégie et des affaires réglementaires	Ericsson France
BADRINATH	Vivek	Directeur exécutif	Orange Business Services
BARREIRO	Edouard	Directeur adjoint, département des études	UFC-Que Choisir
BEAUGRAND	Vincent	Responsable du bureau Premier Recours	Ministère du travail, de l'emploi et de la santé, Direction générale de l'offre de soins
BON	Dominique	Rapporteur d'une nouvelle étude sur les réseaux PMR du ministère	Direction des systèmes d'information et de la communication du ministère de l'intérieur (DSIC/MIOMCT)
BREGANT	Gilles	Directeur général	Agence nationale des fréquences radio (ANFR)
BRISSET	Hélène	Directrice de projet Réseau interministériel de l'Etat	Direction interministérielle des systèmes d'information et de communication (DSIC), Premier ministre
BROUET	Jérôme	Responsable de l'innovation pour le secteur public	Alcatel-Lucent
BRUNI	Eric	Ingénieur Général de l'Armement,	Directeur adjoint Direction générale des systèmes d'information et de communication (DGSIC), ministère de la défense
BUFFAT	Marine	Chargée de mission médecine d'urgence	Ministère du travail, de l'emploi et de la santé, Direction générale de l'offre de soins
CANTON	Anne-Florence	chef du bureau C1	Direction générale des douanes et droits indirects
CELLMER	Jean	Chef de l'Unité Vie du Réseau Direction du Projet GSM-Rail	Réseau Ferré de France
CHENET	Joël	Vice-Président Strategy & Business Development	Thales Alenia Space
CHOLLEY	François	Président de la section régulation et ressources	Conseil général de l'économie, de l'industrie, de l'énergie et des technologies (CGEIET)

CHOUET	Stéphane	Relation client et développement de l'offre & Tétracité Opérateur de services de communication	RATP - Département des systèmes d'information et de télécommunications
COROLLEUR	Olivier	Adjoint au Directeur Veille technologique et relations avec les équipementiers	Autorité de régulation des communications électronique et des postes (ARCEP)
COURSAGET	Alain	Adjoint au Directeur de la protection et sécurité de l'état	Secrétariat général de la défense et de la sécurité nationale (SGDSN, Premier Ministre)
DAS	Hans	Chef d'unité A/5 - Politique de Protection civile	Commission européenne, Direction générale ECHO
DAVALO	Eric	CTO	Cassidian
DELANNOY	Xavier	Adjoint au chef du bureau C2 Architecture et sécurité	Direction générale des douanes et droits indirects
DUDOUYT	Georges	Chef du bureau C2	Direction générale des douanes et droits indirects
FAIVRE	François	Consultant Manager, Auteur du rapport TERA	Groupe ON-X
FORCE	Pierre	Senior Expert	EADS-Cassidian
FOURMEL	Jérôme	Directeur général des douanes et droits indirects (DGDDI)	Sous-direction C Systèmes d'information et télécommunication
GUITOT	Jean-Jacques	Chef du département planification et prospective	Agence nationale des fréquences radio (ANFR)
GYDE	Laurent	Directeur technique	GIP RENATER
HERVIEU	Thomas	Directeur associé	LD consultants
ISNARD	Numa	Chargé de mission	Association française des opérateurs de réseaux et de services de télécommunication (AFORS Télécom)
JAFFRE	Yann	Directeur stratégie technologies, Direction stratégie	SFR
JEANNERET	Jean-Claude	Directeur général	Institut Mines-Telecom
JUILLARD	Patrice	Membre de la Mission ministérielle de pilotage et de convergence des réseaux et expert en fréquence	Direction des systèmes d'information et de la communication du ministère de l'intérieur (DSIC/MIOMCT)
KIEFFER	Claude	Chef du pole des moyens généraux	Direction générale de la sécurité civile et de la gestion des crises (DGSCGC), Minsitère de l'intérieur
KLES	Virginie	Sénateur d'Ille-et-Vilaine (Bretagne), Vice-Présidente de l'office parlementaire d'évaluation des choix scientifiques et technologiques	Sénat

