Inspection générale de l'Administration
07 – 023 - 01

Conseil général des Ponts et Chaussées

Conseil général des technologies de l'information
III – 2 – 3 - 2007

Contrôle général des Armées
2061/DEF/CGA/SIA/MEI/JTX

Inspection générale des Finances

Conseil général des Mines

Rapport sur

la résilience des réseaux de télécommunications

présenté par:

Gilles SANSON
Inspecteur général
de l'administration

Bernard FLURY-HERARD
Ingénieur en chef
des ponts et chaussées

Jean CUEUGNIET
Ingénieur général des
télécommunications

Xavier de THIEULLOY
Contrôleur général
des armées

André TANTI
Inspecteur général
des finances

François BARTHELEMY
Ingénieur général
des mines

Juin 2007

Sommaire

2/ C'est pourquoi une posture de sécurité civile beaucoup plus circonspecte à l'encontre de ces risques mériterait d'être adoptée. 33

Les pistes ouvertes de réflexion visent à:

21/ Conforter d'abord l'efficacité de notre dispositif d'urgence. 33

- privilégier effectivement l'échelon centralisé de réaction.

- élargir la notion de priorités de rétablissement.

- planifier la communication d'alerte.

22/ Sécuriser ensuite spécifiquement et plus complètement la sphère administrative. 35

- garantir sur la durée l'étanchéité des réseaux de sécurité propres à l'administration.

- imposer pour les services publics névralgiques des prescriptions plus strictes de sécurité des télécommunications.

- mieux prémunir l'administration contre les risques engendrés par l'externalisation croissante de ses systèmes d'information.

23/ Inciter autant que faire se peut les opérateurs à intégrer plus d'impératifs de sécurité. 37

- reconstituer préalablement au sein de l'Etat un pôle consistant de dialogue technique avec les opérateurs.

- développer une conception extensive de la démarche SAIV/ DNS.

- préférer de façon générale une logique d'incitation financière plutôt que de prescription normative.

- définir, à défaut, un certain nombre de normes quantifiées sur la qualité de service susceptible d'être exigée de la part des opérateurs.

- renforcer, en dernière instance, les pouvoirs de sanctions de l'administration à l'encontre des exploitants de réseaux.

24/ Promouvoir en dernier lieu des éléments de robustesse simples à mettre en œuvre ou qui ont déjà fait leur preuve. 42

- standardiser des équipements à disposition de l'usager qui soient de conception plus sûre.

- tirer les conséquences de la résistance particulière et jusqu'ici avérée des messageries.

*
* *

La résilience des réseaux de télécommunications

a) La France, à mesure qu'elle se développe, étend et interconnecte des réseaux de types multiples dont elle devient de plus en plus dépendante. *Alors que des menaces nombreuses (risques technologiques, actes de malveillance, catastrophes naturelles) pèsent sur ces différents réseaux, les risques de répercussions de l'un à l'autre d'une panne ou d'une détérioration sont accrus par leur enchevêtrement*.

Pour autant, si la vulnérabilité de notre société apparaît ainsi intuitivement très grande, elle reste globalement mal mesurée et la préparation pour y faire face encore laborieuse.

Certes, s'agissant d'une rupture d'alimentation énergétique et plus particulièrement d'une panne de notre réseau d'électricité, la nature des risques encourus et leurs effets sur la vie économique et sociale apparaissent maintenant relativement correctement appréhendés.

En revanche, ceux qui ont trait aux *dysfonctionnements propres des réseaux de télécommunications* le sont de façon nettement moindre : les études disponibles sont rares alors que le bouleversement constant des technologies et du monde des télécommunications non seulement rend complexe toute analyse de cette question mais périme aussi très vite les jugements qui peuvent avoir cours.

b) Aussi, *le Conseil national de la sécurité civile a souhaité qu'un groupe de travail interministériel porte prioritairement son attention sur ce problème*.

Il ne s'agissait pas, dans le cadre du *mandat* et du temps impartis, de chercher à formuler à ce stade des propositions de solution. Le champ couvert par la réflexion était défini limitativement. Il convenait avant tout de prendre la mesure de la vulnérabilité de ces réseaux, notamment en envisageant, comme première piste de travail, divers scénarii de pannes possibles, avec une ambition: celle d'aider à ce titre à l'élaboration en cours du volet "télécommunications" du plan Orsec.

Ce *groupe de travail* a réuni les membres de 6 corps de contrôle ou conseils généraux de ministères différents: Inspection générale de l'administration, Conseil général des technologies de l'information, Conseil général des ponts et chaussées, Contrôle général des armées, Inspection générale des finances, et Conseil général des mines.

Il a procédé aux *auditions* des représentants tant des principaux opérateurs (France Télécom, Bouygues Télécom, SFR, Neuf/Cégétel, Iliad/Free…) que des administrations (Industrie, Défense, Intérieur, SGDN, CICREST[1]) et de l'autorité de régulation (ARCEP[2]) concernées. Le cercle a été élargi aux responsables de différentes entreprises publiques (EDF, RTE, RATP, SNCF), de réseau spécialisé (GIP RENATER), d'hébergeurs (ATOS-Worldline, Telehouse), d'acteurs centraux de la vie économique (Groupement des cartes bancaires, Association française des banques) et de défense des usagers (AFUTT[3]).

[1] CICREST : commission interministérielle de coordination des réseaux et des services de télécommunications.
[2] ARCEP : autorité de régulation des communications électroniques et des postes.
[3] AFUTT : association française des utilisateurs de télécommunications.

c/ Au terme de cette première réflexion, c'est un ***constat*** assez nuancé mais, exprimé avec beaucoup de prudence, plutôt rassurant *à court terme* que le groupe de travail est tenté de formuler quant à la vulnérabilité globale de nos réseaux de télécommunications.

Mis à part une rupture massive et durable de l'alimentation en électricité (dont les répercussions sont majeures et globales sur les dispositifs de télécommunications), les occurrences les plus probables avec lesquelles nous pourrions avoir à composer semblent emporter *des risques d'ampleur qui serait limitée*. Un grand nombre de facteurs sont en effet à prendre en considération. Cependant, la multiplication désormais du nombre des systèmes de télécommunications concurrents (systèmes reposant par ailleurs sur des technologies pour partie indépendantes) devrait permettre le plus souvent des recours de substitution en cas de panne de l'un d'eux.

A *moyenne échéance*, s'exprime en revanche une foule d'incertitudes liées notamment à la place de plus en plus prépondérante d'Internet au sein des systèmes de télécommunications. Ce contexte ne rend plus possible d'exclure *a priori* l'hypothèse d'un effondrement éventuel significatif de ces derniers.

d/ C'est pourquoi il est proposé d'adopter une posture de sécurité civile qui soit très circonspecte à l'encontre des risques exposés.

Différentes ***propositions*** de mesures sont formulées à ce titre.

À ce stade de l'analyse, elles ne prétendent cependant ni à l'exhaustivité, ni à la pertinence assurée. Elles doivent être conçues comme un premier point d'ancrage à la réflexion et comme une contribution méthodologique au travail en cours de planification de la prévention et des secours.

*

1/ Le constat d'ensemble n'est partiellement rassurant qu'à court terme.

Si les dysfonctionnements ponctuels de systèmes de télécommunications sont jusqu'à présent relativement courants (1.1), plusieurs facteurs accréditent malgré tout l'idée:

- que, à bref horizon, un effondrement global des réseaux est peu probable (1.2),

- et que le danger, aujourd'hui, d'une répercussion en cascade de la défaillance d'un ou de plusieurs de ces réseaux doit être, en tout état de cause, relativisé (1.3).

A moyenne échéance (4/5 ans) en revanche, les évolutions discernables dans le monde des télécommunications et de l'information recèlent de nombreuses inconnues qui ne peuvent manquer d'inquiéter (1.4).

1.1 / Les dysfonctionnements observés jusqu'à présent sont nombreux et les menaces multiformes.

De fait, les opérateurs ne sont épargnés ni par les pannes matérielles, ni par les pannes logicielles.

1.1.1/ Des pannes matérielles variées continuent d'affecter les réseaux.

1.1.1.1/ Les opérateurs sont confrontés quotidiennement à des problèmes d'équipements défaillants.

Cependant, ceux-ci sont en général gérés sans conséquence grave pour les usagers qu'il s'agisse d'artères coupées ou de sites ponctuellement hors service:

- *des câbles ou fibres coupés* :

Alors que les acheminements interurbains sont presque toujours multiples, les opérateurs savent généralement pallier dans des délais raisonnables la moindre coupure d'artère, même si l'acheminement de substitution emprunté a souvent une capacité moindre et pâtit d'un certain taux d'échec. En tout état de cause, les boucles locales impliquées ne concernent par nature qu'un nombre restreint d'abonnés. Par ailleurs, les organismes névralgiques (hôpitaux, pompiers…) susceptibles d'être concernés sont censés, *a priori*, à la fois avoir été sensibilisés par l'administration et par les opérateurs sur la nécessité de prévoir pour eux même une double desserte et s'être équipés en conséquence.

- *des sites hors service* :

Les équipements périphériques sont les plus concernés. Les *stations radio (BTS) des opérateurs mobiles* subissent ainsi régulièrement des pannes, que ce soit du fait d'intempéries locales ou par rupture ponctuelle d'alimentation en électricité. SFR a signalé à cet égard avoir en permanence de l'ordre d'une centaine de sites en défaut sur ses 15 000 BTS en fonctionnement. Toutefois, grâce à leurs chevauchements de couverture les uns par rapport aux autres, l'effet sur les usagers de cette situation est quasiment imperceptible.

Ces matériels, il est vrai, sont particulièrement vulnérables aux coupures d'alimentation énergétique. Ils ne possèdent pour la plupart qu'une autonomie sur batteries de l'ordre de 3 à 4 heures et ne comprennent pas de groupe électrogène de secours. Quant aux opérateurs qui en ont la charge, ils ne disposent pas d'un parc de générateurs toujours suffisamment bien réparti ou suffisamment important pour répondre aux besoins dès lors que ces derniers sont étendus.

Les *grands sites de commutation* sont par contre moins exposés à ce type de contingences en raison du nombre de précautions prises (équipements propres en groupes électrogènes, multiplication des alarmes incendie, attention portée aux problèmes de sécurité d'accès …) De ce point de vue, l'incendie du central survenu à *Lyon Sévigné* en novembre 1981 fait exception : un million d'usagers de la région Rhône Alpes avait, à cette occasion, été isolé du monde extérieur pendant 1 à 3 jours.

1.1.1.2 / Plus exceptionnellement mais régulièrement, les systèmes pâtissent aussi de catastrophes naturelles.

Les conséquences peuvent en être alors plus notables. Les *tempêtes de 1999*[4] en ont été l'exemple le plus marquant (mais il serait loisible de citer de nombreux autres évènements de même ordre, quoique sur des zones plus réduites, comme la tempête qui a soufflé sur la Bretagne en 1987 ou celle sur l'île de la Réunion en février dernier.)

Ces tempêtes ont, à l'époque, très sérieusement affecté nos réseaux de télécommunications à cause de leur intensité et de leur étendue, les 2/3 du territoire ayant été touchés. Deux dépressions, en effet, ont successivement traversé la France le dimanche 26 décembre et la nuit du 27 au 28 décembre. Les vents qui avaient dépassé 150 km/h dans plusieurs villes[5] ont provoqué près de 100 milliards de francs (soit de l'ordre de 15 milliards d'euros) de dégâts dont *1,12 milliard de francs de dégâts aux seuls réseaux de télécommunications* :

- *1 million d'abonnés* ont été privés dans ces circonstances de téléphone *fixe* tandis que 15% des sites de téléphone *mobile* avaient été mis hors service[6]. (La France ne comptait alors que 5 millions d'abonnés mobiles environ alors qu'ils dépassent 51,7 millions à présent : 15% des sites représenteraient donc probablement aujourd'hui une incapacité de communiquer pour près de 5 millions de détenteurs de mobiles);

- il a fallu *une semaine* environ pour remettre en état de fonctionnement les télécommunications sachant qu'au bout de 3 jours le nombre d'abonnés privés de téléphone fixe avait pu toutefois être divisé par deux[7].

[4] Cf. rapport de la mission interministérielle chargée de l'*évaluation des dispositifs de secours et d'intervention mis en œuvre à l'occasion des tempêtes des 26 et 28 décembre 1999* -juillet 2000-.
[5] Alençon, Paris, Metz, Colmar, La Rochelle, Clermont Ferrand… Le record étant de 198 km/h à l'Ile d'Oléron.
[6] Soit, notamment, 1400 sites *Itinéris* sur 9000.
[7] L'ensemble des autres réseaux avait été également détérioré: 3,5 millions de foyers avaient été privés d'*électricité.* (Le retour à la normale s'est effectué en une semaine environ mais avec un « coup de collier » plus net que pour les télécommunications puisque plus de la moitié d'entre eux avait pu être rétablie en 24 heures.)

Or, ces tempêtes se sont déroulées dans un contexte particulier qui en a malgré tout limité la portée dramatique. Elles ont eu lieu non seulement en période de faible activité mais alors, par ailleurs, que des centaines de cellules de crises avaient été pré activées dans la crainte du "bug de l'an 2000" et que des milliers de groupes électrogènes avaient été réquisitionnés dans ce cadre, moyens qui ont été immédiatement affectés au rétablissement des infrastructures.

1.1.2 / Les pannes logicielles sont également courantes.

Elles sont aussi bien d'origine interne qu'externe.

1.1.2.1 / Parmi celles ayant une origine interne, les plus notables récemment ont été analysées par le CGTI[8].

L'étude a porté sur trois cas intervenus en 2004, le premier mettant en cause un réseau fixe, les deux autres des réseaux mobiles :

► lors du *week-end du 30 au 31 octobre 2004,* **France Télécom** a connu un dysfonctionnement partiel de ses commutateurs MT25 (qui traitent 30% de ses abonnés) se traduisant par l'échec des appels "arrivée" longue distance vers ces centraux (les appels locaux continuant de leur côté à être acheminés normalement).

