INFRA-STRUC-TURES NUMÉ-RIQUES

ESSENTIELLES
C'EST UNE ÉVIDENCE,
RÉSILIENTES
C'EST UNE EXIGENCE

InfraNum

BANQUE des TERRITOIRES | Caisse des Dépôts GROUPE

PHILIPPE LE GRAND
PRÉSIDENT D'INFRANUM

Echéance initiale du Plan France THD, 2022 nous invite à mesurer le chemin parcouru ensemble dans cette grande aventure. Dix ans plus tard, le succès est incontestable et les promesses ont été largement tenues. Le chantier n'est toutefois pas achevé, et l'ambition des pouvoirs publics d'aller encore plus loin dans le déploiement de la fibre, en fixant un objectif de généralisation du FttH à l'horizon 2025, va continuer de mobiliser pleinement toute la filière.

Cependant, pressés d'obtenir des résultats, d'accélérer, nous avons été depuis plusieurs années guidés par les urgences et n'avons pas eu l'opportunité de prendre du recul sur notre action. La crise sanitaire a été le déclencheur d'une prise de conscience pour beaucoup d'entre nous :

- les confinements auraient-ils été soutenables sans ces réseaux qui maillent déjà largement la France, et dont l'absence s'est faite ressentir de manière criante pour certains citoyens ?
- mobilisés par des déploiements toujours massifs, avons-nous collectivement anticipé toutes les implications de la bascule d'un réseau cuivre vers des réseaux en fibre optique ?

C'est le sens de l'appel de Deauville que j'ai formulé le 29 mars : les réseaux de communications électroniques et, plus largement, toutes les infrastructures numériques qui maillent nos territoires, sont les fondations de la France de demain. C'est à partir de ce constat que nous avons décidé de mener une étude dédiée en lien avec la Banque des Territoires.

Cette première étude a pour objectif de faire de la pérennité des infrastructures numériques une priorité nationale. En effet, si le caractère essentiel des réseaux n'est plus à démontrer, il est désormais urgent d'assurer leur résilience.

LA RÉSILIENCE DES INFRASTRUCTURES NUMÉRIQUES, PRÉREQUIS DE NOTRE SOUVERAINETÉ NATIONALE

RÉSILIENCE

« Capacité de résister aux conséquences d'une crise ou d'une agression et de retrouver le plus rapidement possible un fonctionnement normal, même si celui-ci est différent du fonctionnement précédent. »

LES INFRASTRUCTURES NUMÉRIQUES SUPPORTENT DES SERVICES DÉSORMAIS « ESSENTIELS »

Les réseaux de communications électroniques ont joué un rôle déterminant dans la poursuite des activités du pays au cours des confinements successifs. Malgré la soudaineté des évènements, les réseaux n'ont pas connu de difficultés significatives et les communications n'ont jamais été interrompues.

La crise sanitaire a ainsi révélé, si cela était encore nécessaire, le caractère essentiel des infrastructures numériques dans la poursuite de la vie de la Nation.

Dans les prochaines années, la transformation numérique des territoires va se poursuivre : déploiement de la 5G, essor de l'IoT mais aussi dématérialisation de certains services publics et développement d'usages encore émergents, comme la télémédecine. Le rôle des infrastructures sera de plus en plus crucial.

LA RÉSILIENCE DES INFRASTRUCTURES NUMÉRIQUES DOIT ÊTRE ASSURÉE

La permanence de ces réseaux, et leur capacité à surmonter les différents aléas, ne sont pourtant pas évidentes et constituent des défis pour la filière et les pouvoirs publics.

Le risque climatique, comme l'ont démontré les dégâts provoqués par la tempête Alex dans les Alpes-Maritimes, estimés à plus d'un milliard d'euros, est encore mal évalué. Le contexte international, marqué par la pandémie et la résurgence des conflits armés sur le sol européen, interroge. Enfin, de nombreux cas de vandalisme, mais également d'atteintes coordonnées physiques ou cyber sont recensés.