LAUNE	Michel	Sous-directeur des réseaux et des technologies avancées	STSI²
LE FLOCH	Yves	Conseiller scientifique du SGDSN	Secrétariat de la défense et de la sécurité nationale (SGDSN)
LIDUREAU	Pierre-Philippe	Directeur de programme Infrastructure Nationale Partagée des Télécommunications (INPT)	Direction des systèmes d'information et de la communication du ministère de l'intérieur (DSIC/MIOMCT)
MADELIN	Robert	Directeur général	Commission européenne, Directorate-General for Information Society and Media
MARTIN	Gilles	Colonel, Chef du bureau des communications opérationnelles	Service des technologies et des systèmes d'information de la sécurité intérieure STSI², Ministère chargé de l'Intérieur
MIRABAUD	Philippe	Chef de la mission ministérielle de Pilotage et de convergence des réseaux (MMPCR)	Direction des systèmes d'information et de la communication du ministère de l'intérieur (DSIC/MIOMCT)
MOREL	Mathieu	Direction des systèmes d'information et de la communication	Ministère de l'intérieur (DSIC/MIOMCT)
PAILLOUX	Patrick	Directeur général	l'Agence nationale de la sécurité des systèmes d'information (ANSSI)
PAPPALARDO	Bernard	Général, Chef du service des technologies et des systèmes d'information de la sécurité intérieure (STSI^2), Ministère de l'intérieur, de l'Outre-mer, des collectivités territoriales et de l'immigration - Direction générale de la gendarmerie nationale	Service des technologies et des systèmes d'information de la sécurité intérieure (STSI2)
RAMES	Jacques	Ex président Motorola France (2009-2011)	
RIVIERE DE LA SOUCHERE	Arnaud		Bureau Assistance et Conseil (ANSSI)
RIVOAL	Gérard	Ingénieur en Chef	Chargé de mission DID, Ministère de la Défense
ROUSSEAU	Jérôme	Directeur Veille technologique et relations avec les équipementiers	Autorité de régulation des communications électronique et des postes (ARCEP)
ROSTAMBEIK	Sasan	Direction de la Stratégie	SFR
SILVY	Alain	Général, inspecteur de l'armée de l'air	Ministère de la Défense et des Anciens combattants État-major de l'armée de l'air Inspection de l'armée de l'air
TAUPIN	Fabrice	Lieutenant-Colonel, Adjoint au chef du bureau des communications opérationnelles	STSI²

VIALA	Jean-Claude	Directeur des systèmes d'information et des télécommunications	Réseau de transport d'électricité (RTE)
VIOLLET	Philippe	Adjoint au chef de la mission ministérielle de pilotage et de convergence des réseaux	Direction des systèmes d'information et de la communication du ministère de l'intérieur (DSIC/MIOMCT)

Glossaire

ADRASEC : Association des radioamateurs pour la sécurité civile
AIRWAVE : réseau PPDR TETRA britannique
ACROPOL : Réseau de radiocommunications numérique sécurisé de la police nationale faisant partie de l'INPT (TETRAPOL)
AGURRE : Association des grands utilisateurs de réseau radio d'exploitation
ANFR : Agence nationale des fréquences radio
ANTARES : Système de radio TETRAPOL des forces de sécurité civile faisant partie du réseau INPT
AM : Modulation d'amplitude
ARCEP : Autorité de régulation des communications électroniques et des postes
ASTRID : Réseau PPDR TETRA Belge
ATEX : Atmosphère explosive
AUT : Architecture unique des transmissions
AVACMA : Alarme de veille automatique par contrôle appui
BNP : Banque nationale de Paris
CAPEX : Dépenses d'investissement
CEA : Commissariat à l'énergie atomique et aux énergies alternatives
CEPT : Conférence européenne des administrations des postes et télécommunications
CGEIET : Conseil général de l'économie, de l'industrie, de l'énergie et des technologies
CIC : Centre d'information et de commandement
CORAIL-NG : réseau TETRAPOL de la Gendarmerie mobile en Ile-de-France faisant partie du réseau INPT
CORG : Centre opérationnel et de renseignement de la Gendarmerie
CPE : Contrat premier embauche
CTA : Centre de traitement d'alerte
C2000 : réseau PPDR TETRA Néerlandais
DSC : Direction de la sécurité civile et de la gestion des crises (Ministère de l'Intérieur)
DSIC : Direction des systèmes d'information et de communication (Ministère de l'Intérieur)
DMO : Direct mode operation
DMR : Digital mobile radio – technologie simplifiée de radio PMR numérique
EDF : Électricité de France
EDGE : Enhanced Data Rates for GSM Evolution
ERDF : Électricité Réseau Distribution de France
ETP : Équivalent temps plein (emploi)
ETSI : Institut européen des normes de télécommunication
FCC : Federal communication commission aux USA
FM : modulation de fréquence
FM 49 : Groupe de travail de la Conférence européenne des administrations des postes et télécommunications (CEPT) dont l'objectif est de trouver une solution pour un spectre harmonisé pour les futures communications PPDR à très haut débit
GDF : Gaz de France
GHN : Government Home Network (Ericsson) – concept d'un opérateur de réseau mobile virtuel (MVNO) pour les forces de sécurité et de secours s'appuyant sur les réseaux mobiles existants ouvert au public
GPRS : General packet radio service
GSM : Global System for Mobile Communications
GSM-R : GSM-rail, norme dérivée du standard GSM et utilisée dans les réseaux ferroviaires
HSDPMA : technologie dérivée de l'UMTS, (3,5G)