Si France Télécom a réagi en une heure environ, créant une cellule de crise au bout d'une heure et demie, la perturbation s'est poursuivie près d'une journée.

L'origine de ce trouble est une erreur humaine de configuration d'un équipement pare-feu à l'interconnexion du réseau téléphonique commuté avec le service VoIP. Ce problème a engendré en cascade des messages erronés vers les MT25, puis un désordre de fonctionnement de ces derniers eux-mêmes. Il est à noter que cet incident sur le réseau fixe n'a pas affecté le réseau mobile.

► le *mercredi 17 nov. 2004*, une panne majeure également a touché pratiquement tous les clients de **Bouygues Télécom**, interdisant les appels "départ" et "arrivée". Elle était due, à l'occasion d'une saisie importante de nouveaux numéros, à une défaillance logicielle d'une base (HLRV[9]) qui gère les profils des abonnés et leur localisation. Cet équipement était certes dupliqué mais en type "miroir", ce qui fait que l'équipement de secours existant s'est retrouvé insusceptible de prendre le relais.

Cette panne a commencé vers 6h du matin. Une cellule de crise a été déclenchée dès 7h30. Des mesures de corrections partielles ont été mises en oeuvre progressivement jusqu'à 13h, heure de correction de la panne elle-même. Toutefois, les perturbations se sont prolongées encore une partie de la journée.

► de la même façon, le *30 mars 2004*, le trafic à destination des mobiles **Orange,** après une période de dégradation progressive entre 16h00 et 19h00, a été totalement interrompu jusqu'à 20h50.

Quant à la *distribution d'eau, elle* a été parallèlement perturbée: 2,5 million de personnes ayant été privées d'*eau* (pour 40% d'entre elles pendant plus de 3 jours).

[8] *Enquête sur les dysfonctionnements récents ayant touché des opérateurs de télécommunications* – CGTI – décembre 2004.

[9] HLR : "*home location register"*.

Ce dérangement était lié à l'introduction (qui s'est mal passée) d'une fonctionnalité nouvelle sur les HLR et il s'est propagé ensuite au HLR de secours.

Depuis, des mesures ont été prises à la fois pour éviter que de tels incidents ne se reproduisent (grâce notamment à une duplication mieux conçue des HLR) et pour que l'information, dans des cas de figure similaires, circule de façon plus fluide entre tous les acteurs amenés à réagir (projet de création d'un guichet de contact unique au sein de l'administration).

Il reste que, selon le CGTI, *des pannes de cette nature restent inévitables dans un contexte de plus en plus informatisé et évolutif.* L'accélération de l'innovation dans les services proposés, l'interaction en temps réel d'un nombre croissant de bases de données, l'interconnexion de réseaux de plus en plus diversifiés et la convergence des mondes différents des télécommunications et de l'Internet rendent de plus en plus complexes les systèmes et "délicate et problématique une maîtrise exhaustive de l'ensemble des situations possibles".

En l'espèce, la réactivité des opérateurs a cependant été jugée convenable. Le temps de remise en état auquel on doit rester s'attendre dans ce genre d'hypothèses est estimé à quelques heures et, au plus, à une journée.

Avec le temps, des progrès ont, il est vrai, sans doute été réalisés si l'on se réfère, par exemple, à une panne comme celle qu'a connue le réseau **Transpac** en *juin 1985* : à la suite de la forte croissance du trafic Vidéotex, caractérisé par des communications courtes et nombreuses, l'unité de commande qui traitait les appels a été saturée. Cette situation a conduit à une altération prolongée du service pour la plupart des abonnés. Des solutions palliatives ont bien été mises en place en quelques jours. Cependant la situation n'est vraiment redevenue normale qu'au bout de deux semaines.

1.1.2.2/ Les attaques externes susceptibles d'engendrer des pannes sont, quant à elles, quasi permanentes.

Une illustration aiguë en est la diffusion du ver **Slammer**, qui a fortement perturbé Internet en *janvier 2003*. Ce ver a utilisé une faille Microsoft sur les serveurs de bases de données SQL pour, d'une part se propager en quelques minutes vers d'autres serveurs dans le monde entier et, d'autre part, émettre des messages saturant le réseau.

L'ensemble des opérateurs souligne, pour ce qui est d'Internet et de la messagerie, le jeu perpétuel du chat et de la souris, d'attaques et de défenses, auxquels ils sont soumis au quotidien. Près de 80% du trafic de la messagerie est actuellement composé de *spams* générés par des PC d'usagers ordinaires mais infectés, sachant que certaines organisations revendent pour quelques centimes d'euros le contrôle d'un PC capable d'envoyer des *spams*[10]. Les opérateurs sont donc contraints de renouveler en continu leurs dispositifs de protection, "*black listant*" les sites ou *FAI*[11] qui génèrent un trafic suspect, essayant de filtrer leur propre flux sortant afin de ne pas être eux mêmes "*black listés*" par d'autres, etc. Lors de tentatives d'intrusion, le flux est multiplié par un facteur de 10 à 1000 : "c'est comme si toutes les voitures de France convergeaient vers un arrondissement de Paris", rapporte un opérateur.

De fait, le déni de service[12] par infection de multiples serveurs (ou par des PC "*zombies*" préalablement infectés qui se déclenchent à une heure donnée) est difficile à conjurer, même si les diligences des opérateurs permettent d'amoindrir l'effet de ces attaques continuelles.

[10] Orange/ Wanadoo subit ainsi une attaque par seconde sur sa plate-forme de messagerie.
[11] *FAI*: fournisseur d'accès à Internet.
[12] Déni de service (*denial of service /DoS)* : saturation d'une portion du réseau, d'une ligne d'accès, d'un ordinateur sous une avalanche de paquets parasites.

1.2 / A bref horizon, sauf rupture prolongée de l'alimentation électrique, un effondrement global des réseaux apparaît peu probable.

Mis à part le cas d'une panne électrique d'envergure, les précautions prises par les opérateurs comme les caractéristiques, pour un temps encore, des réseaux devraient permettre d'éviter une paralysie d'ensemble des systèmes de télécommunications (qu'elle soit locale ou de grande étendue).

1.2.1/ Les opérateurs, de façon générale, ne semblent pas sous estimer l'ampleur des risques encourus.

1.2.1.1/ Ils expriment une perception assez identique des menaces: l'alimentation électrique est ressentie comme la principale vulnérabilité des réseaux.

Toute interruption de l'alimentation électrique a des répercussions fâcheuses dès qu'elle dépasse quelques heures. L'émission comme la réception sont alors désorganisées.

Jusqu'à *deux-trois heures de coupure*, la situation reste maîtrisée. Mêmes les sites radio ou commutation les plus précaires bénéficient en effet d'une autonomie énergétique minimale de cet ordre mais guère supérieure[13]. Ainsi, la panne électrique de près d'une heure subie le 4 novembre dernier en soirée (et dont ont pâti près de 5 millions de personnes dans la moitié nord de la France[14]) n'a pas eu d'impact sur la fluidité des télécommunications[15].

En revanche, *au delà de ce délai*, les équipements périphériques tombant progressivement en panne plus ou moins rapidement, les opérateurs, si la zone concernée est importante, ne disposent pas des moyens humains et matériels pour les secourir. La stratégie des opérateurs ne consiste pas, au demeurant, à se prémunir contre une panne durable (jugée très improbable) de l'alimentation électrique, mais plutôt de disposer autant que faire se peut (grâce à des batteries) d'une autonomie permettant de tenir jusqu'à l'intervention d'une équipe de dépannage. La disponibilité d'un groupe électrogène ne rentre que marginalement dans le choix d'un site radio.

Au bout d'une demi-douzaine d'heures, ne peut donc subsister de fait qu'un service de télécommunications excessivement dégradé à partir des seuls sites dotés de générateurs.

Ainsi:

- s'agissant des réseaux *mobiles*, fonctionnent certes la plupart des commutateurs (MSC[16]) mais un nombre dérisoire des sites radio. La couverture géographique n'est plus alors que de *quelques % du territoire* incriminé;

[13] La situation est également encore susceptible d'être tenue en main s'il s'agit d'une coupure plus longue mais dont le secteur concerné reste circonscrit, compte tenu à la fois du tuilage des champs couverts par les sites radio et de la possibilité d'acheminer si besoin un groupe électrogène de secours sur place.

[14] Cette panne s'est produite vers 22h à partir d'une défaillance en Allemagne du réseau de EON Netz qui a conduit à des procédures de délestages en chaîne dans toute l'Europe et particulièrement en France.

[15] Si l'on fait exception d'une part de certains phénomènes mineurs de déconnections de terminaux sur Internet et de reconnections un peu laborieuses et, d'autre part, de demandes massives d'information qui ont pu faire craindre ici ou là aux services d'urgence une éventuelle saturation de leurs lignes d'appels.

[16] MSC : *Message Switching Centers*.

- s'agissant du réseau *fixe*, si les cœurs de chaîne des centraux continuent à fonctionner grâce à des générateurs, il n'en est pas de même des unités de raccordement d'abonnés distants dont l'autonomie énergétique est limitée à quelques heures. France Télécom[17] estime qu'en cas de *black out* énergétique *un tiers des abonnés* fixes serait aujourd'hui privé de communications.

Cette proportion est appelée à augmenter notamment en raison de la *plus grande dépendance en énergie des installations chez l'abonné*. Le temps n'est plus, en effet, au fonctionnement "contre vents et marées" du téléphone fixe, grâce à l'alimentation 48V de la ligne France Télécom : désormais la plupart des postes vendus dans le commerce nécessitent une alimentation électrique propre (tel est le cas, par exemple, des téléphones "sans fil" ou des combinés "téléphone/répondeur/fax"). Il en est de même des "*boxes"*, ces boîtiers électroniques installés chez l'usager au bout de la ligne ADSL. Ainsi, les lignes totalement dégroupées ne fonctionnent plus en cas de panne électrique à domicile[18]. Faiblesse supplémentaire des "*boxes*": elles fonctionnent sur le modèle d'un ordinateur et mettent plusieurs minutes à se reconnecter après une panne d'alimentation. France Télécom a reconnu que, lors de la panne électrique de novembre dernier, certaines "*boxes*" avaient mis une heure à se reconnecter en raison de la charge.

Or, cette sensibilité majeure aux ruptures d'alimentation électrique est accentuée également par l'importance croissante prise progressivement dans les centraux par deux éléments :

- les besoins cruciaux de *climatisation* de matériels dont le fonctionnement ne tolère plus d'écarts de températures;

- la part des *équipements ADSL* à laquelle conduit le développement rapide de l'Internet haut débit et qui, malgré la miniaturisation et les progrès techniques, est fortement consommatrice d'énergie réduisant d'autant l'autonomie initiale des sites[19].

C'est pourquoi nos interlocuteurs (notamment Bouygues et SFR) se sont plaints de ne pas être *prioritaires vis à vis d'EDF*, autrement dit que leur situation en cas de délestage ne soit pas privilégiée.

Ce problème a été abordé avec EDF. Du fait de la dispersion de leurs installations sur le territoire et de la consommation relativement faible de chacune d'entre elles, les opérateurs n'ont pas le statut de "grand compte" auprès d'EDF. Ils ne bénéficient donc pas de priorités d'alimentation. Ce n'est pas non plus techniquement illogique car le réseau de distribution d'électricité est organisé à partir des départs des postes MT/BT[20]. Le fait d'avoir un abonné prioritaire sur un départ conduit à rendre la globalité de ce dernier (et ses milliers d'abonnés) prioritaire.

Par contre, rien n'empêche que les sites des opérateurs de communications électroniques soient systématiquement considérés comme *prioritaires pour le rétablissement du courant* à la suite d'un sinistre. Ce besoin devrait être mécaniquement pris en compte par les préfets dans leur planification de crise.

[17] France Télécom représente 80% des abonnés de téléphonie fixe. Or, les autres opérateurs, plus liés à des technologies de dégroupage total (*box*) sont encore plus vulnérables face aux coupures énergétiques.

[18] Dans le cas d'une ligne partiellement dégroupée, le fonctionnement reste possible sur la bande basse France Télécom avec un poste alimenté par la ligne.

[19] Tel opérateur rencontré a ainsi confié que la durée d'autonomie de ses centraux avait de la sorte été réduite par un facteur 6; autrement dit, là où celle-ci était auparavant de 24h, elle était désormais tombée à 4h.

[20] *MT/BT*: moyenne tension / basse tension.

C'est parce que non seulement les conséquences d'une rupture d'alimentation électrique sont donc grandes mais aussi parce que les opérateurs s'affirment particulièrement démunis pour s'en prémunir que cette menace est regardée comme la plus aiguë, bien avant les risques physiques aux installations (malveillance, incendie) ou les pannes de logiciels.

1.2.1.2 / Des efforts indéniables sont réalisés pour fiabiliser les réseaux.

L'impression a été confirmée à partir des rencontres ayant eu cours avec les responsables tant des principaux opérateurs de réseaux commerciaux ouverts au public (SFR, Bouygues France-Télécom, Neuf/Cégétel, Iliad) que des institutions disposant d'un réseau propre pour l'exercice de leurs missions (RATP, EDF, RTE, RENATER) d'une indiscutable prise en compte des risques encourus.

► À l'exception des balises émettrices réceptrices (BTS) des réseaux mobiles[21], la plupart des *équipements actifs sont dupliqués*.

Les *centres de supervision* nationaux le sont en principe. Ils peuvent se suppléer de l'un à l'autre. Les opérateurs mobiles[22] s'appuient ainsi sur de centres de supervision 24/24 qui, en permanence, connaissent l'état du réseau et sont en mesure de dépanner à distance les sites, de réagir aux crises en télécommandant des équipements actifs, par exemple pour isoler une zone sur laquelle apparaît un problème, voire d'envoyer des équipes sur le terrain si besoin. Ces centres de supervision/ exploitation disposent de doubles raccordements.

