# Résilience des infrastructures numériques

Nov 2025

## Avant-propos

L'AFUTT, association des utilisateurs des télécommunications veille, depuis sa création, à ce que tous les citoyens disposent, partout sur le territoire, d'une bonne connectivité fixe et mobile, avec un taux de disponibilité élevé, pour accéder aux services numériques dont ils ont besoin dans leurs usages personnels ou professionnels.

Donc nous suivons de près les questions de résilience en particulier à travers les travaux de notre groupe de réflexion multilatéral Qostic.

Pour conduire une politique de résilience efficiente, il faut pouvoir se fixer des objectifs en ligne avec les attentes des utilisateurs finaux, sans quoi les efforts seraient vains ou pourraient être parfois inutilement surdimensionnés.

C'est pourquoi les travaux de l'AFUTT sur l'expérience utilisateur c'est-à-dire la qualité perçue mise en perspective avec la qualité attendue, et la qualité rendue, sont utiles en toile de fond pour aborder la question de la résilience des infrastructures numériques[1]. C'est à l'aune de ces regards croisés et de données à la fois quantitatives et qualitatives, que l'on peut établir des objectifs de résilience en termes de : *niveau de service acceptable, niveau de service insatisfaisant, et niveau de service inacceptable*.

## Résilience : de quoi parle-t-on ?

Le terme de résilience est aujourd'hui largement usité dans de nombreux domaines, c'est pourquoi il peut apparaitre très général et finalement assez flou. Il est donc nécessaire dans un premier temps de cerner le concept dans le domaine spécifique des infrastructures numériques. Sans une clarification préalable sur le périmètre à couvrir, il n'est pas possible de bien identifier les problèmes à traiter et les solutions ou actions à mettre en place.

Or, les approches diffèrent quelques peu selon la manière dont on envisage les interactions entre différentes notions associées à la résilience, telles que : sureté, sécurité, résistance, robustesse, intégrité, réparabilité…

On peut d'abord donner la définition retenue par l'Union Internationale des Télécoms (UIT) en 2019, dans un document traitant de l'exploitation des réseaux de communications électroniques et les services associés.

[1] Voir notre livre blanc sur la qualité de service et la qualité d'expérience dans le secteur des télécommunications https://www.afutt.org/livre-blanc-qos

« aptitude à fournir et à maintenir un niveau acceptable de service en présence de défauts et de problèmes affectant le fonctionnement normal d'un réseau de communication donné »

De manière plus indirecte, l'Union Européenne aborde ce sujet sous l'angle de la cyber sécurité, en particulier par le biais de la directive dite NIS 2 de 2022 qui prône une approche « tous risques » qui par-delà la protection contre les attaques cyber, vise également « à protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre des événements tels que le vol, les incendies, les inondations, une défaillance des télécommunications ou une défaillance électrique ».

En France, la banque des territoires dans son guide méthodologique pour élaborer son schéma local de résilience, adopte une approche plus restreinte, centrée sur la résistance et la défense face à des évènements exceptionnels, avec cette définition :

« 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 »

Enfin citons les travaux du cercle Credo sur la résilience des réseaux FttH (2024) avec cette définition :

« La résilience est la capacité de résistance et d'absorption des défaillances sans perte majeure de fonctionnalités et avec une restauration rapide du service, totale ou partielle »

Avec les sous définitions suivantes :

résistance : capacité du réseau et de ses équipements à résister aux défaillances
absorption : capacité à fonctionner et à s'adapter en dépit d'incidents
Restauration : capacité à rétablir rapidement les services

## Des métriques à mettre en place

Pour prendre les bonnes décisions et rendre les réseaux numériques plus résilients, il est essentiel dans un premier temps d'établir des métriques qui permettent de bien cerner les problèmes.

Il s'agit de bien identifier les risques de défaillance, leur origine, leur occurrence, leur impact, autrement dit leur gravité.

