Référence: RR 2004.04 du 24/05/04 **Diffusion libre**

# Les télécommunications en cas de crise

*(Relevé des points essentiels)*

♣♣♣

**Objet :** Table ronde de l'IREST (1) au Palais du Luxembourg le 17 mai 2004.
**Intervenants :**

- **Catherine Bourassin** (Animateur) : Ingénieur en télécommunications et Conseillère technique
- **Gilles Sanson** : Inspecteur Général au Ministère de l'Intérieur
- **Jean Douat** : Ingénieur Général de l'armement au Ministère de la Défense
- **Philippe Duluc** : Ingénieur en Chef de l'armement, Directeur de la Sécurité à France Télécom
- **Richard Lalande** : Président de l'Association française des opérateurs de télécommunications
- **Alain Coursaget** : Ingénieur général des télécommunications, Directeur Adjoint de la protection et de la sécurité de l'Etat

## Préambule

Cette table ronde animée par Catherine Bourassin, qui fut responsable du CICREST (2), visait à analyser les mesures de prévention nécessaires pour réduire les conséquences d'une crise dans les télécommunications. Il convenait également de se préparer à toute forme d'attaque des réseaux et des services de télécommunications au niveau national. En effet, ce thème reste l'un des plus préoccupants pour les télécommunications car il touche à la sécurité des citoyens.

## La gestion de la crise, un enjeu majeur de sécurité *(Gilles Sanson)*

Gilles Sanson a présidé la commission interministérielle chargée d'établir le rapport sur les conséquences à tirer des dégâts innombrables causés par les deux tempêtes Lothard et Martin des 26 et 28 décembre 1999. Ce rapport a servi de base à la préparation du projet de loi sur la réforme de la protection civile et des zones de défense.

- **Un constat accablant**

Chacun garde en mémoire les conséquences des tempêtes car elles ont été catastrophiques pour les réseaux de télécommunications comme pour ceux de l'EDF: trois millions et demi de foyers privés d'électricité, un million de lignes fixes téléphoniques hors d'usage et une part notable des réseaux mobiles détériorée.
Pour sa part, France Télécom a dû consacrer un milliard de francs à la remise en état de ses réseaux car soixante neuf départements étaient concernés.
Ces évènements ont mis en évidence la grande vulnérabilité de notre pays en cas de catastrophe d'envergure, notamment celle de nos réseaux vitaux de plus en plus interdépendants.
Les réseaux concernés, très malmenés durant ces tempêtes, ne font pas l'objet de prescriptions sur la sécurité minimale de leurs équipements et ne prennent pas en compte les impératifs d'une gestion de crise, en particulier les réseaux pour mobiles.

- **Les leçons à tirer**

A l'avenir, la viabilité des communications devra être mieux garantie et il convient de ne plus laisser aux seules logiques du marché l'exclusivité de la réponse à cette préoccupation majeure, autrement dit ne pas laisser aux seuls opérateurs le soin de définir le niveau de sécurité de leurs équipements.
Actuellement, aucune contrainte externe objective *(logique contractuelle, assurance commerciale ou concurrentielle)* ne pousse les opérateurs à prendre en compte la sécurité au regard de l'intérêt général.
Il a été recommandé de faire prévaloir, plus ouvertement, la notion de service public pour imposer aux opérateurs, par voie réglementaire ou concertée, un niveau plus élevé de sécurité des équipements. C'est le cas notamment de l'**autonomie énergétique** des commutateurs secondaires ou des stations de base pour mobiles.
L'introduction de formules de responsabilisation financière directe des opérateurs a également été suggérée.

*(1) Institut de Recherches Economiques et Sociales sur les Télécommunications*
*(2) Commission Interministérielle de Coordination des Réseaux et des Services de Télécommunications pour la défense et la sécurité civile en cas de crise (Commission regroupant 22 ministères ainsi que les opérateurs)*

…/…

## La stratégie de diversification des réseaux *(Jean Douat)*

Jean Douat rappelle que le Ministère de la défense a misé sur la diversification des réseaux, adaptés aux besoins de communications vitales, pour faire face aux différentes situations de crise des télécommunications :

- ✓ **Réseau Rita :** c'est un réseau tactique de l'armée de terre (réseau mobile connectable sur micro-ordinateur) qui a été conçu comme aide à la gestion des conflits internationaux et comme outil de communications pour des opérations d'envergure nationale. Il a été déployé par brigades et chaque brigade dispose des 283 stations de supervision, transmission et commutation.