Les *bases de données clients* (HLR), qui sont un élément essentiel de la gestion des abonnés[23] sont également entretenues en deux ou trois exemplaires. Les mesures prises pour les sécuriser à la suite des pannes de 2004 devraient notamment permettre le cas échéant un basculement plus sûr des unes aux autres.

► La *topologie des réseaux* est le plus souvent conçue pour supporter des ruptures d'artère, avec une organisation maillée et des capacités largement dimensionnées auxquelles s'ajoute le recours éventuel à des technologies différentes pour assurer les liaisons, comme les faisceaux hertziens, les fibres optiques ou le satellite (Il subsiste cependant des zones qui ne peuvent pratiquement être alimentées que par une ligne et sont donc plus vulnérables que les autres).

Les opérateurs fixes s'appuient ainsi sur des *réseaux autoreconfigurables*, soit grâce à des maillages, soit sur des boucles optiques dans lesquelles l'acheminement peut emprunter indifféremment un sens ou l'autre de la boucle.

Même si elle introduit des vulnérabilités nouvelles (*bugs* logiciels qui se propagent de manière incontrôlée), l'évolution vers IP offre aussi des possibilités de reconfiguration : un de nos interlocuteurs nous a indiqué pouvoir secourir un *softswitch* (commutateur pour les communications vocales en IP) par un autre

[21] Mais les cellules de ces réseaux se recouvrent partiellement, si bien que la défaillance de l'une d'elles peut partiellement être compensée par les voisines.

[22] La description de l'un de ces réseaux est ainsi la suivante : 15 000 stations radio (*BTS*) disposent d'une autonomie électrique de 4 heures sur batteries. Ces sites radio sont pilotés par des *BSC* (environ 430) qui disposent de 8 heures d'autonomie, et, pour 30% d'entre eux, sont pourvus de groupes électrogènes et "redondés" en transmission. Les commutateurs (65 *MSC*) sont dans des sites sécurisés avec groupes électrogènes et double alimentation EDF. La panne d'un *MSC* aurait pour conséquence la neutralisation des *BTS* qui lui sont rattachées. De ce fait les opérateurs ont prévu des plans de secours (lourds) pour ces situations. Les *HLR* (élément sensible du réseau, cf ci-dessus) disposent de 2 redondances.

[23] Elles servent notamment à identifier les terminaux qui se présentent sur les balises émettrices-réceptrices (BTS).

softswitch en cas de panne, ce qui n'était pas possible dans la configuration historique où chaque abonné était intimement lié à son commutateur de rattachement.

A titre d'exemple, un opérateur nous a décrit son réseau, fortement basé sur un cœur de réseau IP et des routeurs pour relier le cœur de réseau aux boucles de collecte locales. Un tel réseau est largement auto reconfigurable en cas de panne. Il y a séparation du réseau public assurant la desserte de l'ensemble des abonnés et du réseau « fermé » offrant un service de transport de data (type VPN IP ou MPLS) aux gros clients, ces deux réseaux n'étant reliés que par des passerelles contrôlées.

► Le *pilotage des équipements*[24] *est indépendant du réseau de trafic* et donc, dans les architectures actuelles, des éventuelles perturbations de ce dernier. Encore convient-il de noter que cette protection liée à l'architecture traditionnelle des réseaux téléphoniques est susceptible de disparaître dans les prochaines années.

► L'*autonomie énergétique des opérateurs est censée avoir été améliorée*[25]. Les grands sites de commutation seraient apparemment dotés plus largement de groupes électrogènes. Cependant, si dans des villes moyennes, certains opérateurs ont développé un double raccordement au réseau EDF, ils ne sont pas allés pour autant jusqu'à systématiser l'installation de groupes permanents (ils s'en tiennent à la simple possibilité de brancher un générateur externe de secours). Quant à la durée d'autonomie des équipements fonctionnant sur batteries, il n'est rien moins que certain que des efforts aient été vraiment entrepris, depuis l'expérience fâcheuse de décembre 1999, pour la prolonger[26].

► Les *contrats de maintenance des équipements* [27] incluent systématiquement des garanties de délai de rétablissement.

► La *résistance aux risques d'inondations* a été, elle aussi, renforcée avec l'essor de la fibre optique. Celle-ci continue à fonctionner même dans l'eau et seuls ses points de terminaison sont sensibles à l'humidité (sachant que les répéteurs ont eux-mêmes quasiment disparu compte tenu des distances de plusieurs centaines de km désormais possibles sans amplification).

► La résistance des dispositifs d'ensemble aux *chaleurs hors normes* a pu, à l'expérience de la canicule de 2003, apparaître jusqu'ici convenable. Ainsi, les fortes températures prolongées constatées à cette occasion n'ont pas induit de conséquences lourdes sur le fonctionnement de systèmes techniques essentiels. Trains, métros, centrales de production électriques, systèmes informatiques ont fonctionné quasi normalement. Aucune faille majeure n'est apparue du point de vue technique.

Les équipements de *climatisation* des cœurs de réseaux de télécommunications et d'information continuent cependant à apparaître comme des points de fragilité ponctuels. Ces systèmes sont en général redondants (en N+1), mais leur dysfonctionnement pourrait être bloquant au niveau d'un service particulier, même en dehors des fortes chaleurs d'été. Ce danger est toutefois masqué par un risque d'ordre supérieur: celui d'une coupure électrique sur une large échelle provoquée par

[24] Le pilotage s'effectue soit en *mode associé* (la signalisation utilise des voies logiques différentes mais suit la même architecture physique que les voies de trafic), soit en *mode quasi associé* de type réseau Sémaphore n°7 (relativement indépendant lui-même du réseau de trafic physique).

[25] Mais en même temps certains équipements se révèlent désormais plus consommateurs d'énergie: cf. note bas de page n° 12.

[26] Les opérateurs, de façon générale, ont manifesté de grandes réticences à communiquer les performances exactes de leurs matériels.

[27] Les opérateurs commerciaux n'assurent pas eux-mêmes la maintenance des équipements de leur réseau, mais la sous-traitent à des sociétés spécialisées.

l'impossibilité de refroidissement des centrales d'EDF, la température atteinte dans les rivières dépassant alors les seuils autorisés[28].

► Plusieurs opérateurs ont indiqué réaliser des *exercices périodiques de sécurité* pour vérifier l'état de préparation de leurs matériels et de leurs équipes.

► Les mesures prises en matière de *sécurité physique des locaux*, pour ce qui a été donné de constater, n'appellent pas de remarques.

1.2.1.3 / Il reste que le contexte de concurrence ne constitue pas un élément dynamisant de réalisation d'efforts.

Malgré certains discours de convenance entendus, *le niveau de sécurité offert par les différents opérateurs commerciaux n'est pas un argument fort de conquête des marchés et de fidélisation de la clientèle*. La bataille continue à se livrer en premier lieu sur les fonctionnalités du service et, plus encore, sur le niveau de prix des prestations que sur la qualité de service.

Les opérateurs rencontrés concèdent, il est vrai, n'avoir subi aucune perte importante d'abonnés, fussent-ils professionnels, à la suite de pannes les ayant affectés.

L'administration elle-même les conforte dans une telle approche. Nombre de services publics (dont ceux consacrés à l'urgence) retiennent, dans la passation de marchés de télécommunications, le prix comme premier critère de choix. Même les ministères clef dont les préoccupations de sécurité devraient être primordiales sont de plus en plus tentés, non sans risques, de privilégier une seule logique d'économies budgétaires. L'un des plus importants et des plus sensibles d'entre eux vient d'être confronté à plusieurs défaillances successives de son système de télécommunications après avoir décidé de recourir, essentiellement pour des raisons de coût, à un opérateur de réputation pourtant médiocre.

Les cadres contractuels standard reflètent d'ailleurs le fait que la sécurité n'est pas considérée comme un enjeu commercial central. Dans bien des cas, à l'exception des gros clients, les clauses de pénalités introduites pour indisponibilité du réseau n'apparaissent pas significatives. En tout cas, elles sont insuffisantes pour considérer qu'elles obligent les opérateurs à optimiser, de façon conforme à l'intérêt général, la configuration de leur réseau face à la variété de risques susceptibles de se présenter.

Or, aucune réglementation contraignante pour les opérateurs en matière de sécurité ne corrige cette situation. Les obligations résultant du CPCE[29] et des cahiers de charge accompagnant l'octroi des licences radio sont à caractère extrêmement générales ("permanence" et "continuité de service") et non formalisées au travers de prescriptions techniques spécifiques. Le niveau actuel de sécurité résulte ainsi, avant tout, d'un consensus plus ou moins tacite entre les différents acteurs s'alignant sur les pratiques de leurs concurrents.

En réalité, les opérateurs apparaissent sans doute plus inquiets de se prémunir contre les risques encourus en interne (bug logiciel par exemple) qu'à l'encontre de risques collectifs comme les catastrophes naturelles:

- pour lesquelles il leur sera toujours loisible d'évoquer la force majeure (ou la dépendance vis à vis de l'opérateur historique),

- et dont les conséquences, *a priori*, ne les pénaliseront pas spécialement par rapport à leurs concurrents.

[28] Ce risque n'a été maîtrisé en 2003 que moyennant l'acceptation d'une température supérieure des cours d'eau.
[29] *CPCE*: code des postes et communications électroniques.

Si le degré de préparation qu'ils manifestent vis à vis des crises peut être qualifié de convenable, ceci résulte autant:

- d'une organisation générale destinée à assurer une bonne qualité de service dans un contexte de concurrence et de vigilance permanente face à des attaques logicielles quotidiennes,

- que de plans élaborés pour faire face à des crises majeures.

Les travaux réalisés par France Télécom dans le cadre du plan "crue de la Seine" sont illustratifs de cet état d'esprit. L'objectif premier (non critiquable par ailleurs) a été de prévoir des protections pour les équipements non pas pour que ces derniers puissent fonctionner pendant la crue, mais pour qu'ils ne soient pas détruits par l'eau, de telle sorte que le service puisse reprendre rapidement après la décrue.

En même temps, cette exacerbation de la concurrence et l'accélération des innovations de services proposées aux clients qu'elle impulse renforcent certaines vulnérabilités. La tentation est grande par exemple de raccourcir les délais pour tester les changements de palier de nouvelles configurations logicielles.

1.2.2 / Les réseaux disposent d'une protection structurelle pour un temps encore : leur cloisonnement les uns par rapport aux autres.

L'*augmentation du nombre des opérateurs et le développement des réseaux mobiles et de la voix sur Internet* a créé de nouvelles façons de faire circuler l'information et démultiplié les circuits de transit de l'information.

En quelques années, le paysage des télécommunications s'est profondément transformé :

- *techniquement*, d'un réseau de téléphonie fixe on est passé à un système qui s'est enrichi de réseaux de téléphonie mobile et de l'Internet mais aussi de réseaux de transmission de données privatifs;

- *institutionnellement*, à un opérateur en situation de monopole a succédé, aussi bien pour la téléphonie fixe que mobile, une multiplicité d'opérateurs dont certains spécialisés sur des créneaux particuliers (fourniture d'accès, fourniture de services…). On en dénombre actuellement près de 260 déclarés sur notre territoire.

Certes, compte tenu de la concurrence sur les coûts qui s'est accentuée à cette occasion, l'hypothèse peut être soutenue d'une éventuelle moins grande fiabilité individuelle que par le passé des équipements et des réseaux déployés. De même, la prolifération des réseaux dont l'usager exige qu'ils sachent de mieux en mieux communiquer entre eux impose également d'accroître les dispositifs-interfaces qui constituent une source potentielle supplémentaire d'incidents logiciels et de perméabilité intempestive.

S'agissant de la sécurité d'ensemble, les avantages semblent pourtant l'emporter encore sur les inconvénients.

1.2.2.1/ Pour l'heure, les risques de contagion de pannes d'un réseau à l'autre s'en trouvent certainement atténués.

Les technologies et les fournisseurs sont en effet encore nettement distincts.

Les représentants des opérateurs nationaux rencontrés nous ont confirmé que la configuration de leurs infrastructures propres était encore indépendante d'Internet en France métropolitaine, et qu'il en serait encore ainsi pendant quelques années. France Télécom indique par exemple que, même dans le cas d'une panne des DNS[30] Internet, la téléphonie sur IP (et *a fortiori* la téléphonie classique) continuerait à fonctionner sur son réseau.

Ces garanties vont néanmoins avoir tendance à s'émietter progressivement:

- déjà pour des liaisons internationales ou, par exemple, pour des liaisons entre le continent et la Réunion, la dynamique de coûts entraîne un repli croissant sur Internet;

- la mutualisation d'équipements d'opérateurs mobiles réduit, au moins localement, la diversité qui devrait résulter de l'existence de réseaux séparés : les sites radio les mieux placés sont souvent utilisés simultanément par les 3 opérateurs mobiles;

- la convergence entre les équipements fixes et mobiles, avant même le glissement prévisible prochain vers le "tout IP", risque aussi de faire s'écrouler peu à peu ces cloisonnements.

Pour autant, il est un fait que chacune des pannes logicielles observées jusqu'à maintenant est restée effectivement confinée dans le périmètre du réseau d'un seul opérateur.

Il est clair que la conservation, le plus longtemps possible, de démarcations techniques entre les différentes catégories de réseaux constitue un atout en termes de sécurité alors même que la vulnérabilité respective de chacune d'entre elles n'est pas identique selon les menaces. Le coeur des dispositifs fixes a peu à craindre des tempêtes tandis qu'une des caractéristiques fondamentales d'Internet est sa capacité à trouver un chemin pour faire passer l'information malgré les dégradations subies sur telle ou telle artère. Un élément d'appréciation en a été donné lors du séisme sous-marin du 26 décembre 2006 au large de Taiwan qui a détruit plusieurs câbles mais dont l'impact, au bout du compte, est resté mesuré.