**Origine des pannes** : il est généralement admis que l'on peut distinguer les erreurs humaines (dont le non-respect des normes et bonnes pratiques), les actes malveillants (dont les cyber-attaques), les catastrophes naturelles, et les défaillances système.

Il est possible ensuite d'approfondir l'origine des pannes en détaillant les pannes par sous-catégories.

Ainsi, dans la catégorie des défaillances système, il est utile de disposer d'une déclinaison plus fine, par exemple avec la typologie suivante : pannes matériel / bugs logiciel / mises à jour de logiciel / coupures d'alimentation / ruptures de câble

**Mesure d'impact :** En matière d'impact on doit principalement s'intéresser à l'occurrence des défaillances (autrement dit leur fréquence), leur durée et leur empreinte géographique. En fonction des impacts prévisibles ou constatés, on peut associer un ***niveau de gravité*** comme on le verra plus loin.

Une manière simple et pertinente de mesurer l'impact consiste à rechercher le nombre d'heures de service perdue par l'ensemble des utilisateurs finaux affectés par les défaillances. En effet, cet indicateur est un agrégat de la fréquence, de la durée et de l'ampleur géographique des pannes, donc de la gravité de celles-ci, et de plus il rend compte de l'expérience utilisateur.

On peut noter que par soustraction cet indicateur fournit le taux de disponibilité qui est généralement utiliser pour qualifier la fiabilité d'un équipement ou d'un service.

Pour en faire bon usage et prendre les décisions adéquates, il convient de décliner cet indicateur par type de panne, par opérateur, et par territoire.

On peut nourrir ou compléter cet indicateur avec des métriques plus opérationnelles et usuelles à l'échelle des réseaux ou de leurs éléments constitutifs, que sont le taux de pannes, le temps moyen de bon fonctionnement (MTBF) et le temps moyen de réparation (MTTR).

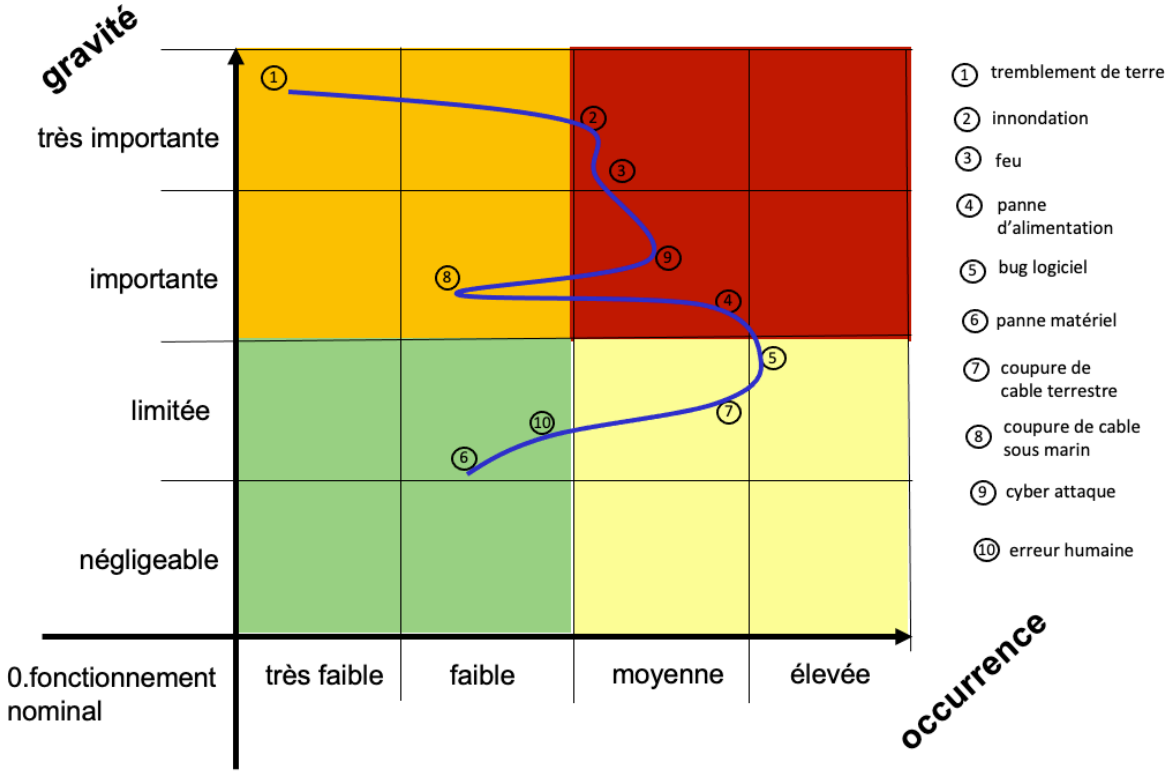
On peut également s'intéresser à l'impact économique des défaillances qui peut constituer également un bon indicateur, mais dont l'estimation est plus complexe et sujet à controverses selon que l'on considère seulement les impacts économiques directes ou également les impacts économiques indirectes.