- ✓ **Réseau Socrate :** c'est un réseau de transit maillé et dense, à couverture nationale, dont les débits peuvent varier de 64 kbps à plusieurs dizaines de Mbps. Il est capable de hiérarchiser les flux entrants par degré de priorité et il a été durci pour résister aux piratages, aux catastrophes naturelles ou chimiques, ainsi qu'aux autres crises de toutes natures.

- ✓ **Réseau Syracuse III :** c'est un réseau de trois satellites à hauts débits variables en fonction des circonstances. Il peut se connecter aux deux réseaux précédents, ainsi qu'à celui de l'Elysée.

L'une des caractéristiques les plus intéressantes de ces trois types de réseaux, dont les configurations sont très différentes (réseau fixe, réseau mobile, réseau à grande élongation …), c'est leur aptitude à se relayer et à se connecter en cas de besoin pour des applications civils ou militaires.

## La gestion de crise chez France Télécom *(Philippe Duluc)*

Philippe Duluc présente d'abord un historique des diverses « crises » que connut France Télécom au cours des dernières décennies :

- **Novembre 1981 :** suite à un incendie au centre de transmissions de Lyon Sévigné, un million d'usagers lyonnais furent privés de télécommunications pendant deux ou trois jours.
  *Remède: re-routage des communications*
  *Décision: sécurisation du réseau et création du «Service de Sécurité des Télécommunications»*

- **Décembre 1999 :** suite à des tempêtes climatiques, un million d'usagers se trouvaient isolés sur une période allant de quelques heures à trois semaines.
  *Remède: 5200 km d'artères à réparer et 150000 poteaux à remettre en état*
  *Constat: interdépendances des infrastructures vitales (EDF et FT)*

- **Janvier 2003:** suite à la propagation du virus informatique « Slammer-Sapphire », 90% des serveurs ont été infectés en moins de 10 minutes, entraînant une paralysie d'Internet et une fermeture de nombreux réseaux d'entreprises.
  *Constat: méconnaissance du problème et réactivité trop longue*
  *Décision: remèdes palliatifs au « tout IP » à déployer pour amoindrir les risques*

Quelle que soit la typologie des crises *(tempêtes, inondations, incendies, virus informatique …),* les remèdes s'appuient sur des mécanismes parfois similaires *(remontée des alertes vers les services concernés, mise en commun des moyens des opérateurs, communications descendantes vers les populations …)* tout en s'appuyant sur les services de l'Etat *(police, gendarmerie, pompiers, SAMU, réseau Rimbaud* …).
Bien que France Télécom ait mis au point un outil de gestion de crise : le **réseau d'alerte et d'intervention national** qui relie les 80 centres les plus stratégiques avec des liaisons spécialisées, il faut développer une politique d'entraide des opérateurs et réserver des ressources de télécommunications communes.

## L'implication des opérateurs alternatifs dans la crise *(Richard Lalande)*

La stratégie des opérateurs alternatifs repose sur plusieurs données :

- ✓ des procédures prédéfinies avec les « zones de défense »,
- ✓ une organisation pour prendre en charge les interventions dans un délai de quatre heures,
- ✓ une sécurisation par redondance des boucles locales *(réseaux fixes et mobiles),*
- ✓ une flotte de **générateurs de secours** dédiés aux mobiles pour compenser les défaillances du réseau.

Dans l'assistance, Jean-Jacques Damlamian fait remarquer que la prise de conscience du **rôle fondamental des réseaux en matière de sécurité des personnes** est tout à fait nouvelle et que les attaques des réseaux n'étaient apparues que très récemment.

…/…

## Conclusion sur la gestion des crises *(Alain Coursaget)*

Pour le Secrétariat Général de la Défense Nationale (SGDN), le **concept de sécurité** exige un travail en amont : une analyse critique des risques et un recensement exhaustif des disponibilités d'accès, en sachant bien que l'on devra faire face à une **saturation des réseaux**, comme des moyens, en temps de crise. Néanmoins, tous les réseaux civils sont interconnectés et le nouveau réseau ACROPOL fournira des solutions appréciables en fin 2006, avec **40 000** terminaux disponibles pour des applications sur le terrain. On classe d'ailleurs les réseaux selon leur niveau de disponibilité : disponibilité élevée pour les réseaux sécurisés (Rita, Socrate, ACROPOL …), disponibilité normale pour les réseaux publics (RTC, GSM, Internet).
Dans un scénario impliquant toutes les chaînes opérationnelles *(chaînes de commandement nationales, grands opérateurs nationaux, chaînes territoriales, équipes d'intervention tactiques …)* on dénote néanmoins un manque de transversalité dans le fonctionnement des institutions gouvernementales.

**René REVOL** (24/05/04)