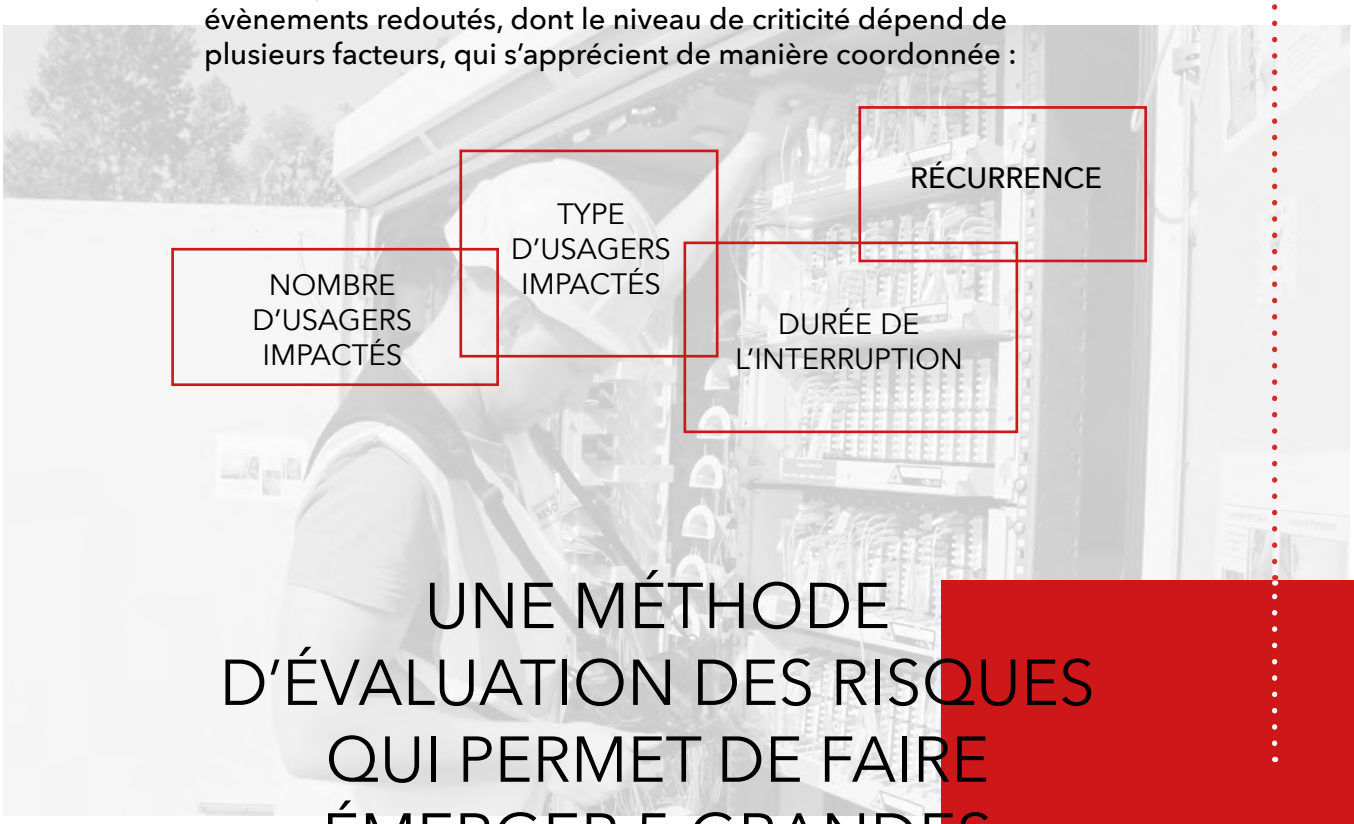
Par ailleurs, le contexte actuel de transition progressive d'un réseau historique exploité par un acteur unique vers de multiples acteurs locaux, relevant de régimes différents (initiative privée ou initiative publique), implique une coordination étroite entre tous les acteurs publics et privés.