Il faut par ailleurs, porter une attention particulière à certains éléments qui jouent un rôle essentiels dans les infrastructures numériques, et dont le dysfonctionnement induit potentiellement des conséquences graves, par exemple les points d'échange internet (IPX) ou les câbles sous-marins.

Enfin, on doit chercher à traiter spécifiquement les réseaux de communication utilisés par les services de secours (Public Protection and Disaster Relief – PPDR) pour lesquels le niveau d'exigence en matière de fiabilité, de disponibilité et de résilience se doit d'être le plus élevé possible.

**Cartographie des risques**

Armés de ces métriques, et de leur analyse, il est possible de cartographier les risques et d'y porter la courbe de résilience comme ceci :




**Important** : ce graphique est donné pour exemple, et l'évaluation des risques qui y figure n'est qu'une évaluation grossière à partir de quelques données très partielles. L'objectif ensuite, par des actions ciblées, est de faire glisser la courbe vers la gauche.

## Les défaillances organisationnelles

Elles forment une catégorie particulière de cause de faible résilience: ce peut être des problèmes de mauvaise coordination entre intervenants, des problèmes de dilution des responsabilités ou plus basiquement une absence de plan de continuité d'activité (PCA) et de Plan de Reprise d'Activité (PRA). Elles ne sont pas à la source des pannes mais jouent un rôle sur leur durée, et sur la capacité à la réduire. Elles sont généralement identifiées à travers des Rex (retours d'expérience) sur évènements.

La dilution des responsabilités entre les acteurs est l'un des problèmes qui se pose en France à la suite de la mise en œuvre du Plan France très Haut Débit. En effet, celui-ci est fondé sur deux niveaux de densité de population, les zones très denses et les zones moins denses, et trois niveaux de responsabilité, les collectivités locales, les opérateurs d'infrastructures et les opérateurs commerciaux, ce qui a pour effet d'atomiser les responsabilités.

C'est exactement ce que L'Agence National de la Cohésion des Territoires (ANCT) pointe du doigt dans son guide méthodologique pour l'élaboration d'un schéma local de résilience des infrastructures numériques (Aout 2023) :

« Celles-ci (les dispositions régaliennes), pensées pour les crises majeures et les opérateurs les plus puissants, ne tiennent pas compte de la diversité des territoires et des acteurs. Dans ce cadre, la responsabilité de chacun des acteurs demeure floue et diluée. »

On ne saurait mieux dire, sauf à préciser l'ampleur du problème, puisque nous avons désormais en France pas moins de 220 opérateurs d'infrastructure en fibre optique différents sur le terrain !

Le réseau fixe d'accès à l'internet génère aujourd'hui des pannes longues même en service nominal, c'est-à-dire en dehors des pannes induites par des évènements naturels ou d'actions malveillantes. Selon une enquête réalisée en 2024 pour le compte du régulateur, 33% des abonnés fixe déclarent avoir rencontré au moins un problème de qualité de service au cours des 12 derniers mois, dont 19% une panne totale, et 59% de ceux qui déclarent être toujours en panne le sont depuis plus d'un mois et 23% depuis plus de 6 mois.

