BANQUE des TERRITOIRES | Caisse des Dépôts GROUPE

# Elaborer son schéma local de résilience

## Guide méthodologique

**Aout 2023**
version 1

# ÉDITORIAL

*À l'heure où le comité d'évaluation du Plan France Très Haut Débit parle de « réussite » , où l'objectif de très haut débit pour toutes et tous a été atteint, où 80% des locaux du territoire national ont été couverts en fibre optique, et où l'appétence des usagers pour la fibre est sans cesse confirmée (plus de 22 millions d'abonnements au 31 mars 2023), la généralisation de la fibre optique pour l'ensemble de nos concitoyens constitue l'un des prochains grands défis auquel la France doit répondre. Le déploiement en un temps record de ces nouveaux réseaux ne doit pas nous faire perdre conscience de la nécessité de leur permanence en matière de service, en d'autres termes de leur capacité à surmonter un évènement et à rétablir rapidement un fonctionnement normal.*

*Dans un contexte de crises climatiques ou pandémiques sans précédent, la capacité à prévenir et à gérer les risques apparaît absolument fondamentale pour l'avenir de ces réseaux. En effet, répondre aux attentes légitimes des usagers en matière de continuité de service est essentiel dans un monde toujours plus interconnecté. Les aléas climatiques, actes de malveillance, ou encore les accidents de travaux, représentent autant de risques pour les réseaux et appellent ainsi à une réponse opérationnelle et organisationnelle collective visant à identifier les bons acteurs à mobiliser en cas de crise pour pouvoir assurer à minima un mode de fonctionnement en environnement dégradé et garantir le retour à un service normal le plus rapidement possible.*

*L'Agence nationale de la cohésion des territoires (ANCT) s'est engagée dans un cycle d'échanges avec les acteurs de l'écosystème pour appréhender la vision de chacun sur la résilience. Nous sommes désormais convaincus du rôle de sensibilisation et de pédagogie que nous avons à jouer auprès de nos interlocuteurs au quotidien. Des actions en la matière seront engagées pour vous accompagner au mieux, porteurs de projets de RIP, dans cet exercice de diagnostic, de prévention et de gestion de crise pour des réseaux toujours plus résilients.*

*Le guide que vous tenez entre les mains s'adresse aux collectivités porteuses de projets d'aménagements numériques et aux préfectures. En exposant des informations essentielles pour travailler à l'identification des risques propres des territoires et définir les réponses les plus appropriées, ce guide constitue une brique indispensable dans l'élaboration de schémas locaux de résilience.*

**Zacharia Alahyane**

*Directeur des programmes France Mobile et France Très Haut Débit à l'ANCT*

*Les évènements climatiques récents en France (tempête Alex, ouragan Irma…) et dans le monde constituent des illustrations concrètes du dérèglement climatique. Si les efforts pour maintenir le réchauffement en dessous du seuil des 2°C sont évidemment essentiels pour contrôler l'évolution des aléas, il est désormais primordial de limiter les impacts sur nos territoires en développant une véritable culture de l'adaptation préventive et de l'anticipation de notre résilience. L'évolution du cadre réglementaire (révision du Plan national d'adaptation a u changement climatique pour s'adapter à +4°C, loi "Climat et Résilience", fonds d'accompagnement à la transition écologique des territoires) reflète la prise de conscience par les pouvoirs publics de l'existence d'une complémentarité entre ces approches d' "atténuation" et d'"adaptation".*

*Aujourd'hui véhicules de toutes les données essentielles de notre vie sociale, économique et démocratique, les infrastructures numériques seront demain amenées à jouer un rôle encore plus significatif. Leurs capacités d'adaptation et de résilience doivent donc être une priorité : il est ainsi nécessaire de passer à l'action au plus vite avant que les compétences, les matériels et les équipements de la phase de construction des réseaux ne soient plus autant disponibles. Dans ce cadre, la réalisation de schémas locaux permettra de connaître les risques, d'identifier les mesures à mettre en place, de hiérarchiser les solutions d'investissements et constituera la première étape du chemin menant à la résilience des réseaux. Plus largement, ces schémas permettront de nourrir les réflexions des acteurs industriels et institutionnels au niveau national.*

*La Banque des Territoires est pleinement consciente de l'ampleur de la tâche à accomplir d'autant plus que d'autres grands enjeux mobilisent encore la filière. C'est pour cela que les "schémas locaux de résilience" seront éligibles aux fonds engagés dans le cadre de notre Plan d'adaptation au changement climatique.*