Cette première étude, fondée sur une série d'entretiens auprès d'acteurs de la filière, de collectivités locales et de représentants de l'Etat, a pour objectif de :

- recenser les aléas pouvant impacter la continuité de service des réseaux FttH
- évaluer la criticité de ces aléas
- identifier les moyens d'anticipation et de limitation des risques *ex ante*
- proposer des axes d'amélioration en matière de gestion de crise

MESURER LA CRITICITÉ D'UNE INTERRUPTION DE SERVICE

L'interruption et la dégradation des services sont les deux évènements redoutés, dont le niveau de criticité dépend de plusieurs facteurs, qui s'apprécient de manière coordonnée :



UNE MÉTHODE D'ÉVALUATION DES RISQUES QUI PERMET DE FAIRE ÉMERGER 5 GRANDES CATÉGORIES DE RISQUES

Suivant la méthode EBIOS 2010, une série de scénarios de menace a été établie. Le risque de chaque menace est apprécié en fonction de sa gravité et de sa vraisemblance. A chaque menace, des mesures de sécurité ont été identifiées afin de réduire son niveau de risque.

Cette approche théorique a ensuite été soumise aux contributeurs de l'étude, représentant plusieurs familles d'acteurs : opérateurs d'infrastructures, intégrateurs-constructeurs, équipementiers, datacenters, gestionnaires de réseau d'envergure nationale, représentants de l'Etat, collectivités locales et associations représentatives.

1 ACTES DE MALVEILLANCE ET ACCIDENTS

RISQUES IDENTIFIÉS

RECRUDESCENCE DES ACTES DE MALVEILLANCE

Ces actes de malveillance, qui concernent tant les infrastructures fixes que mobiles, sont de plus en plus fréquents (section de câbles, incendie, destruction d'armoires, etc.).

VIGILANCE CONCERNANT LES SITES TRÈS CRITIQUES (DATACENTERS, POP)

Les mesures de sécurité concernent souvent l'accès au site, l'alimentation électrique ou la sécurité incendie, mais on constate cependant des points de fragilité dans les infrastructures assurant la connectivité du site.

LES ACCIDENTS RESTENT L'UNE DES PRINCIPALES CAUSES D'INTERRUPTION DE SERVICE

Par exemple lors de la réalisation de travaux de voirie ou en cas d'accident sur la chaussée impactant un armoire.

SPÉCIFICITÉ DU RISQUE CYBER

Les systèmes d'information pourraient être la cible d'une cyberattaque aux impacts forts.

RÉPONSES POSSIBLES

Redonder les infrastructures sensibles et renforcer la sécurité des sites très sensibles (datacenters, POP, NRO), notamment les portes de sortie des plaques réseau

Prévoir des infrastructures de rechange (« spare ») afin de limiter le temps de rétablissement (SRO, NRO, groupe électrogène)

Adapter la sécurité des points de mutualisation, simple ou renforcée, aux spécificités des territoires et des projets

Renforcer la sécurité des infrastructures, notamment en développant la vidéoprotection en lien avec les collectivités locales

2 FRAGILITÉ DES INFRASTRUCTURES AÉRIENNES

RISQUES IDENTIFIÉS

Une partie importante des réseaux FttH s'appuie sur des supports aériens : plus de 500 000 km de linéaire, en particulier dans les zones rurales.

Ces segments de réseau sont particulièrement exposés aux intempéries, à la végétation ou au risque d'incendie, ces segments de réseaux sont plus fragiles que le génie civil souterrain

La fragilité des infrastructures aériennes est accentuée par plusieurs facteurs :

- obsolescence de parts significatives du génie civil aérien
- difficultés à assurer, sur l'ensemble du territoire, l'entretien de la végétation environnante
- fragilité des matériaux composites, en particulier en cas de chocs

RÉPONSES POSSIBLES

Enfouissement des réseaux, à minima les plus sensibles (collecte, transport) et desservant des sites stratégiques (entreprises, services publics, etc.)

Veiller à l'organisation et à la disponibilité d'unités d'intervention rapides en cas d'incident

Renforcer les actions entre la filière et les acteurs publics pour améliorer l'élagage à proximité des réseaux

Prévoir un fond de soutien exceptionnel, le cas échéant mutualisé avec d'autres réseaux, en cas de catastrophe de grande ampleur, en particulier dans les territoires ultramarins (cyclone, séisme, éruption volcanique, etc.)