1.2.2.2/ Au-delà de gênes immédiates, l'hypothèse la plus plausible dans la majorité des cas est celle du maintien à disposition de solutions de substitution pour communiquer.

En cas de dérangement d'un réseau, les usagers ont de plus en plus à disposition (qu'elle soit personnelle, de voisinage ou institutionnelle) un panel de moyens alternatifs de communication (mobiles familiaux ou professionnels relevant d'opérateurs différents + fixe + Internet) jusqu'à présent relativement indépendants. L'expérience a montré qu'ils pouvaient généralement compter sur ces moyens même si, le cas échéant :

- les communications s'exercent sur un mode dégradé;

[30] *DNS* (*Domain Name Service*) = serveurs de noms de domaines fournissant la correspondance entre les noms et les adresses utilisées par les processus de routage.

- les opérateurs ont sans doute à gérer de façon complexe des problèmes de report de flux significatifs;

- les temps de calage et d'adaptation de chacun par rapport à cette situation sont parfois aléatoires.

Une illustration ultime en a été donnée lors des attentats du *11 septembre 2001*. Les messageries (SMS et sur l'Internet) ont exercé un rôle apprécié de substitut à la téléphonie, le fonctionnement de cette dernière étant perturbé par les destructions physiques mais plus encore par des phénomènes de saturation à grande échelle induits par l'augmentation prodigieuse de la demande de communications [31].

*

Ces éléments autorisent par conséquent à penser que, sauf dans le cas d'une catastrophe naturelle dépassant largement celles que la France a connues jusqu'ici ou d'une rupture prolongée et générale de l'alimentation énergétique, une paralysie totale des télécommunications et, partant, de la vie économique et sociale est encore à présent, mais à présent seulement, assez improbable.

1.3. Le danger de répercussions en cascade d'une défaillance initiale d'un ou plusieurs de nos réseaux de télécommunications parait devoir, au moins aujourd'hui, être également relativisé.

L'infiltration de notre vie quotidienne par les technologies de l'information est telle que des effets en chaîne à partir du dérangement d'un réseau public de télécommunications sont inévitables. Pour autant, de nombreux acteurs ayant développé des réseaux autonomes, ces effets ne doivent pas, à l'heure actuelle, être surestimés.

1.3.1 / L'ensemble du réseau de transport et de distribution d'électricité est théoriquement configuré pour ne pas souffrir d'une détérioration quelconque des réseaux publics de télécommunications.

Un évènement de type "chinois" n'est *a priori* pas concevable en France. Pour construire plus rapidement une partie de son réseau électrique, la Chine en effet s'est, semble-t-il, fondée, dans un cas au moins, trop massivement sur un pilotage par voie Internet. Et l'interconnexion peu sécurisée entre son réseau interne et Internet l'a confrontée récemment à de sérieux déboires[32].

[31] Cf. rapport 1-4.1-2002 du CGTI (de MM.P. Fritz, P-Y Schwartz et B.Prunel) sur *les risques présentés par Internet* (janvier 2003).
[32] Les spécialistes évoquent un "plantage" électrique notoire.

1.3.1.1/ Pour l'essentiel, EDF et RTE s'appuient sur un réseau dédié de sécurité pour leurs télécommunications.

Cette situation devrait les prémunir, dans leur activité, des conséquences d'incidents susceptibles d'affecter un ou plusieurs des opérateurs de télécommunications.

En réalité, la situation est plus subtile et le degré de dépendance effectif de ces deux institutions vis à vis des autres réseaux de télécommunications mérite malgré tout d'être précisé :

Le transport de l'électricité en très haute tension (90 à 400 kV) est piloté par RTE, qui remplit un rôle d'interface entre d'une part les centrales électriques (quelles que soient leur nature ou leur statut) et d'autre part le réseau de distribution d'EDF. Le courant transite par 1000 ou 2000 postes MT/BT qui, eux-mêmes, alimentent un réseau de distribution EDF plus près de l'abonné. Ces postes MT/BT sont télécommandés (depuis quelques dizaines de postes de dispatching) aussi bien par RTE que par EDF, mais pour des fonctions différentes: RTE gère l'approvisionnement de ces postes, tandis que EDF prend en charge plus finement par télécommande les délestages vers des zones plus circonscrites.

On sait, en effet, que les réseaux d'électricité sont de type "château de cartes ". Si une consommation excessive fait chuter la fréquence du courant, au delà d'un certain seuil, certaines centrales de production ne peuvent plus suivre. Elles se déconnectent du réseau. Le déséquilibre entre la consommation et la production tend alors à s'amplifier risquant d'entraîner l'effondrement de ce dernier.

Pour éviter ce phénomène, EDF organise donc des délestages grâce, précisément, à la télécommande des postes MT/BT, certains départs étant prioritaires et d'autres non. EDF doit d'ailleurs composer avec une contrainte dans la gestion des priorités, car, dès lors qu'un départ (depuis le poste MT/BT) est prioritaire, tous les abonnés de ce départ le deviennent[33]. Le plan de production d'électricité est en général calculé avec une marge suffisante mais, en cas d'incident ou de consommation plus forte que prévu, la réactivité nécessaire pour délester se compte généralement en minutes ou en dizaines de minutes.

Or, les postes MT/BT ainsi impliqués sont sans personnel permanent. Leur télécommande est opérée à travers un réseau spécifique de sécurité qui offre des services de voix, de *data* et de téléaction, grâce à des *liaisons louées à France Télécom* (d'une distance moyenne de 50 km, parfois sur des faisceaux hertziens). Des liaisons RNIS ou RTC assurent un premier secours. Et, possibilité ultime, RTE dispose de 250 valises satellite qu'il pourrait envoyer sur certains sites (10 à 20%) en réquisitionnant des personnels.

Les précautions prises sont notables. Pour autant, compte tenu de l'importance des enjeux collectifs concernés, il n'y aurait qu'avantage à ce que la vulnérabilité potentielle de ce circuit de télécommande fasse l'objet d'une étude spécifique.

L'intérêt de ce réseau de sécurité n'est d'ailleurs pas que d'ordre technique. Lors de l'explosion d'AZF, les réseaux publics de télécommunications étant saturés, RTE a utilisé celui là pour les communications managériales (avec une capacité réduite, un seul poste par service étant disponible).

[33] Ceci explique que EDF ne puisse pas rendre prioritaires tous les centraux télécoms ou les BTS des opérateurs mobiles.

1.3.1.2/ Indépendamment de ce réseau de sécurité à vocation opérationnelle et technique, EDF et RTE partagent par ailleurs un réseau classique.

Ce réseau (dit "tertiaire") est sous-traité à Neuf/Cégétel. Son arrêt n'aurait au départ que des conséquences indirectes sur la distribution de l'électricité. Cependant, certaines applications sensibles l'utilisent, notamment le calcul du plan de production du lendemain en fonction des données météo, ou les calculs des paramètres de remise en route d'une centrale après un arrêt.

1.3.2 / Nombre d'acteurs majeurs de la vie économique intègrent déjà des logiques préventives convaincantes.

Les investigations très partielles réalisées dans des secteurs aussi vitaux que ceux de la banque, de l'info gérance, des transports publics ou de la recherche en témoignent.

1.3.2.1/ Le "Groupement des cartes bancaires", par exemple, a pris plusieurs types de mesures protectrices.

La continuité de son fonctionnement représente un impératif certain car un tiers des paiements sont aujourd'hui effectués par cartes dans la zone Euro et une bonne partie de l'argent liquide provient des DAB (distributeurs automatiques de billets). Le groupement, en 2005, a réalisé 6,3 milliards de transactions représentant 325 milliards € de paiements et de retraits.

Les banques (ou les DAB) sont reliées aux centres de traitement du groupement interbancaire, par un *réseau IP fermé et chiffré non lié à Internet*. Ce dernier, toutefois, n'a pas été encore dédoublé et relève encore d'un fournisseur unique. Le Groupement prévoit cependant de le dupliquer prochainement avec un 2ème opérateur. Les centres de traitement par contre sont déjà dupliqués et capables de se suppléer mutuellement.

En aval, les paiements en magasin ou auprès de prestataires de services tout comme les retraits d'argent mettent en œuvre une grande *variété de moyens de transmissions* (liaisons louées, liaisons Transpac, réseaux VPN IP, RTC, voire Internet ADSL) entre les terminaux de points de vente (ou les DAB) et les différentes banques concernées. La diversité de ces moyens met donc les usagers relativement à l'abri d'un blocage total généralisé et permet d'espérer des gênes qui restent circonscrites en cas de panne éventuelle d'un de ces réseaux.

1.3.2.2 / Parallèlement, dans le domaine de l'info gérance, une société comme *ATOS Worldline* s'est entourée de garanties.

Atos est *leader* sur le marché du traitement des échanges électroniques grands volumes et de l'hébergement de services bancaires : un grand nombre de banques ont recours à ses services soit pour héberger leurs applications courantes, soit comme recours en cas de panne d'une de leurs installations gérées directement. (Cette compagnie gère près d'1 milliard de transactions à partir de terminaux de points de vente et 100 millions de paiements Internet).

La sécurité, pour autant que l'on a pu en connaître et l'analyser, paraît avoir été bien prise en compte à travers un maillage fort des infrastructures réseau, la protection physique des salles informatiques réparties dans 3 sites centraux, et la forte capacité des groupes électrogènes de secours (sachant que dans de telles salles, la climatisation est critique toute l'année, la température devenant excessive au bout de 1 h 30 en cas de panne).

1.3.2.3 / De leur côté, tant *la SNCF* que *la RATP* disposent de leur réseau propre de télécommunications.

Aussi, l'une et l'autre estiment que les trains ou les rames de métro sont en mesure de circuler quel que soit l'état de fonctionnement des réseaux de télécommunications publiques.

Certaines fonctionnalités seraient cependant réduites : ainsi, comme le réseau radio de la RATP reste malgré tout dépendant de liaisons louées à France Télécom, les bus ne seraient plus en relation avec leur poste de commandement ; il en est de même pour la sonorisation dans les stations de métro qui ne marcherait plus. Ces gênes apparaissent accessoires.

1.3.2.4 / L'essentiel des transmissions liées à *la recherche* est également sécurisée.

Pour assurer ses besoins, le GIP RENATER[34] dont sont membres de multiples organismes primordiaux de recherches (CEA, CIRAD, CNES, CNRS, INRA, INRIA, INSERM, BRGM, CEMAGREF et IRD, ainsi que le MENESR) déploie et exploite en effet un réseau indépendant de transmission optique de très haut débit. Celui-ci est redondant sous plusieurs aspects : duplication des serveurs centraux, topologie de réseau maillé, cloisonnement des flux, autonomie d'une semaine en cas de coupure d'alimentation électrique... Configuré notamment à partir de fibre noire[35] (ou de longueurs d'ondes privatives sur des fibres appartenant à des opérateurs), il est protégé des incidents que pourraient être amenés à connaître les réseaux des grands opérateurs.

Vis à vis d'attaques par déni de service provenant d'Internet, un système de suivi permanent et d'analyse par corrélation des "*logs*" a été mis en place lui permettant de détecter à l'avance la plupart des attaques et donc de s'en prémunir à temps en bloquant les ports concernés.

1.3.3 / L'administration cherche elle aussi à se protéger contre certains effets "domino", encore que ses efforts restent insuffisants.

Ses réseaux de commandement ont précisément été conçus pour rester à l'écart des troubles extérieurs.

1.3.3.1 / Elle dispose de plusieurs réseaux dédiés, indépendants des réseaux publics et d'Internet.

RIMBAUD en est le prototype. Il est physiquement séparé de tout autre réseau. Une altération,

---

[34] *RENATER* (Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche) fédère les infrastructures de télécommunication pour la recherche et l'éducation dont, en premier lieu, celles des organismes de recherche membres du GIP (CEA, CIRAD, CNES, CNRS, INRA, INRIA, INSERM, BRGM, CEMAGREF et IRD, ainsi que le ministère de l'éducation Nationale, de l'enseignement supérieur et de la recherche). Il fournit des services à très haut débit pour les grands projets scientifiques nationaux et internationaux. Plus de 800 sites sont raccordés via les réseaux de collectes régionaux au réseau national. Il est relié aux autres réseaux de la recherche et de l'enseignement dans le monde via le réseau pan européen également indépendant et sécurisé GEANT.

[35] Autrement dit, de la fibre optique souscrite en dehors de tout service de transport des données ("noire" c.a.d "éteinte").

quelle qu'en soit la nature, de la continuité ou de la qualité des télécommunications "grand public" est donc censée ne pas avoir de conséquence sur lui. RIMBAUD est en outre assez bien protégé contre des coupures d'alimentation énergétique puisque la plupart des centraux sont équipés de groupes électrogènes. Il est protégé également contre des coupures de câbles grâce à un maillage des artères interurbaines. Sa capacité reste néanmoins limitée (de l'ordre de quelques dizaines de postes par département)

Le Ministère de la Défense, quant à lui, peut s'appuyer sur SOCRATE[36] indépendant également des réseaux publics et d'Internet. Ce réseau est largement sécurisé par des doubles acheminements et par l'utilisation de plusieurs opérateurs pour des liaisons spécialisées interurbaines.

Enfin, plusieurs ministères ont monté des réseaux radios de sécurité propres (ACROPOL pour la Police, complété par le projet ANTARES pour les SDIS, RUBIS pour la Gendarmerie, réseau 40 MHz[37] pour les services déconcentrés de l'Equipement) qui, en plus de leur capacité à relier les hommes entre eux sur le terrain, pourraient aussi servir pour des communications de commandement entre autorités.

Si ces réseaux, confrontés à différents types de crises, ont jusqu'ici fait leurs preuves, leur usage relève cependant d'un cercle fermé d'utilisateurs.