IMPEX : coûts de construction
INPT : Infrastructure nationale partagée des transmissions
OIV : Opérateurs d'importance vitale
OPEX : Dépenses de fonctionnement
LOLF : Loi organique relative aux lois de finance
LOPSI : Loi d'orientation pour la sécurité intérieure
LTE : Long term evolution
MHz : Mégahertz (unité de mesure de fréquence)
MVNO : Opérateur de réseau mobile virtuel
Nødnett : réseau PPDR TETRA Norvégien
PCRD : programme-cadre européen de R&D
PMR : Professional mobile radio ou private mobile radio
PPP : Partenariat public-privé
PTT : clé d'émission Push to talk
PPDR: Public protection and disaster relief, (voir aussi PSS)
PSS: Public safety and security
P25 : norme de radio PPDR utilisée principalement aux USA et en Australie
TEDS : TETRA enhanced data service
TETRAPOL : Technologie numérique propriétaire mise en œuvre sur les réseaux PPDR
TETRA : Terrestrial trunked radio – technologie numérique ouverte mise en œuvre sur les réseaux PPDR
TETRACITE : réseau TETRA de la RATP ouvert à des tiers
T.S.F. : Téléphonie sans fil
RAIMBAUD : Réseau interministériel de base uniformément durci (Réseau téléphonique interministériel de défense)
RAMAGE : Réseau Radiophonique Mobile Automatique pour GDF et EDF
RATP : Régie autonome des transports parisiens
ROAMING : au sens opérateur commercial du terme, désigne plus généralement la capacité des clients à accéder à leurs services de téléphonie mobile (voix ou données) depuis différents réseaux
RFF : Réseau Ferré de France
RGT : Partie fixe du réseau du Ministère chargé de l'Intérieur
RNA : Réseau national d'alerte
RUBIS : Réseau TETRAPOL de la Gendarmerie nationale
SAIP : Système d'alerte et d'information des populations
SAMU : Service d'aide médicale urgente
SCADA : Systèmes de contrôle-commande
SDIS : Service départemental d'incendie et de secours
SFR : Société française radio-électrique (Début du XXès)
SFR : Opérateur commercial de téléphonie mobile
SIRDEE : Sistema de Radiocomunicaciones Digitales de Emergencia del Estado, réseau PPDR TETRAPOL Espagnol
SMUR : Service médicalisé d'urgence
SNCF : Société nationale des chemins de fer
SOCRATE : réseau dédié du ministère de la Défense
SSO : Protocole d'authentification centralisée
SZSIC : Service zonal des systèmes d'information et de communication (Ministère de l'intérieur)
UIC : Union internationale des chemins de fer
UIT : Union internationale des télécommunications
UTC : Utilities Telecom Council, association des opérateurs de télécom des entreprises d'énergie
UMTS : Universal Mobile Telecommunication System, technologie de téléphonie mobile de troisième génération (3G)

VIRVE : réseau PPDR TETRA Finlandais
WiMAX : technologie 4G
2G : technologie de seconde génération (voir GSM)
3G : technologie de troisième génération (voir UMTS)
4G : technologie de quatrième génération (voir LTE)