Cela concerne tous les abonnés fixe, ADSL et fibre, mais les témoignages reçus à l'AFUTT ne laissent guère de doute sur le fait que les principaux problèmes sur le fixe proviennent très majoritairement des abonnés fibre, et apparaissent en raison de défauts de coordination et de coopération entre opérateurs d'infrastructure et opérateur commerciaux[2].

## Interdépendance télécoms / électricité

Les pannes télécoms dues aux coupures d'alimentation électrique sont nombreuses, en particulier en cas d'évènements naturels (50% des pannes selon une étude américaine)

Sur ce sujet, il faut distinguer les pannes :

- Sur l'installation privative, peu de clients sont équipés d'onduleurs
- Sur les équipements opérateurs : tous les équipements ne sont pas équipés de systèmes de secours.

Le réseau électrique de son côté dépend de plus en plus de la haute disponibilité des réseaux de télécommunication**.** Avec l'extension des solutions de réseaux intelligents au niveau le plus bas, c'est-à-dire le réseau de distribution au client, la dépendance des deux infrastructures augmente considérablement, même si des initiatives sont en cours, par exemple pour assurer l'indépendance de la supervision des équipements de RTE

À la recherche de marges sur un marché très concurrentiel, les opérateurs du secteur des télécommunications ont limité l'installation de batteries de secours et de générateurs diesel sur leur nouveaux réseaux mobile et fibre optique. Ces batteries et groupes électrogènes assuraient il y a encore quelques années la continuité de service en cas de défaillance du réseau électrique. On notera au passage qu'à l'époque des réseaux téléphoniques analogiques (sur prise en T) le secours alimentait également l'équipement du client final.

L'AFUTT invite les pouvoirs publiques à se pencher sur cette question et à fixer des durées minimale de continuité de service des équipements actifs des réseaux avec du matériel de secours électrique, comme l'a fait le régulateur anglais.

[2] Voir notre observatoire des plaintes 2025

## Résilience et règlementation

**L'Article L35-5** du CPCE fixe globalement aux acteurs du secteur des obligations de **service public** qui doivent être assurées dans le respect des principes d'égalité**, de continuité** et d'adaptabilité. Il précise :

*« qu'en vue de garantir la permanence, la qualité et la disponibilité des réseaux et du service, l'entretien des réseaux assurant des services fixes de communications électroniques ouverts au public et de leurs abords est d'utilité publique »*

**Article D98-4** du CPCE ainsi rédigé : « *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 œuvre les protections et redondances nécessaires pour garantir une qualité et une disponibilité de service satisfaisantes* »

A noter que les dispositions de l'article D98-4 s'applique indistinctement aux exploitants de réseaux fixes comme de réseaux mobiles, tandis que l'article L35 ne s'applique qu'aux réseaux fixes sauf dans le cas d'une box 4G/5G faisant fonction de service fixe.

**SAIV (Sécurité des Activités d'Importance Vitale)**: Cette instruction générale interministérielle de 2006 révisée en 2013 fait figurer les télécommunications parmi les 12 secteurs d'importance vitale.

**La directive CER (Critical Entities Resilience)**: Cette directive européenne de 2022 vise à réduire les vulnérabilités et renforcer la résilience physique des entités critiques dans l'Union européenne (UE) afin d'assurer la prestation sans entrave de **services essentiels** à l'économie et à la société dans son ensemble. Elle incite à accroître la résilience des entités critiques qui fournissent ces services.