1.3.3.2 / Toutefois, les principaux services, et notamment les services de secours, restent pour l'essentiel tributaires des réseaux publics et de leurs défaillances éventuelles.

Certes, certains de ces services bénéficient parfois de doubles raccordements. Cependant, la plupart d'entre eux ne recourent qu'à un seul opérateur car les critères financiers l'emportent, on le constate hélas fréquemment, sur tout autre type de considérations (particulièrement celles qui ont trait à la sécurité) lorsqu'il s'agit de définir la configuration de leurs dispositifs.

La taille de l'établissement de rattachement est de ce point de vue déterminante:

- ainsi, les *centres de réception des appels au 15* sont plutôt privilégiés. Ils sont généralement situés au sein d'une entité importante (hôpital, SAMU) qui fait l'effort de financer un double acheminement. Pour autant, même dans ce cas, le basculement des appels sur le 2ème raccordement ne se fait généralement pas automatiquement si le premier tombe en panne. En effet, les opérateurs mobiles ne programment dans leurs centraux que le seul acheminement à 10 chiffres correspondant au 1er raccordement;

- en revanche, *les centres 18* sont souvent implantés dans des casernes de pompiers d'importance plus réduite et, partant, sont parfois moins enclins à réaliser les investissements nécessaires à la sécurisation de leur raccordement.

Cette situation est évidemment singulièrement préoccupante s'agissant de services d'urgence. L'usager peut être pénalisé par la défaillance de l'opérateur soit de départ (celui sur lequel est raccordé l'usager qui compose le 15, le 18 ou le 112), soit de celui qui dessert le centre de secours. La panne d'un seul d'entre eux compromet donc le bon déroulement de l'appel, même si des solutions de substitution peuvent être cherchées :

[36] Il raccorde 400 sites militaires mais ne dessert pas les préfectures.

[37] Ce réseau permet au DDE de communiquer avec les équipes qui interviennent sur les routes. Indépendant des réseaux publics, il constitue, pour les préfets, une possibilité de communication intéressante avec des équipes opérationnelles sur le terrain en cas de crise. Sa couverture n'est cependant pas totale, visant principalement les axes de la responsabilité des DDE.

- à travers le recours, pour l'usager en situation d'urgence, à un autre réseau fixe ou mobile si le dérangement n'est pas général ;

- à travers d'opérations de *reroutage*, si c'est le raccordement du centre de secours qui est en panne. Il est possible en effet dans certains cas (mais pas partout) de rerouter automatiquement sans délai les appels vers un autre centre de secours qui n'a pas de problème de raccordement ;

- à travers de mesures administratives: en dernière extrémité, le préfet de département (qui gère les tables d'acheminement des appels de secours) peut en effet demander à tous les opérateurs de modifier les tables d'acheminement des appels de secours pour faire arriver les appels vers un centre correctement desservi. Ceci exige malgré tout un certain délai (de l'ordre de la journée) et pose le problème de la gestion de ces appels par des centres qui seraient alors saturés.

*

Ainsi, même s'il existe et doit être scruté avec beaucoup d'attention, le danger de répercussions en cascade d'une défaillance initiale d'un ou plusieurs réseaux de télécommunications doit être relativisé. Des îlots majeurs de la vie économique et sociale devraient pouvoir en être, en tout ou partie, préservés.

1.4 / Néanmoins, à moyenne échéance, les évolutions les plus perceptibles en matière de télécommunications recèlent des inconnues qui ne peuvent pas manquer d'inquiéter.

Ce ne sont pas tant le déploiement annoncé des accès en fibre optique, lequel n'interviendra que progressivement, que quatre autres tendances lourdes qui méritent, de ce point de vue, d'être mises en exergue :

- la capillarisation toujours plus prononcée des réseaux et des systèmes d'information;
- la dynamique de plus en plus marquée vers le "tout IP";
- le manque de fiabilité d'Internet avec lequel les interconnexions deviennent de plus en plus importantes ;
- l'externalisation croissante des systèmes d'information.

1.4.1/ La capillarisation croissante des réseaux et des systèmes d'information rend de plus en plus difficile une perception synthétique d'ensemble.

1.4.1.1/ Pratiquement plus aucun domaine de la société n'échappe à cet envahissement.

Si, voici encore une vingtaine d'années, établir un réseau privé à finalité particulière était une opération délicate, il n'en va plus de même actuellement. Il n'est plus besoin de louer des lignes chères à un opérateur. Les équipements de télécommunications comme la logique informatique à base de micro ordinateurs sont bon marché. Leur banalisation est générale.

Les réseaux s'enchevêtrent et tissent des liens qu'on ne soupçonne plus toujours et que parfois seules les pannes révèlent.

Quel rapport, par exemple, existe-t-il maintenant entre un réseau de téléphones mobiles et les *panneaux modernes d'affichage urbain* ? Le fait que le premier est l'instrument privilégié de gestion des seconds. Ces panneaux disposent de plusieurs affiches qui sont changées à partir d'ordres donnés à distance transitant par le mobile GSM dont ils sont équipés. Cette commande par SMS depuis un PC économise l'intervention de multiples personnels.

L'aspect anodin de cette illustration masque cependant, dans des domaines répartis géographiquement, bien d'autres applications plus sensibles à base de capteurs ou de dispositifs d'alertes. Citons par exemple la transmission de plus en plus automatisée *des informations sur les hauteurs des cours d'eau* (dont l'importance est évidemment vitale en matière de prévention de crues) ou celles ayant cours dans le domaine hospitalo-sanitaire.

De fait, les opérateurs mobiles développent de plus en plus ce qui s'appelle le *"M to M* : *machine to machine"*, autrement dit, des mobiles spéciaux adaptés à toutes sortes d'applications industrielles.

Ainsi, par exemple, depuis 3 ans, PSA Peugeot-Citroën équipe ses voitures de haute et moyenne gammes de l'option *Navidrive*, qui contient un *système automatisé d'alerte individuelle* combinant GSM et GPS. Ce système est appelé à être installé sur tous les véhicules, et est en cours de normalisation. En cas de déclenchement des airbags, il envoie à un centre d'assistance la position GPS du véhicule accidenté. Ces coordonnées sont transmises par deux SMS au centre unique d'assistance Inter Mutuelle Assistance de Niort. 12 000 accidents sont ainsi signalés par an, le système étant déjà implanté sur 320 000 véhicules.

Le cheminement de ces alertes est au demeurant instructif : le SMS passe tout d'abord du réseau mobile (Orange, SFR, Bouygues) au réseau de la société Netsize. Puis celle ci l'envoie à la société STERIA, qui décrypte le message, puis STERIA le transmet à la société IMA. En cas de validation de l'alerte, IMA passe enfin l'alerte au centre de pompiers concerné. Une multiplicité de réseaux est donc successivement sollicitée.

1.4.1.2 / Les diagnostics sont de plus en plus complexes.

La rapidité de déploiement de ces réseaux, leur foisonnement continuel, leur enchevêtrement, les bouleversements incessants de technologies mises en œuvre, les bifurcations aléatoires susceptibles d'être prises par elles rendent de plus en plus illusoire le projet d'une quelconque maîtrise d'ensemble de cette architecture.

Les interlocuteurs de la mission et la diversité de spécialistes rencontrés se sont tous exprimés à ce propos de façon concordante. Ils ont souligné combien la nature de la dynamique en cours empêchait l'expression de jugements prospectifs autres que circonspects et partiels s'agissant de la résilience à venir des réseaux et de l'impact d'éventuelles pannes de ces derniers.

Plus personne ne possède "les plans". Au demeurant, les opérateurs eux-mêmes ne jouent le jeu que d'une transparence partielle à la fois pour des raisons commerciales et, vis-à-vis des pouvoirs publics, sans doute par crainte d'imposition de prescriptions règlementaires nouvelles. Quant à l'Etat, il dispose de moins en moins, depuis l'inscription de France Télécom dans la mouvance privée, de capacités d'expertise technique publique.

1.4.2/ Parallèlement, les réseaux s'orientent de plus en plus vers des configurations **TCP/IP**.

1.4.2.1/ Le "tout IP" (ou, si l'on préfère, la convergence "voix-données" sur Internet) a vocation à devenir le mode prédominant[38].

L'aspect qui en est le plus immédiatement saisissable pour l'usager et le non technicien est la banalisation de l'offre dite *triple play* par les opérateurs, permettant l'accès concurrent à la télévision, au téléphone et à Internet haut débit à partir d'un seul raccordement à Internet. Elle se matérialise, chez le particulier, par l'installation d'une "*box*" sur laquelle sont connectés télévision/ téléphone analogique/ ordinateur. L'offre est même dite *quadruple play* lorsque, de surcroît, le téléphone mobile fait, pour des raisons d'économies, transiter les appels non plus via la borne publique de téléphonie mobile, mais par ce boîtier à domicile.

Or, cette mutation prévaut en premier lieu pour les réseaux des opérateurs eux mêmes. Actuellement, les grands opérateurs (comme celui de type "historique") disposent de trois réseaux :

- le réseau de téléphonie fixe, à base de commutateurs de circuits (" les centraux téléphoniques" traditionnels),
- le réseau de transmission de données, qui leur permet de faire transiter les données de leurs clients Internet,
- le réseau mobile, reliant les stations de base hertziennes aux commutateurs téléphoniques.

A court terme, c'est-à-dire à l'horizon 2010 / 2012, il paraît acquis:

- *que ces trois réseaux n'en feront plus qu'un,*
- *et que ce réseau unique sera basé sur la technologie IP*.

La raison profonde de cette dynamique tient aux économies d'échelle importantes que génère un réseau unique.

[38] Déjà, la part du trafic IP au départ des postes fixes est passée, selon l'ARCEP, de 5,7% à 23% au cours de ces seules deux dernières années (2005-2006).

1.4.2.2/ Cette évolution suscite toutefois des craintes.

Elles se rapportent[39]:

► en premier lieu, à *la dépendance plus complète qui en découle vis-à-vis de l'énergie 220 V.*

Actuellement, France Télécom alimente en 48 V les lignes analogiques de ses clients, depuis son central téléphonique. Cette sécurité disparaît avec les offres *triple* ou *quadruple play*.

Alors qu'auparavant une coupure de téléphone n'empêchait pas non plus que la télévision continue, si besoin en était, d'informer les populations, cette possibilité risque d'être de plus en plus restreinte à l'avenir. Dans les immeubles câblés, les antennes ont en effet été démontées au profit du "service antenne" des câblo-opérateurs[40]. Il est prévisible que cette évolution va s'étendre à l'habitat individuel à mesure que leurs occupants souscriront aux offres de type *triple play*.

► en second lieu, aux *plus grands risques de contagion des incidents et à l'absence de recours alternatifs.*

Combinée à la diversification et la multiplication des opérateurs[41], l'hétérogénéité des réseaux a contribué jusqu'ici à compartimenter les pannes. La perméabilité croissante des catégories de réseaux entre eux, puis à terme leur fusion en un seul régi par la norme TCP/IP, modifient la donne. Le système perd la protection structurelle que procuraient ces cloisonnements.

1.4.3 / Les interconnexions deviennent corollairement de plus en plus importantes avec **Internet** dont la fiabilité n'est pas assurée.

Le trafic IP en réseau fermé, indépendant d'Internet devrait progressivement constituer l'exception. Or, la nature même d'Internet et sa dynamique d'organisation sont empreintes de multiples incertitudes. Sa résistance intrinsèque aux agressions externes de toutes sortes est régulièrement vantée. Pour autant, celle-ci présente des failles potentielles qui ne permettent pas de tabler sur sa fiabilité assurée. Deux d'entre elles au moins méritent d'être soulignées:

1.4.3.1/ L'équipement du réseau est trop dépendant d'un seul fournisseur.

La prédominance du fabricant américain de routeurs *CISCO* est patente. Le scénario catastrophe d'une infection virale étendue ne peut donc en soi être d'office écarté. Il est loisible d'imaginer, par exemple, l'introduction d'un virus à réveil tardif lors d'un changement de version logicielle sur ces routeurs. Lorsque la majorité des routeurs de la planète auront

[39] Au-delà de celles qui ont trait au manque de fiabilité des "*boxes"* qui est celle des ordinateurs et non plus celle des commutateurs. Le cahier des charges des commutateurs publics type E10 était, "du temps du CNET", de une heure de panne en 40 ans de fonctionnement. Les ordinateurs aujourd'hui sont près de 100 fois moins fiables.

[40] Le "*service antenne*" est l'obligation pour ces derniers de fournir les chaînes gratuites au même coût qu'une maintenance d'antenne.

[41] Mouvement au demeurant qui touche sans doute maintenant à sa fin. A terme, le nombre des fournisseurs d'accès devrait vraisemblablement être amené à se réduire. On semble s'orienter désormais vers une phase de concentration, l'exemple le plus marquant en France étant celui de Neuf Télécom qui résulte de la réunion de 9 opérateurs différents.

implémenté la nouvelle version du logiciel, le virus pourrait se réveiller et "éteindre" en quelques secondes l'Internet mondial.

Certes, le réseau ne repose pas exclusivement sur des matériels *CISCO* (*Juniper* et *Alcatel* sont également des fabricants de routeurs même si leur part de marché est nettement moindre). Mais si ces derniers tombent en panne, le trafic devra se répartir sur les quelques artères résiduelles non atteintes, et saturera dans des délais très brefs les routeurs épargnés par le virus. La répercussion serait majeure.

1.4.3.2 / Son fonctionnement reste subordonné à des nœuds cruciaux d'interconnexion.

Un incident sur un nombre faible de ces nœuds pourrait immobiliser le réseau.

Il est notoire que près de la moitié du trafic mondial transite par le seul Etat de Virginie où arrivent la plupart des terminaisons maritimes et où sont situés les principaux centres de routeurs "racines"[42]. Mais, de façon générale, les points névralgiques sont nombreux et très répartis. Il s'en trouve aussi en France bien que d'importance moindre.