*Ce guide a pour ambition d'accompagner les différents acteurs dans la réalisation des schéma locaux de résilience en suggérant des pistes de réflexion, en présentant le cadre réglementaire en vigueur et en détaillant les responsabilités de chacun. Au-delà des investissements lourds potentiels (enfouissements, sécurisations, déplacements etc…), de nombreuses mesures organisationnelles, moins onéreuses tout en étant efficaces, doivent être explorées pour favoriser l'adaptation des infrastructures numériques aux risques.*

**Antoine Darodes**

*Directeur du département Transition Numérique de la Banque des Territoires*

# SOMMAIRE

# SYNTHESE DE DIRECTION

Le plan « France Très Haut Débit » lancé en 2013 s'est donné l'objectif ambitieux de procurer à l'ensemble des territoires une connexion très haut débit (>30Mbit/s) en 2022. Si ce plan est généralement considéré comme un large succès, il s'est concentré sur un objectif d'efficacité du déploiement. Or, les infrastructures fibres sont exposées à divers risques (climatiques, technologiques, cyber, malveillance). L'étude « Résilience des réseaux FttH » récemment menée par Infranum en partenariat avec la Banque des Territoires[1] suggère que la fragilité des infrastructures aériennes au risque climatique demeure la principale vulnérabilité des réseaux fibres. Selon cette même étude, il existe en France 500 000 km de réseaux aériens dont 10% sont des réseaux de distribution intra-bourgs déployés en forêt. Ce guide insistera donc sur les risques climatiques.

Alors qu'Infranum met également en évidence les risques liés aux accidents de la route et aux actes de malveillance, il est aussi nécessaire de considérer les interdépendances avec le réseau électrique et notamment les dangers provenant des politiques de délestage. A cet égard, les opérateurs télécoms entretiennent des équipements de secours électrique pour permettre une continuité de service en cas de délestage. Toutefois, l'état des batteries et les aléas des bascules et redémarrages poseraient de sérieux problèmes si les délestages devenaient fréquents et massifs. Il faut ainsi permettre une meilleure insertion des réseaux de télécoms dans les paliers de priorisation en cas de délestage décidés par les différentes préfectures. Par ailleurs, d'autres pistes qui permettraient de tenir compte des nœuds de réseau de télécoms dans les délestages sont également à l'étude.

Cette vulnérabilité intrinsèque du réseau fibre est d'autant plus importante qu'elle fait face à une augmentation des risques à la fois climatiques et organisationnels :

- En ce qui concerne les risques climatiques, les évènements climatiques qui ont frappé la France mais également le reste du monde récemment témoignent d'un accroissement des risques climatiques. Le 6ème rapport du GIEC[2] alerte encore une fois sur l'aggravation exponentielle des risques climatiques d'autant plus que, peu importe les efforts opérés, le niveau de réchauffement global de 1,5°C serait atteint dès les années 2030.
- Concernant les risques organisationnels, les changements importants intervenus ces dernières années à la fois dans l'écosystème des opérateurs télécoms (dégroupage, réseaux d'initiative publique, etc…) que dans l'organisation des compétences des collectivités territoriales (loi MAPTAM, loi NOTRe, etc.) ont complexifié la répartition des responsabilités dans la gestion de crise. Cette difficulté des différents acteurs à identifier leur responsabilité a été pointée du doigt par les acteurs ayant fait face à des crises.

[1] Etude Infranum x Banque des Territoires : https://infranum.fr/etude-infrastructures-numer/
[2] 1er volet du 6ème rapport : https://www.unep.org/fr/resources/rapport/sixieme-rapport-devaluation-du-giec-changement-climatique-2022

La vulnérabilité des réseaux fibres doit également s'étudier au regard des différentes alternatives disponibles en cas de rupture du service. Ce sont particulièrement les entreprises et les principaux services publics, les sites dont le fonctionnement est très affecté par les indisponibilités qui doivent disposer de solutions de secours (4G ou 5G, satellite, double adduction fibre, liaisons de secours en faisceau hertzien…) leur permettant de basculer en cas de problèmes, éventuellement en mode dégradé pour prioriser les flux. Les alternatives sont particulièrement ciblées sur des usages spécifiques et certains usagers finaux doivent contribuer à leur propre résilience :