10 MILLIARDS € : évaluation du montant nécessaire pour enfouir environ 50% du génie civil aérien

Source : Observatoire du Très Haut Débit 2022, InfraNum

3 NON-CONFORMITÉ ET MALFAÇONS

RISQUES IDENTIFIÉS

LORS DE LA CONSTRUCTION ET DE L'EXPLOITATION

Hétérogénéité, en dépit d'un important effort de standardisation, de certains éléments de réseau, lié notamment à la diversité des maîtres d'ouvrage et des intervenants, ainsi qu'à l'évolution des bonnes pratiques.

Des cas de non-conformité par rapport aux standards lors de la construction sont observés :

- règles de construction (lovage des câbles, profondeur du génie civil, grillage avertisseur)
- matériaux recommandés (type de câble optique, boitier)
- règles d'ingénierie (dimensionnement des armoires, des câbles)

En matière d'exploitation, des manquements sont également observés, notamment dans les systèmes d'informations parfois mal renseignés (ex : routes optiques).

LORS DES OPÉRATIONS DE RACCORDEMENTS

Les problématiques observées en matière de raccordements amplifient les risques identifiés : multitude d'intervenants, dégradation prématurée des équipements, décalage entre le référentiel réseau et la réalité.

RÉPONSES POSSIBLES

En cohérence avec le plan d'action relatif à la qualité des raccordement présenté en juin 2022 par InfraNum, plusieurs mesures peuvent être mise en place :

- labellisation des entreprises et des intervenants
- partage des plannings d'intervention entre opérateurs commerciaux et opérateurs d'infrastructures
- faire du compte-rendu d'intervention la clef de voûte du dispositif de validation de la qualité du raccordement, renforcer et homogénéiser les moyens de contrôle à l'aide de l'IA

Par ailleurs, des mesures complémentaires peuvent être envisagées :

- **engager** une campagne pour remédier aux singularités et dégradations observées sur certains réseaux
- **renforcer** la sécurité des éléments de réseau (armoires intelligentes, videoprotection)

4 INTERVENTIONS SUR DES RÉSEAUX EN EXPLOITATION

« Le fait d'intervenir sur des réseaux en exploitation génère mécaniquement un taux d'accidentologie plus important. »

RISQUES IDENTIFIÉS

Le décommissionnement du cuivre pourrait présenter des risques importants sur les infrastructures optiques :

- arrachage des câbles dans les fourreaux
- chutes de poteaux
- etc.

D'autres interventions, plus ponctuelles, pourraient également présenter un risque :

- forte densification, nécessitant un redéploiement d'ampleur
- ré-ingénierie d'un réseau.

RÉPONSES POSSIBLES

Poursuivre et amplifier la concertation entre l'ensemble des acteurs concernés par les interventions sur les réseaux en exploitation, en particulier dans le cadre de la fin du réseau cuivre :

- **renforcer** les moyens de maintenance temporairement lorsque des interventions sont prévues sur ou à proximité des réseaux FttH
- **coordonner** les intervenants sur le terrain
- **évaluer** la nécessité de renforcer les actions de formation auprès des intervenants

Orange, en tant qu'opérateur de réseau cuivre, a annoncé en novembre 2019 sa volonté de fermer techniquement le réseau cuivre d'ici à 2030 et a défini un plan de fermeture. Transmis à l'Arcep en début d'année, ce plan a fait l'objet d'une consultation publique entre février et avril 2022. Une phase d'expérimentation, achevée dans la commune de Lévis-Saint-Nom (78), est actuellement en cours dans 6 communes : Issancourt-et-Rumel, Vivier-au-Court, Vrigne-au-Bois, Gernelle (08), de Provin (59) et de Voisins-le-Bretonneux (78). La fermeture technique s'échelonnera entre 2023 et 2030.