Les sites d'hébergement multi-opérateurs, et notamment les sites de Peering constituent un point de fragilité notable.

[…….]

[42] Des efforts importants ont toutefois été accomplis ces dernières années pour dupliquer ces DNS racine. Il reste que la disponibilité de ces serveurs reste un point de fragilité du réseau (contre lesquels beaucoup d'attaques sont d'ailleurs dirigées).

[…….]

Un rapport du CGTI sur *les risques présentés par Internet*[43] dénonçait déjà en 2003 cette vulnérabilité globale. Il concluait à la possibilité d'un effondrement significatif du réseau. Certes, la structure très répartie de ce dernier protège contre le risque de son écroulement total, mais ne le garantit nullement contre une panne partielle (de 30 à 60%), donc très sérieuse.

Cette vulnérabilité relative a d'ailleurs été illustrée par les dysfonctionnements dont Internet a fait l'objet en décembre dernier et qui ont été générés par le tremblement de terre intervenu au large de *Taïwan*[44]. Ce séisme, dont l'impact direct était assez localisé, a néanmoins perturbé notablement le continent est-asiatique et affecté sensiblement les communications internationales.

Le CGTI a mis en évidence, par ailleurs, que si la résolution d'une panne majeure consécutive à une attaque virale par exemple ne devrait pas durer plus de 48 heures, la durée d'indisponibilité du réseau pourrait être plus importante en cas d'attaques successives. Les conséquences des attaques coordonnées que *l'Estonie* a subies au cours de la deuxième quinzaine de mai 2007 contre les principaux sites web régissant l'activité gouvernementale et économique du pays en sont l'illustration la plus récente.

Or, dès lors que l'Internet traitera l'ensemble des flux, soit d'ici 4 à 5 ans, les services très consommateurs en bande passante, tels que la consultation de services web, la téléphonie, la télévision seront hors service dans l'hypothèse d'une crise importante du réseau.

En pareil cas, une gêne majeure serait occasionnée à la vie économique et un risque certain surviendrait pour la sécurité des personnes en difficulté.

[43] Rapport 1-4.1-2002 du CGTI (de MM.P. Fritz, P-Y Schwartz et B.Prunel) sur *les risques présentés par Internet* (janvier 2003) cité supra.

[44] Tremblement de terre du 26 décembre 2006 qui a provoqué la rupture de plusieurs câbles optiques sous-marins.

1.4.4/ Le déploiement massif annoncé des réseaux optiques pour les boucles locales implique également des vulnérabilités nouvelles, mais sur un terme vraisemblablement plus long.

1.4.4.1/ Les raccordements des usagers en fibre optique devraient être appelés à se banaliser[45].

Cette évolution devrait permettre de répondre notamment à une demande attendue des particuliers : celle exprimée pour le "*très haut débit*" (au delà des 20 Mb/s autorisés par l'ADSL, soit typiquement 100 Mb/s) et motivée par la télévision "haute définition", le téléchargement de films et, de façon plus générale, les services multimédia.

1.4.4.2/ Cette rupture technologique ne devrait pas être sans conséquences en matière de sécurité.

Il existe une différence fondamentale entre la technique ADSL, reposant sur une ligne de *cuivre* depuis le central de France Télécom, et un accès *" fibre"*:

► dans le premier cas, il est possible de garder sur la même ligne un téléphone classique, donc bénéficiant de la sécurité de l'alimentation 48 Volts fournie par le central téléphonique de France Télécom;

► dans le second, les nouvelles technologies empruntées, dites "*FTTx"*[46] se caractérisent par le fait que :

- elles sont émergentes, et multiples: le marché n'a pas encore choisi celles qui deviendront les standards des prochaines années. 4 à 5 technologies différentes sont en compétition (*PON, EPON, BPON, GPON, EthernetP2P*, ...)

- peu d'expériences pilotes sont aujourd'hui disponibles, et à l'intérieur d'une même famille technologique, il existe des variantes entre les différentes implémentations.

Pour autant, par rapport aux réseaux "cuivriques" ADSL, deux types de reproches peuvent leur être adressés:

- d'une part, elles *pérennisent la fragilité apportée par l'ADSL en dégroupage total*, à savoir[47] la nécessité d'une alimentation électrique locale de la "boite" de réception. Elles l'*aggravent* même par rapport à l'ADSL puisqu'elles ne peuvent bénéficier de la téléalimentation par la ligne cuivrique que la fibre vient remplacer.

- et d'autre part, elles *recourent pour certaines à des équipements actifs nécessitant une alimentation dans leur structure de distribution*. Ainsi en est-il notamment des réseaux s'appuyant sur la technique "Ethernet point à point sur fibre optique" (*Ethernet P2P*). Peu d'indications sont actuellement disponibles sur leur sécurisation électrique.

---

[45] L'ARCEP évoque le remplacement d'un million de km de câblage pour la décennie.

[46] **FTTx** : *"Fiber to the x"* : **X** pouvant être **H** -pour *home* : la maison-, **C** -pour *curb* : le coin de la rue-, **B** -pour *building*-...

[47] En plus de l'abandon de la transmission en bande de base du signal vocal (au profit d'une modulation du signal sur des fréquences élevées).

D'autres technologies optiques en compétition sont néanmoins plus robustes vis-à-vis de ce risque particulier de défaut d'alimentation électrique comme celles de type *PON* (*Passive Optical Network*) qui utilisent des équipements optiques ne nécessitant pas d'alimentation (en fait, des "prismes" pour séparer les longueurs d'onde).

En l'état, on peut donc craindre que le remplacement, sur les derniers kilomètres, du cuivre par la fibre ne se traduise au final par une notable fragilisation du réseau d'accès de l'usager aux télécommunications.

1.4.4.3/ Cette mutation n'interviendra cependant en France que progressivement.

Les investissements nécessaires sont en effet, considérables : des montants de l'ordre de 40 à 50 milliards d'euros sont évoqués. Les conséquences n'en seront donc pas globales avant une dizaine d'années. D'ici là, les réseaux mobiles auront eux aussi évolué, et, en matière de télécommunications, 10 ans est un horizon pour lequel les prévisions sont hasardeuses, compte tenu du rythme des innovations.

Face à cette dynamique probablement inéluctable vers la fibre et le "très haut débit", la mission n’est pas en mesure de préconiser une technique plutôt qu’une autre. Elle souhaite toutefois attirer l’attention des décideurs sur l’intérêt d’une solution qui ne comporte pas d’éléments actifs ou d’éléments sensibles à l’inondation sur le trajet entre le NRA et l’abonné.

1.4.5 / L’externalisation des systèmes d’information, enfin, est de plus en plus prononcée mais n'est pas entourée de précautions suffisantes.

1.4.5.1/ Il s'agit d'un mouvement général.

- celui-ci touche désormais autant les *services publics* que les *entreprises privées*.

Il y a une vingtaine d’années, seules les grandes entreprises soucieuses d’améliorer leur rentabilité apparaissaient concernées. Depuis une dizaine d’années, les services publics tendent de plus en plus à s'engouffrer également dans cette voie. Ainsi, la très grosse majorité des services web des administrations est gérée à l’extérieur de celles-ci. Le premier d’entre eux, *Service-public.fr*, dépendant du SGG (via la Documentation Française) est ainsi hébergé chez un prestataire.

- il affecte aussi bien les réseaux de *télécommunications* que les *services et applications informatiques*.

1.4.5.2/ Ce phénomène s'affirme, toutefois, potentiellement préoccupant.

- d’une part, l’externalisation porte sur des *parties de plus en plus stratégiques* des systèmes d'information.

A l’origine, seuls les services secondaires étaient externalisés. Au sein des administrations publiques et sous l’impact de la réduction des budgets d’investissements, généraliser l’hébergement, lequel est susceptible d'être pris en compte en chapitre de "fonctionnement", est apparu comme une solution pratique. Ainsi, des services de moins en moins marginaux sont désormais sous-traités.

- d’autre part, la *fiabilité des hébergeurs* concernés s'affirme en pratique extrêmement hétérogène.

Si les opérateurs de réseaux sont soumis à certaines obligations de qualité de service, souvent issues de leur licence d’opérateur, il n’en est pas de même de la profession d’hébergeur, laquelle n’est asservie à aucune réglementation. Tout informaticien "disposant de 10 k€ et d'un garage" est aujourd'hui en mesure d'ouvrir une société d’hébergement de services Web, ainsi que l'attestent de nombreux exemples de sociétés très fragiles.

Cette fiabilité est d'autant plus sujette à caution que ces hébergeurs peuvent très bien se situer à l'étranger, le lieu d'hébergement étant souvent contractuellement indifférent. Les grandes sociétés du domaine hébergent désormais les données dans des pays comme l'Inde, le Pakistan, l'Irlande ou les Etats-Unis, situation qui a été rendu possible par la disponibilité de liaisons mondiales à haut débit et à bas coût à partir du milieu des années 90.

- en même temps, pour les administrations et institutions publiques, le respect trop strict du *code des marchés publics* accentue de fait les prises de risques.

Il est clair que le moins disant d'un appel d’offres ne sera pas forcément le plus sûr, si tant est que l’aspect sécurité ait lui même été pris en compte. Les exemples ne manquent pas à ce propos.

Ainsi en est-il, à titre d'illustration, des déboires rencontrés par *Météo France* dans la gestion de ses services Audiotel dont l'importance est stratégique. En cas de crise, ses répondeurs informent en effet jusqu’à 1 million de personnes par jour. En 2002, à la suite d'un appel d’offre pour équiper ces serveurs vocaux de lignes de raccordement au réseau téléphonique, cet établissement public n'a pu s'en remettre qu'à l'opérateur le moins disant. Une chute de la qualité de service se traduisant par des interruptions de service ou des incapacités à acheminer les appels s'en est immédiatement suivie. Météo France a donc été conduite dès 2004 à revenir vers l’opérateur historique pour le renouvellement de son marché, mais non sans avoir à développer une argumentation laborieuse afin de justifier le choix d’un prestataire plus onéreux auprès du contrôleur financier.

*

Avec le temps, l'appréhension des différents ***scénarii de pannes*** de réseaux auxquels nous sommes susceptibles d'être confrontés se complique donc:

► À court terme, ces scenarii se répartissent déjà selon *un spectre assez large de probabilités d'occurrences et d'importance éventuelle d'impact* qui peuvent être résumées dans le tableau schématique suivant:

Nombre de réseaux concernés	Type de réseau	Type de flux	Type de panne				
			Panne matérielle	Panne logicielle	Incendie, sabotage	Catastrophe Naturelle	Black out énergie
1 opérateur	Fixe	Voix	R2 / I1	R3 / I2	R1 / I2	R2 / I2	sans objet
		Données	R2 / I1	R3 / I2	R1 / I2	R2 / I2	sans objet
	Mobile	Voix	R2 / I1	R3 / I1	R1 / I2	R2 / I2	sans objet
		Données	R2 / I1	R3 / I1	R1 / I1	R2 / I1	sans objet
Plusieurs opérateurs	Fixe	Voix	R1/ I2	R2 / I3	R1 / I3	R2 / I2	R1 / I3
		Données	R1 / I2	R2 / I2	R1 / I3	R2 / I2	R1 / I3
	Mobile	Voix	R1 / I2	R1 / I2	R1 / I2	R2 / I3	R1 / I3
		Données	R1 / I2	R1 / I1	R1 / I1	R2 / I1	R1 / I1

Les probabilités de pannes (**R)** et d'importance éventuelle de leur impact (**I**) sont classées sur une échelle de 1 à 3 : **1** (faible), **2**(moyen), **3** (fort).

Ces scénarii, pour la plupart, sont malgré tout ceux de crises de portée limitée. Un effondrement éventuel de l'ensemble des types de réseaux (fixe/mobile) qui concernerait l'éventail des flux (voix/données) et mettrait en cause plusieurs opérateurs en même temps ne pourrait relever que d'un *black out* énergétique. Pour autant, les enjeux en cause (continuité de l'action gouvernementale et de la vie économique et sociale), même si la panne est circonscrite dans le temps et l'espace, peuvent être considérables.

Plusieurs de ces situations ont déjà été éprouvées (pannes matérielles ponctuelles, pannes logicielles n'impliquant qu'un opérateur et un réseau, catastrophes naturelles) et des leçons tirées de ces expériences.

Mais plusieurs hypothèses encore inédites devraient appeler un examen poussé, même si elles sont de degrés d'occurrence inégale, compte tenu des conséquences de leur éventuelle survenue. Ainsi, quatre d'entre elles particulièrement mériteraient d'être approfondies dans un cadre planificateur:

- 1) la *diffusion d'un ver* contaminant plusieurs opérateurs favorisée par une standardisation des équipements plus marquée;

- 2) un *black out énergétique* dépassant 6h;

- 3) une *attaque malveillante s*ur les réseaux (attentat physique contre un cœur de réseau ou une intrusion visant un effet de saturation) dont l'intérêt peut devenir particulièrement manifeste s'il est complémentaire d'une action terroriste. La difficulté momentanée de communiquer pour déployer la chaîne de secours,

demander et obtenir de l'information pourrait être alors très démultiplicatrice d'angoisse;

- 4) la *destruction accidentelle ou non d'un nœud crucial d'interconnexion Internet* et ses répercussions sur les réseaux IP.

► À moyenne échéance, c'est-à-dire rapidement: dans les 4/5 ans à peine à venir, les *facteurs d'incertitudes et de complexité* auront pris plus de poids encore, brouillant d'autant les possibilités de prospective.

*

2 / C'est pourquoi une posture de sécurité civile beaucoup plus circonspecte à l'encontre de ces risques mériterait d'être adoptée.