Si des faiblesses sont manifestes aujourd'hui en France en matière de résilience des réseaux de télécommunications, ce n'est donc **pas par défaut d'encadrement législatif.**

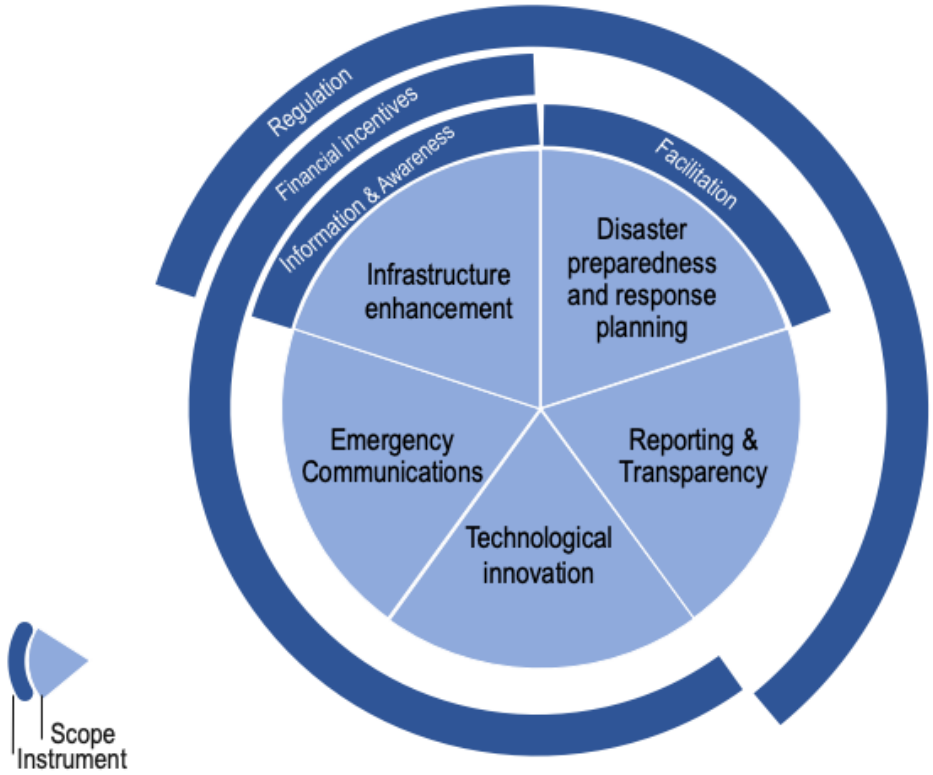
Si le recours à la loi n'est pas nécessaire en revanche l'implication des pouvoir publics reste insuffisante à ce jour en France, en particulier il est indispensable d'œuvrer au développement d'une métrique commune de mesure de la résilience des infras numériques telle que vu précédemment.

Plus largement l'OCDE dans son papier n°374 de 2025, préconise d'agir dans cinq domaines avec quatre leviers :

Les cinq domaines sont: le reporting, l'aider à la sécurisation des infrastructures, le soutien à l'innovation, le développement des moyens de secours, l'anticipation et la planification.

Les quatre leviers sont: la régulation, le financement, l'information, la facilitation.

**. Categorisation framework of policy measures for network resilience**




Source papier 374 de l'OCDE

## Redondance et diversité

La résilience des réseaux de communication reposent principalement sur les principes de redondance et de diversité. La redondance garantit que les composants critiques, tels que les commutateurs et les liaisons de communication, disposent de systèmes ou voies de secours prêts à prendre le relais en cas de panne. Dans le même esprit, il faut ajouter des mesures de secours en alimentation électrique, comme vu précédemment. La diversité, quant à elle, réduit le risque de pannes grâce à l'utilisation de différents fournisseurs et technologies, et par conséquent concerne plus particulièrement les stratégies de résilience du côté des utilisateurs finaux, ou les offres commerciales des opérateurs pour les entreprises qui peuvent intégrer nativement un « package » double abonnement fixe et mobile avec basculement automatique en cas de panne du lien fixe.

A cet égard, il est important de noter que les solutions de diversification de cheminement des communications proposées par les réseaux hertziens se sont considérablement développées au cours des dernières années.