CAPACITÉ À FAIRE FACE AUX CRISES

5

RISQUES IDENTIFIÉS

UNE ORGANISATION DE L'ETAT CENTRAL ET DÉCONCENTRÉ MÉCONNUE PAR UN CERTAIN NOMBRE D'ACTEURS, PRIVÉS COMME PUBLICS

Le Secrétariat général de la défense et de la sécurité nationale (SGDSN), rattaché au Premier ministre et chargé notamment d'anticiper, prévenir et répondre D'autres administrations peuvent être amenées à intervenir : Commissariat des communications électronique de Défense (CCED), Direction générale de la Sécurité civile et de la gestion des crises (DGSCGC), Haut-fonctionnaire de défense et de sécurité (HFDS). Enfin, le rôle des préfets est généralement bien identifié sur les territoires en cas de crise.

L'ENJEU DE LA COORDINATION ENTRE LES ACTEURS DE LA FILIÈRE, PUBLICS ET PRIVÉS, LOCAUX ET NATIONAUX

Le découpage des déploiements FttH en France, d'initiative privée ou publique, entre plusieurs opérateurs d'infrastructures - parfois 4 ou 5 à l'échelle d'un département, sans compter les réseaux FttO - **implique une coordination étroite entre ces acteurs**.

LA NÉCESSAIRE ARTICULATION AVEC LES AUTRES GESTIONNAIRES DE RÉSEAUX

Les réseaux sont interdépendants, tant en raison de leur proximité physique (réseaux FttH déployés sur le domaine public routier ou appuis communs du réseau de distribution d'électricité) qu'aux lienx entre les exploitants (par ex : besoin d'alimentation électrique pour les réseaux télécoms).

RÉPONSES POSSIBLES

Dans ses « **trente propositions pour une France connectée et durable** » publiées en mars 2022, InfraNum demandait l'organisation d'un *« Grenelle de la résilience et de la souveraineté des infrastructures numériques, à l'aune de la décentralisation des réseaux »*.

CONCLUSION

AMÉLIORER LA COORDINATION

Améliorer la coordination des différents acteurs

- **1** Grenelle de la résilience, permettant d'établir une feuille de route nationale
- soutenir la réalisation, par les collectivités locales, de schémas locaux de résilience
- encourager la mutualisation des moyens en réponse aux incidents majeurs

VEILLER À L'EXPLOITABILITÉ ET À LA DURABILITÉ DES RÉSEAUX

Veiller à l'exploitabilité et à la durabilité des réseaux / préserver l'intégrité des réseaux

- **3** axes du plan d'action relatif à la qualité des raccordements proposé par InfraNum, afin d'assurer un niveau de formation satisfaisant et d'accentuer et d'automatiser les contrôles
- maintenir la vigilance vis-à-vis du risque cyber

ASSURER LA PÉRENNITÉ DES INFRASTRUCTURES

Assurer la pérennité et la sécurisation des infrastructures

- **10** Mds€ pour effacer 50 % du génie civil, prioritairement ceux supportant des liens de collecte et de transport et pouvant représenter 7 000 ETP

  Source : Observatoire THD 2022
- renforcer la sécurité des installations grâce aux différentes technologies existantes, le cas échéant en lien avec les forces de l'ordre

Les acteurs de la filière ont déjà fait la démonstration de leur résilience, en particulier lors de la crise sanitaire, en réussissant tant à maintenir les communications mais aussi à poursuivre massivement les déploiements et les raccordements.

Cependant, une partie des risques identifiés ne sont aujourd'hui pas suffisamment appréhendés. La filière, les collectivités locales et l'Etat ont la responsabilité de poursuivre leurs efforts afin de réduire ces risques, mais aussi de prévoir des mesures en réponse aux crises qui ne pourraient être évitées.

Infrastructures numériques :
Essentielles, c'est une évidence,
Résilientes c'est une exigence.

INFRASTRUCTURES NUMÉRIQUES

ESSENTIELLES
C'EST UNE ÉVIDENCE,
RÉSILIENTES
C'EST UNE EXIGENCE

InfraNum

BANQUE des TERRITOIRES

Caisse des Dépôts GROUPE