L'analyse en cours n'a vocation à être qu'un premier défrichage. Mais, d'ores et déjà, elle montre qu''une grande prudence s'impose. Il serait judicieux, à ce stade, d'orienter la réflexion administrative dans quatre directions prioritaires visant à :

- conforter l'efficacité de notre dispositif d'urgence (2.1);
- mieux sécuriser en soi la sphère administrative contre ces différents dysfonctionnements (2.2);
- inciter autant que faire se peut les opérateurs à intégrer plus encore des impératifs de sécurité (2.3);
- promouvoir des éléments de robustesse simples à mettre en œuvre ou qui ont déjà fait leurs preuves (2.4).

2.1/ Conforter l'efficacité de notre dispositif d'urgence.

Alors que l'expérience a mis en évidence les faiblesses de notre chaîne de réaction à plusieurs reprises lors des défaillances de réseaux de ces dernières années, l'administration n'a pas encore tiré toutes les conséquences de cette situation et continue à s'organiser avec lenteur.

Les problèmes posés à ce titre sont pourtant depuis longtemps identifiés. Ils ont trait, en cas de crise, à la détermination du niveau le plus pertinent de traitement de celle-ci (2.1.1), à la gestion des différents types de priorités à mettre en œuvre (2.1.2) et aux modalités de planification des alertes (2.1.3). Ainsi faudrait-il :

2.1.1/ Privilégier effectivement l'échelon centralisé de réaction.

A rebours de ce qui est préconisé pour nombre d'autres domaines d'intervention de la sécurité civile -y compris ceux relatifs au rétablissement d'autres catégories de réseaux vitaux-, le niveau de gestion que chacun s'accorde désormais dà recommander comme *a priori* le plus approprié en cas de crises des systèmes de télécommunications est l'échelon centralisé.

Le nombre et l'hétérogénéité des opérateurs potentiellement concernés, leur organisation qui ne se décalque pas sur les cartes administratives, leurs modes d'intervention en cas d'incidents, la technicité des problèmes sont autant de facteurs qui militent en ce sens.

Mis à part France Télécom, les préfets ne disposent pas le plus souvent d'interlocuteurs locaux chez les opérateurs qui, dans leur majorité, sont organisés au niveau national. Or, c'est à partir des salles de supervision de ces derniers que la détection des pannes sur les réseaux peut

intervenir le plus rapidement, que l'information peut être diffusée efficacement et que les actions de réparation peuvent être pilotées.

Ce constat est déjà largement partagé depuis plusieurs années. Un arbitrage interministériel a, semble-t-il, été enfin rendu pour l'instauration d'un "***guichet unique***" de l'administration (*COGIC/ CTD)*:

- à prévenir en temps réel par les opérateurs en cas de panne sérieuse;
- auprès de qui les préfets peuvent se renseigner et recevoir des directives.

Cette solution devrait éviter les effets souvent déplorés d'une gestion en "tuyaux d'orgues" et permettre une alerte rapide des pouvoirs publics dont les opérateurs n'ont pas toujours montré le souci prioritaire.

► Cet arbitrage n'a toutefois encore été traduit par aucun texte. L'urgence est donc *que les mesures règlementaires le mettant en œuvre interviennent effectivement mais qu'à cette occasion soient aussi établies des dispositions qui en imposent le respect*.

2.1.2/ Elargir la notion de priorités de rétablissement.

Les *priorités et les conditions générales de rétablissement des communications* dont bénéficient certains *usagers* font l'objet d'un arrêté actualisé du 12 janvier 2007[48]. Ce dernier prend en considération les réseaux aussi bien fixes que mobiles. Les opérateurs doivent désormais proposer des mesures pour pallier en priorité auprès de certains abonnés les conséquences les plus graves des défaillances des réseaux (soit par des remises en état graduelles, soit par des prestations particulières, telles que des moyens de substitution adaptés).

► En amont, il est cependant souhaitable que *les installations des opérateurs eux mêmes* soient prioritaires :

- pour être de nouveau raccordés aux réseaux et services essentiels (alimentation électrique au premier chef);
- et, dans la mesure du possible, qu'ils soient consultés sur les actions prises par les pouvoirs publics (délestages EDF, arrosages canadairs, positionnement des digues en cas d'inondation…).

2.1.3/ Planifier la communication d'alerte.

Dès la mise en évidence de perturbations de réseaux majeurs, une communication publique pour notamment indiquer aux usagers la marche à suivre en cas d'urgence est indispensable.

Ses conditions de réalisation, selon les circonstances, ne sont pas évidentes.

► Privilégier au sein de la zone concernée la diffusion immédiate par la *radio* ou la *télévision* de messages parait la solution la plus expédiente. L'information devrait préciser la nature de la panne, le (ou les) réseau(x) concerné(s) et les moyens alternatifs de prendre contact avec les

[48] Arrêté IND/0609264A du 12 janvier 2007 relatif aux priorités de rétablissement des communications électroniques.

services d'urgence (15/17/18/112) dès lors que l'ensemble des réseaux n'est pas touché. Il ne serait au demeurant pas anormal que cette information, à l'initiative du Cogic mais selon des modalités planifiées, intervienne aux frais des opérateurs eux-mêmes[49].

Il reste que la réception de la télévision sera elle même de plus en plus dépendante des réseaux de télécommunications et de leurs défaillances.

► Parallèlement, un recours à la *messagerie interpersonnelle (par SMS et par Internet)* devrait être prévu et intégré dans le dispositif de réaction. Non seulement les messageries sont désormais d'usage de plus en plus banal mais leur résistance particulière lors de catastrophes apparaît avérée[50]. Elle s'explique, pour des raisons à la fois techniques et socio comportementales, par les plus faibles débits numériques concernés comme le rapport Fritz[51] l'a souligné.

22/ Mieux sécuriser en soi la sphère administrative.

Trois types de mesures notamment seraient de nature à y contribuer:

2.2.1/ Garantir dans la durée l'étanchéité des réseaux de sécurité propres à l'administration.

Plus que jamais, il est essentiel pour les pouvoirs publics de conserver à terme une infrastructure minimale de *réseaux non raccordés à ceux des opérateurs*.

► Autrement dit, il faudra veiller à ce que Rimbaud, Socrate, Rubis/ Acropol ou encore le réseau 40 MHz Equipement et les réseaux appelés à leur succéder ne cèdent pas rapidement et pour des raisons avant tout budgétaires à la tentation d'emprunter certaines facilités (même présentées *a priori* comme sécurisées par des dispositions spécifiques). Ainsi en serait-il du transit par Internet ou de l'utilisation partielle de tronçons d'acheminement communs avec d'autres réseaux.

Pour autant, le maintien de telles architectures publiques autonomes ne devrait pas interdire de recourir à des "briques standard" plutôt qu'à du "sur mesure" inévitablement onéreux[52].

2.2.2/ Imposer pour les services publics névralgiques des prescriptions plus strictes en matière de sécurité des télécommunications.

Une plus grande directivité institutionnelle parait en l'espèce indispensable.

[49] L'article 8 de la loi du 13 août 2004 de modernisation de la sécurité civile prévoit déjà des obligations à cet égard pour les organismes de radiodiffusion et de télévision, mais dans un champ limité qui ne couvre pas tous les cas de figure évoqués ici.
[50] L'exemple du 11 septembre est déterminant à cet égard.
[51] Rapport du CGTI de janvier 2003 cité supra.
[52] Bien qu'il soit critiqué parce que son usage est limité, Rimbaud coûte finalement à l'Etat à peine 10 M€/an (en plus du rachat initial pour 38 M€ de son infrastructure à France Télécom) ; a contrario Acropol dont la configuration est certes plus ambitieuse et plus complexe mais qui est du "sur mesure", sera revenu pour les finances publiques, rien qu'en investissements, à près de 1 000 M€.

Les politiques suivies par les administrations en ce qui concerne la définition du niveau de sécurité de leurs équipements et la nature des liens qu'elles entretiennent avec les opérateurs sont en effet extrêmement hétérogènes sur le terrain.

Au moins ceux de ces services considérés comme les plus sensibles en raison tant de leurs missions (services de secours -SDIS/ Hôpitaux/ SAMU-, préfectures/ commissariats, EDF…) que de leur lieu d'implantation (importance stratégique de l'activité) devraient être soumis à une réglementation plus contraignante.

► Il est suggéré par conséquent de mieux encadrer au niveau national les efforts de planification locale les concernant par des *préconisations* portant à la fois sur :

- le type de protection à mettre en œuvre contre les pertes d'alimentation électrique, les incendies, les inondations etc.;

- le nombre et le mode de raccordements à respecter en matière de téléphonie fixe (au moins à deux centraux géographiquement distincts, arrivées de lignes sur des câbles distincts…) et le basculement automatique des appels arrivées sur le central en état de marche;

- la diversification souhaitable des abonnements de téléphonie mobile avec au moins deux opérateurs distincts;

- l'introduction de clauses de qualité de service (fréquence des pannes, délais de rétablissement, pénalités pour non respect des engagements) contraignantes dans les appels d'offres.

► Il pourrait être également envisagé de *soumettre les projets de passation de marchés les plus significatifs à l'examen d'une commission de sécurité des télécommunications.*

2.2.3/ Mieux se prémunir contre les risques engendrés par l'externalisation croissante des systèmes d'information.

La dynamique observée à ce titre au sein des administrations devrait être accompagnée de plus de précautions. Il est suggéré :

► en premier lieu, de *sensibiliser à l'encontre de ces risques l'ensemble des directeurs responsables de SI de services publics*. Une circulaire devrait leur être adressée précisant les règles quant à l'assurance qualité qu'il leur revient d'exiger lors d'une externalisation de services informatiques;

► en second lieu, de *définir des critères de qualité avec la profession des hébergeurs informatiques*. Un label pourrait être défini, lequel permettrait d'avoir des assurances telles que la présence d'un groupe électrogène, d'un centre de *back up* sur le territoire national ou l'établissement de doubles raccordements des salles d'hébergements aux réseaux de communications.

23/ Inciter autant que faire se peut les opérateurs à intégrer plus d'impératifs de sécurité.

Les relations entre les pouvoirs publics et les opérateurs s'inscrivent dans un cadre qui n'a pas réussi à s'affranchir jusqu'ici de ses contradictions. Les textes[53] reflètent à la fois la volonté de libéraliser le développement des télécommunications et d'affirmer certaines obligations de sécurité. Mais en pratique, ces dernières, faute de précisions suffisantes, de contrôles tangibles et de sanctions réellement appliquées en cas d'inobservation[54], se présentent à bien des titres plus comme des incantations que comme des contraintes véritables:

► depuis la *loi du 9 juillet 2004 relative aux communications électroniques*[55] (adoptée en application des directives européennes issues du "paquet télécom"), l'établissement et l'exploitation des réseaux ouverts au public et la fourniture au public des services de communications électroniques sont libres sous réserve d'une déclaration préalable auprès de l'Autorité de régulation des télécommunications;

► le *code des postes et communications électroniques* (CPCE) définit des obligations de résultats mais qui ne sont pas quantifiées en matière :

- de permanence, de qualité et de disponibilité des réseaux et des services rendus[56](assurer par exemple un accès ininterrompu aux services d'urgence),

- et d'ordre public, de défense nationale et de sécurité publique[57];

► *la loi du 13 août 2004 de modernisation de la sécurité civile* impose aux opérateurs de réseaux de télécommunications ouverts au public (donc réseaux fixes comme mobiles) de "prévoir les mesures nécessaires au maintien de la satisfaction des besoins prioritaires de la population lors de situation de crise". La nature de ces mesures reste toutefois maintenant à déterminer.

La nécessité de mieux préserver les intérêts de l'Etat et de la collectivité vis-à-vis de défaillances majeures d'un ou plusieurs réseaux de télécommunications milite donc pour une approche renouvelée du problème. Celle-ci devrait être plus dynamique de la part des pouvoirs publics et plus équilibrée.

Cette approche suppose rempli un préalable: la reconstitution au sein de l'administration d'un pôle consistant de dialogue technique avec les opérateurs (2.3.1). Elle pourrait emprunter un éventail de pistes dont les pertinences respectives devront toutefois être approfondies dans la continuité de ce premier travail (2.3.2 à 2.3.5).

---

[53] Cf. le recensement et l'analyse de ces textes faits par le CGTI dans *Propositions pour accroître le niveau de sécurité des réseaux des opérateurs de communications électroniques* – rapport DP 13-2005 de juin 2005-.

[54] En cas de non respect des obligations de l'art. D.98 (4 et 7), le CPCE prévoit (*L-36-11*) une mise en demeure par l'ARCEP qui peut être suivie: d'une suspension partielle ou totale du droit d'établir un réseau ou d'une sanction pécuniaire (<3% du CA) et en cas de manquement grave et immédiat de l'imposition de mesures conservatoires.

[55] Article *L. 33-1* du Code des postes et communications électroniques.

[56] Article *D. 98-4* du CPCE: "L'opérateur doit prendre les dispositions nécessaires pour assurer de manière permanente et continue l'exploitation du réseau et des services de communications électroniques et pour qu'il soit remédié aux effets de la défaillance du système dégradant la qualité du service pour l'ensemble ou une partie des clients, dans les délais les plus brefs.
Il prend toutes les mesures de nature à garantir un accès ininterrompu aux services d'urgence L'opérateur met en oeuvre les protections et redondances nécessaires pour garantir une qualité et une disponibilité de service satisfaisantes".

[57] Article *D. 98-7* du CPCE.

2.3.1/ Reconstituer préalablement au sein de l'Etat un pôle consistant de dialogue technique avec les opérateurs sur les questions de sécurité.

L'administration est *de moins en moins en mesure d'échanger* de façon assurée avec les opérateurs. De multiples facteurs contribuent à expliquer cette situation: la sortie de la mouvance publique de France Télécom et de son centre de recherche[58] qui a mis fin à une irrigation continue de compétences; ou encore le bouleversement permanent des technologies qui rendent rapidement obsolètes les connaissances non actualisées au cœur même des sociétés qui promeuvent ces changements.