Aujourd'hui il est possible de secourir un réseau filaire avec un abonnement sur réseau mobile et/ou sur réseau satellitaire. Ceci à des prix abordables et des niveaux de performances, sans doute un peu inférieurs à ceux de la fibre, mais très confortables tout de même pour la plupart des usages résidentiels comme professionnels. Toutefois la sécurisation de services fixes par

des moyens 4G ou 5G, suppose une couverture indoor (pénétration des ondes des réseaux mobile dans les bâtiments) ce qui est loin d'être garanti partout et pour tous.

A cela s'ajoute une redondance fonctionnelle qui existe également dans le sens mobile vers fixe, grâce à la communication des smartphones sur box fixe à travers le WiFi, en data et en communication vocale (VoWiFi). Cette fonctionnalité contribue elle aussi à augmenter la résilience globale des communications électroniques.

Les réseaux par satellite, de leur côté offrent une résilience théorique intéressante en situation de catastrophe naturelle notamment, comme on a pu le voir déjà à plusieurs reprises dans le monde. Toutefois il faut garder à l'esprit que la capacité d'écoulement du trafic diminue en cas de nombreuses connexions simultanées sous un même satellite, que les taux contractuels de disponibilité sont faibles (95%) et les dysfonctionnements en cas de forte pluie sont nombreux.

En matière de redondance sur le réseau fibre, l'AFUTT signale un point souvent négligé concernant l'architecture de cette infrastructure, à savoir une certaine faiblesse sur le réseau de collecte. En effet, si dans les grandes villes les réseaux d'interconnexion des points de présence (NRO, points hauts) sont souvent diversifiés, ce n'est pas le cas dans les zones rurales. Les réseaux optiques de collecte, sont le plus souvent uniques et desservent l'ensemble des moyens télécom donc aussi les points hauts mobiles. Ces infrastructures de collecte, n'ont pas été mise à niveau lors des déploiements FttH, au prétexte qu'existaient des offres de type LFO. Or ces offres correspondent à des câbles souvent uniques et disposés en étoile, ce qui interdit des architectures bouclées et donc résilientes. Ces fibres étant utilisées par l'ensemble des opérateurs, rendent vain le recours à une sécurisation multi-opérateurs par les clients entreprise de type SDWAN.

## Sécurisation des infrastructures physiques

les infrastructures physiques dans lesquelles ou sur lesquelles se trouvent les équipements de télécommunications, doivent être correctement protégé et sécurisé.

Nous pouvons évoquer ici la faiblesse des systèmes de fermeture des armoires des NRO et des PBO qui laissent trop souvent ces équipements ouverts et donc offerts à la dégradation ou aux intempéries.

L'accès aux sites critiques doit être anticipé et planifié en cas de crise majeur, pour faciliter le dépannage par les équipes d'intervention.

Parmi les solutions évoquées pour sécuriser les infrastructures en réseau de type électrique ou de communication, on entend souvent la préconisation d'enfouissement des câbles. Néanmoins, lutter tout à fois contre les grands feux et les inondations n'est pas simple, et l'alternative enfouissement versus appuis aériens mérite d'être posée et évaluée.

## Nouvelles technologies : promesses ou nouveaux risques ?

Les récents développements en matière de transformation logicielle des réseaux, également appelée « cloudification », offrent des possibilités d'amélioration de leur résilience. Le réseau défini par logiciel (SDN), en utilisant des contrôleurs logiciels ou des interfaces de programmation d'applications (API) pour acheminer le trafic sur un réseau, permettent une reconfiguration dynamique afin d'utiliser des ressources alternatives en cas de panne.

Le slicing (découpage) réseau permet la création de segments logiques hautement fiables dans les réseaux mobiles. Cela peut prendre en charge, par exemple, le déploiement de réseaux de protection publique et de secours en cas de catastrophe (PPDR) en superposition aux réseaux mobiles commerciaux, permettant ainsi de bénéficier des avancées technologiques mobiles tout en conservant la haute disponibilité et l'isolation requises par les communications d'urgence.

Toutefois, dans le même temps, l'inflation du nombre de lignes de code dans les réseaux peut conduire à une augmentation des pannes logicielles, y compris lors de la mise en place de nouvelles fonctionnalités ou correctifs, comme signalé précédemment.