Les capacités d'expertise publiques sur les nouveaux réseaux IP, par exemple, sont faibles. Elles sont sans commune mesure avec l'importance des enjeux avec lesquels il faudra de plus en plus composer.

► *Reconstituer une telle compétence*[59] au sein de l'administration pour d'une part pouvoir suivre l'évolution technique chez les opérateurs et dans les instances européennes et d'autre part garder une capacité à légiférer et règlementer correctement à ce propos constitue donc un impératif.

Encore faudrait-il que l'administration se reconnaisse pour autant pleinement en charge de règlementer la sécurité des réseaux. Elle ne s'est pas encore organisée complètement à cette fin: la *DGE* ne semble pas intégrer cette préoccupation; le *CTD* (commissariat aux télécommunications de défense) est sous-doté en personnels; l'*ARCEP*, quant à elle, contrairement à ce à quoi ses textes constitutifs l'invitent et en dépit de l'importance de ses moyens, semble beaucoup plus focalisée (comme du reste la Commission européenne) sur le maintien d'un contexte concurrentiel que sur le renforcement de la sécurisation globale des systèmes.

► *Un balayage des répartitions de responsabilités*, qu'elles soient de diagnostic ou de prescription, entre les services publics multiples appelés à intervenir serait opportun.

Il serait utile par exemple de désigner au sein de l'administration (ARCEP ou Minefi/ HFD) une entité chargée de suivre l'évolution de la qualité de service pour l'usager entraînée par le développement de la *VoIP*, des *boxes* et du dégroupage total. Cette entité pourrait à cette fin effectuer régulièrement (annuellement ou tous les 2 ans) un exercice majeur de simulation de panne opérateur.

Ce n'est que dans un tel cadre que le "partenariat Etat-opérateurs" auquel le rapport de J-M Hubert[60] se réfère pourra trouver sa consistance.

[58] FT R&D, ex CNET.

[59] Le ministère de la défense dispose bien d'une certaine capacité technique avec le centre électronique de l'armement (CELAR) de la délégation générale pour l'armement, mais il considère pour l'instant qu'elle n'a vocation qu'à traiter de questions militaires ; ses ressources sont d'ailleurs probablement trop limitées pour répondre avec une pleine efficacité aux besoins civils.

[60] Rapport II.D13-2004 du CGTI de décembre 2004 cité supra.

2.3.2/ Développer une conception extensive de la démarche SAIV/DNS[61].

Cette démarche initiée début 2006[62] concerne au total une douzaine de secteurs, dont celui des télécommunications. Elle n'intéresse par nature que les seuls opérateurs considérés comme d'*importance vitale*, soit, s'agissant du secteur des télécommunications, *a priori* 5 à 6 acteurs majeurs.

Elle présente plusieurs types d'intérêts. Notamment, elle impose aux opérateurs de coopérer à la protection de leurs réseaux en mettant en œuvre une autre logique que celle retenue jusqu'ici par le CPCE. Elle devrait conduire en effet à l'édiction non pas d'obligations de résultats mais de moyens[63], assorties par ailleurs de sanctions si elles ne sont pas respectées.

Cette démarche ne portera cependant tous ses fruits que si elle est entreprise, dès le départ, avec une conception extensive tant de son champ d'application que des moyens qu'on souhaite lui affecter.

► *Le spectre des menaces concernées d'abord doit être apprécié de façon large*. Certes, le fondement de cette démarche est essentiellement de "défense". Des risques graves resteront donc nécessairement en dehors de l'épure (catastrophe naturelle par exemple). Le décret de février 2006 évoque "les dommages, l'indisponibilité ou la destruction d'installations par suite d'un acte de malveillance, de sabotage ou de terrorisme". Aussi, devrait-il être clair néanmoins que la protection contre les attaques logicielles devra être intégrée dans l'exercice et qu'on n'en restera pas à une conception physique trop classique des risques.

► *La notion d'opérateur d'importance vitale ne doit pas non plus être enfermée dans un périmètre juridiquement et techniquement trop étroit*. La notion de réseau et les connexions qu'elle suppose impliquent que l'on soumette aux mêmes obligations initiales leurs activités hébergées à l'extérieur.

► La *prise en compte du contexte financier* dans lequel cette démarche doit être amenée à se déployer est enfin fondamentale dans le contexte de concurrence.

---

[61] *SAIV*: sécurité des activités d'importance vitale / *DNS* : directive nationale de sécurité.

[62] *Décret 2006-212 du 23 février 2006*, pris en application des articles L.1332-1 et suivants du *code de la défense*. Il réforme le régime de vigilance et de protection des installations les plus sensibles pour la défense de la Nation et la sécurité de l'État. Il impose aux opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel industriel, militaire ou économique, la sécurité ou la capacité de survie de la Nation, ou dont la destruction ou l'avarie pourrait présenter un danger grave pour la population, de coopérer à la protection de leurs établissements, installations ou ouvrages contre toute menace, notamment à caractère terroriste. Il précise la notion *d'opérateur d'importance vitale* et identifie les *secteurs d'activité d'importance vitale* (SAIV). Pour chacun des secteurs d'activités définis par le Premier ministre, une *directive nationale de sécurité* (DNS) doit être élaborée sous la responsabilité d'un ministre coordonnateur. Dans le cadre de cette directive, les opérateurs majeurs du secteur doivent élaborer des *plans de sécurité* couvrant leurs activités, puis des *plans particuliers de protection* de chacun de leurs *points d'importance vitale*.

[63] Ils doivent notamment réaliser une analyse des risques qu'ils encourent, identifier les points d'importance vitale (PIV), mettre en œuvre des plans particuliers de protection (PPP) pour ramener à un niveau acceptable le risque de pannes.

2.3.3/ Préférer de façon générale une logique d'incitation financière plutôt que de prescriptions normatives.

► *Imposer aux opérateurs, en cas de défaillance de leur réseau, une indemnisation forfaitaire significative de leurs utilisateurs* favoriserait une optimisation de leur effort de sécurisation supplémentaire.

Une telle logique a le mérite de la simplicité. Elle évite de s'enferrer dans une course aux détails et aux nouveautés techniques et dans des actualisations laborieuses de la réglementation. Elle laisse libre les opérateurs du choix de leurs moyens.

Ce principe a déjà été adopté dans un certain nombre de pays européens pour d'autres types de réseaux comme en Grande Bretagne pour celui de l'électricité. Différents rapports[64] ont déjà préconisé la mise en œuvre de ce type de solution.

Déjà des dispositions allant en ce sens commencent à être prévues dans notre droit:

- un arrêté de mars 2006 pris sur la base du code de la consommation impose aux opérateurs d'annoncer, dans leurs conditions contractuelles, le dédommagement qu'ils accorderont à leurs clients en cas de dysfonctionnement du service;

- un avis du conseil national de la consommation de juin 2006 permet à un abonné de résilier son contrat sans pénalité et sans frais si le service contracté n'a pas été rendu.

Il conviendrait désormais d'aller nettement plus de l'avant au travers d'une disposition législative.

2.3.4/ A défaut, définir un certain nombre de normes quantifiées en matière de qualité de service.

Les prescriptions du CPCE sont actuellement essentiellement de nature qualitative. Elles sont donc d'application et de contrôle difficiles.

Même si la problématique de la qualité de service à exiger est complexe en raison de l'évolution permanente des réseaux, la mission considère qu'à défaut d'approche financière incitative des normes quantifiées devraient s'appliquer à tous les opérateurs. Elles porteraient d'une part sur une qualité de service minimale imposée et d'autre part sur l'obligation pour les opérateurs de publier régulièrement leurs résultats en matière de qualité de service.

Ces normes devraient :

- définir des *niveaux minima de qualité de service* (durée d'indisponibilité moyenne par an et par abonné, qualité de la voix, délais de transmission des mails…)

- exiger certaines *bonnes pratiques* (supervisions permanentes des réseaux, astreintes, duplication des équipements sensibles, organisation de cellules de crises, plans de secours, …), notamment en ce qui concerne la sécurité des outils informatiques gérant les réseaux de télécommunication (redondance des moyens

[64] Rapport du Conseil général des mines sur *la sécurisation du réseau électrique français* (2000) ou rapport de la mission interministérielle sur *les tempêtes des 26 et 28 décembre 1999* (2001).

informatiques centraux, sécurité incendie, sécurité des alimentations électriques, sécurité vis-à-vis de certains risques particuliers : inondations, séismes etc.)

Elles devraient en outre imposer des *règles relatives aux réseaux* :

- tenue des ouvrages à diverses sollicitations (vent, inondation, séismes, etc.);

- protection des liaisons, profondeur des lignes enterrées, application du décret de 1991 sur les travaux à proximité, protection des faisceaux hertziens, etc.

- maillage des réseaux pour faire face à une ou plusieurs coupures simultanées sur un réseau;

- protection des nœuds des réseaux;

- gestion des prioritaires en cas de crise (cf. § 2.1.2).

  A cet égard, la mission s'est interrogée sur la nécessité de définir des *classes d'abonnés prioritaires en cas de saturation des réseaux*. Il n'a pas retenu cette option qui a déjà fait l'objet d'une réflexion par un groupe de travail de la CICREST. Les difficultés techniques en effet sont fortes. Les mécanismes envisageables (lignes essentielles pour le fixe, classes de service, voire possibilité d'itinérance, pour le mobile) n'ont jamais été mis en œuvre en pratique pour des raisons organisationnelles et financières.

  En outre, la répartition de la charge financière entre les différents partenaires (les usagers concernés qui ne sont pas forcément demandeurs, l'ensemble des usagers si on taxe les opérateurs, l'Etat) n'est pas simple.

Les opérateurs des divers réseaux de télécommunications devraient avoir non seulement l'obligation de respecter ces diverses règles mais également de présenter à l'administration une étude de sécurité décrivant les risques pris en compte, les mesures de prévention et de secours adoptées et montrant comment cet ensemble permet de respecter les objectifs en terme de sécurité des réseaux de télécommunication.

Le contexte concurrentiel rend pratiquement obligatoire l'égalité de traitement vis à vis de la qualité.

2.3.5/ Renforcer, en dernière instance, le pouvoir de sanctions de l'administration vis à vis des opérateurs et, plus précisément, des exploitants de réseaux.

Les obligations du CPCE ne sont pas appliquées car, indépendamment de leur caractère uniquement qualitatif, elles ne sont assorties en pratique d'aucune sanction:

- il n'est pas sûr que celles qui sont prévues pour le non respect de l'article D-98 soient, compte tenu de leur importance, très réalistes;

- le détenteur du pouvoir de sanctions, en l'espèce l'ARCEP, n'a pas placé la sécurité au centre de ses préoccupations.

► *Il revient d'imaginer les voies et les moyens pour que l'administration (ministère en charge de l'industrie) dispose en propre d'un pouvoir effectif* :

- pour obtenir des informations sur leurs réseaux et leurs vulnérabilités (la mission a eu de réelles difficultés pour obtenir des informations sur le réseau de l'opérateur historique);

- pour sanctionner le non respect du niveau exigé de qualité de service.

2.4/ Promouvoir des éléments de robustesse simples à mettre en œuvre ou qui ont déjà fait leurs preuves.

Sans doute importe-il aussi d'être le plus pragmatique possible. Deux exemples de types d'actions envisageables peuvent être présentés en ce sens:

2.4.1/ Standardiser des équipements à disposition de l'usager qui soient de conception plus sûre.

Sachant que la garantie de pouvoir téléphoner dont chaque abonné bénéficiait jusqu'ici en cas de panne électrique chez lui tend à disparaître avec les nouveaux services, il apparaît nécessaire de prévoir des aménagements simples de précaution tendant à remédier à cette baisse de sécurité..

► Ainsi, il est suggéré que *les "boxes*", par lesquelles passeront dans le futur la quasi intégralité des possibilités de communication à domicile, *soient en mesure de conserver une autonomie de liaison minimum en cas d'interruption de l'alimentation électrique générale*. A ce titre, elles pourraient comporter dans des versions de haute disponibilité une pile permettant au moins l'appel téléphonique..

2.4.2/ Tirer les conséquences de la résistance particulière et jusqu'ici avérée des messageries.

Faisant le retour d'expérience des attentats du 11 septembre 2001, le CGTI[65] a eu l'occasion d'attirer l'attention sur les caractéristiques particulières des messageries interpersonnelles et leur utilité -générale et de recours- en cas de catastrophe[66].

[65] Cf. rapport de 2003 cité supra.

[66] "Cette résistance de la messagerie dans les circonstances dramatiques du 11 septembre ne tient nullement à une vertu spéciale de l'Internet, mais essentiellement aux caractéristiques de la messagerie elle-même, totalement opposées à celles de la téléphonie. Il s'agit d'une communication en temps différé, dans laquelle on ne gère pas la présence du destinataire. Le volume d'un message est très faible, tant qu'on n'y adjoint pas d'image fixe ou surtout animée. Enfin, le volume habituel de messagerie est tel que la crise du 11 septembre ne se traduisit pas par une surcharge perceptible. Ces caractéristiques éliminent le phénomène de répétition des appels, provoquée notamment par la non-réponse du demandé. C'est ce phénomène de répétition d'appels qui est si préjudiciable au réseau téléphonique en cas de crise engendrant une grande anxiété du public. Les caractéristiques de la messagerie entraînent également une modestie des moyens mis en œuvre (le trafic de messagerie représente quelques % du trafic général de l'Internet), et l'acceptation de supports divers et rustiques".

► La mission ne peut que souscrire à sa suggestion d'accorder un soin particulier à leur résistance aux catastrophes, et pour toutes les variantes répandues (SMS, messageries « instantanées », ..), ce qui lui apparaît relativement plus facile que pour les autres services, compte tenu des faibles débits numériques concernés tant qu'on y adjoint pas d'images fixes ou surtout animées.

*
* *