Notons que les équipements informatiques ne sont généralement pas dans des sites « durcis » ce qui les rend vulnérables aux phénomènes des ondes radioélectriques : phénomènes de vents solaires, explosions nucléaires en altitude, …

Du bon côté des choses, l'intelligence artificielle peut aider à prévenir les pannes ou à évaluer les vulnérabilités.

## Conclusions :

Les recommandations de l'AFUTT sont les suivantes :

1. Développer les métriques de mesure de la résilience

Les indicateurs de résilience des réseaux sont essentiels pour permettre aux régulateurs et aux décideurs politiques de surveiller, d'évaluer et d'améliorer la résilience des réseaux. Ils facilitent l'identification des vulnérabilités et l'évaluation de l'efficacité des mesures prises.

L'AFUTT invite le régulateur à définir un ensemble commun d'indicateurs de la résilience des réseaux et à s'assurer de leur production par les acteurs de la filière. A minima, nous pensons qu'il faudrait disposer du nombre d'heures de service perdue par les utilisateurs qui est parmi les plus pertinents, car il rend compte tout à la fois de l'expérience utilisateur et de la gravité des défaillances. Il faut porter une attention particulière à la durée des pannes et pas seulement à leur fréquence. L'AFUTT constate malheureusement que ce type d'information n'est aujourd'hui pas correctement sourcé.

2. Prévoir un secours électrique pour les principaux équipements actifs des réseaux

L'AFUTT incite les pouvoirs publics à lancer une concertation avec toutes les parties prenantes sur les dispositifs de secours électrique à mettre en place sur les nœuds optiques et sur les

relais mobiles pour garantir un minimum de temps de continuité de service, en cas de rupture d'alimentation.

3. Informer les utilisateurs sur les solutions de secours de connectivité

L'AFUTT estime que les pouvoirs publics doivent inciter les utilisateurs finaux, en particulier les entreprises, à mettre en place une solutions de secours en cas de panne de liaison. C'est aujourd'hui plus simple et moins onéreux que par le passé. Il faut également mieux informer les utilisateurs sur la possibilité de secourir l'absence de réseau mobile par le wifi sur réseau fixe, y compris pour la voix et les SMS, ce qu'ils sont encore trop nombreux à ignorer et à savoir paramétrer dans leur smartphone.

4. Définir un territoire connecté, comme parfaitement couvert en fibre et en mobile.

L'AFUTT définit un territoire connecté comme un territoire ou chaque utilisateur peut disposer d'un accès mobile et fixe de qualité. Comme vu dans ce document la redondance entre réseau fixe et réseau hertzien, dans les deux sens, est un élément puissant de résilience. Encore faut-il que la couverture des réseaux mobile soit correcte, y compris en indoor. A l'évidence, en 2025, le statut de zone fibrée est dépassé, et devrait donc être remplacé par celui de territoire connecté.

5. Étudier la résilience des réseaux de collecte

L'AFUTT demande à ce que les NRO et points hauts desservis par une seule collecte optique soient identifiés, et qu'ensuite soient étudiées les mesures à apporter.

6. Faire appliquer la loi

L'AFUTT constate que les dispositions réglementaires régaliennes existent, elles sont nombreuses et sans ambiguïté sur l'objectif de continuité de service imposé aux opérateurs, mais qu'elles ne sont que très partiellement appliquées. Lorsque des décrets d'application apparaissent nécessaires pour préciser leur mise en œuvre, l'occasion doit être saisie pour établir une large concertation sur le sujet et ainsi impliquer et mobiliser l'ensemble des parties prenantes.

7. Mettre en place ou améliorer les plans de résilience

A partir des éléments de causes et d'impacts étudiés sérieusement comme stipulé au point 1, il faut établir des plans de type PCA (plan de continuité d'activité) et PRA (plan de reprise d'activité), ou chercher à les améliorer autant que possible lorsqu'ils existent.