- Dans une certaine mesure, le réseau mobile peut prendre le relai en cas de pannes du réseau fixe pour les usagers. Toutefois, il en est tout autrement en cas de crise générale (multiréseaux) touchant massivement les usagers. En effet, outre le fait que la capacité d'absorption par le mobile des flux réorientés est limitée, que la collecte d'une partie des sites mobiles peut être assurée par les réseaux fibres, il existe une part non nulle (5%) des ménages qui n'ont pas de téléphone mobile et dont le téléphone fixe est le seul moyen de contacter les urgences. Par ailleurs, malgré le fait que le rétablissement des réseaux mobiles sera prioritaire par rapport au fixe en situation de crise (ne serait-ce que pour les services qu'ils rendent en mobilité), les réseaux mobiles seront de plus en plus dépendants des réseaux en fibre optique pour la collecte, et non l'inverse. En ayant connaissance de ces limites, le gouvernement a décidé de mettre en place, à partir de 2024, un réseau radio du futur (RRF). Avec ce dernier, la France va se doter d'un réseau de communication très haut débit (4G puis 5G) commun à l'ensemble des acteurs de la sécurité et du secours, leur permettant de communiquer instantanément les uns avec les autres.
- La guerre en Ukraine a accéléré les prises de décisions à l'échelle européenne pour le lancement d'une constellation de satellites en orbite basse (IRIS 2) dont les premiers satellites sont attendus pour 2024. Toutefois, ces applications seront centrées sur des utilisations gouvernementales pour des communications cryptées.

Les vulnérabilités du réseau ne sont pour l'instant pas prises en compte par les différents acteurs. Des dispositions régaliennes nationales (Code des Postes et des Communications Electroniques, Code de la Sécurité Intérieure, décisions ARCEP…) fixent des obligations de continuité de services aux opérateurs de réseaux de communication électronique. Celles-ci, 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 dilluée. Ces textes pointent tout de même vers une responsabilité de l'Opérateur d'Infrastructures. Toutefois, cette dernière n'est en réalité jamais appliquée : les évènements climatiques étant considérés comme des cas de force majeur, ces derniers exemptent souvent les Opérateurs d'Infrastructures d'une obligation de résultat en particulier pour les opérations de maintenance préventive et pour l'obligation de rétablissement de la continuité du réseau dans des délais impartis. Par ailleurs, de nombreuses obligations de résultats ne sont pas passibles de sanctions.

Des initiatives récentes tentent de trouver une solution à ce problème en avançant un rôle significatif du préfet qui peut tenir compte des particularités locales et apprécier la criticité des situations de crises. Le préfet peut ainsi décider de l'insertion des réseaux fibres dans le dispositif ORSEC en attendant qu'une instruction ministérielle systématise la démarche. Par ailleurs, la loi « Climat et Résilience » précisée par décret en 2022 donne la possibilité au préfet (dans la plupart des cas) de prescrire par arrêté à tout exploitant de réseau, après avis de l'autorité qui a délégué le service, la fourniture :

- D'un diagnostic de vulnérabilité, comprenant une cartographie des points de vulnérabilité du réseau et les zones potentiellement impactées
- D'un programme des investissements prioritaires détaillant les travaux nécessaires pour améliorer la résilience du réseau et réduire les zones potentiellement impactées.

Pour autant, le fait qu'aucun arrêté préfectoral basé sur ce dispositif législatif et concernant un réseau fibre n'a été pris à ce jour montre que ces problématiques nouvelles doivent être endossées dans les territoires.

L'ARCEP reconnait les limites des dispositifs mis en place jusqu'à présent et la nécessité d'action : « L'Arcep appelle de ses vœux la montée en puissance des mécanismes de surveillance et de gestion des risques, notamment au regard de la multiplicité d'acteurs impliqués dans le déploiement des boucles locales en fibre optique. L'Arcep est prête à travailler avec les services compétents de l'État pour participer à une démarche de structuration et formaliser les besoins liés aux enjeux de résilience des réseaux de communications électroniques ». A cet égard, le cadre réglementaire est sûrement voué à évoluer d'autant plus que le COVID-19 a joué un électrochoc et a sensibilisé les pouvoirs publics à la nécessité de mener une stratégie de résilience. Ainsi, différentes options sont à l'étude au niveau national. La mise en place effective d'un Fonds d'Aménagement Numérique du Territoire dont l'une des priorités serait de contribuer à l'augmentation de la résilience des réseaux est notamment suggéré par l'AVICCA, Infranum et la FNCCR.

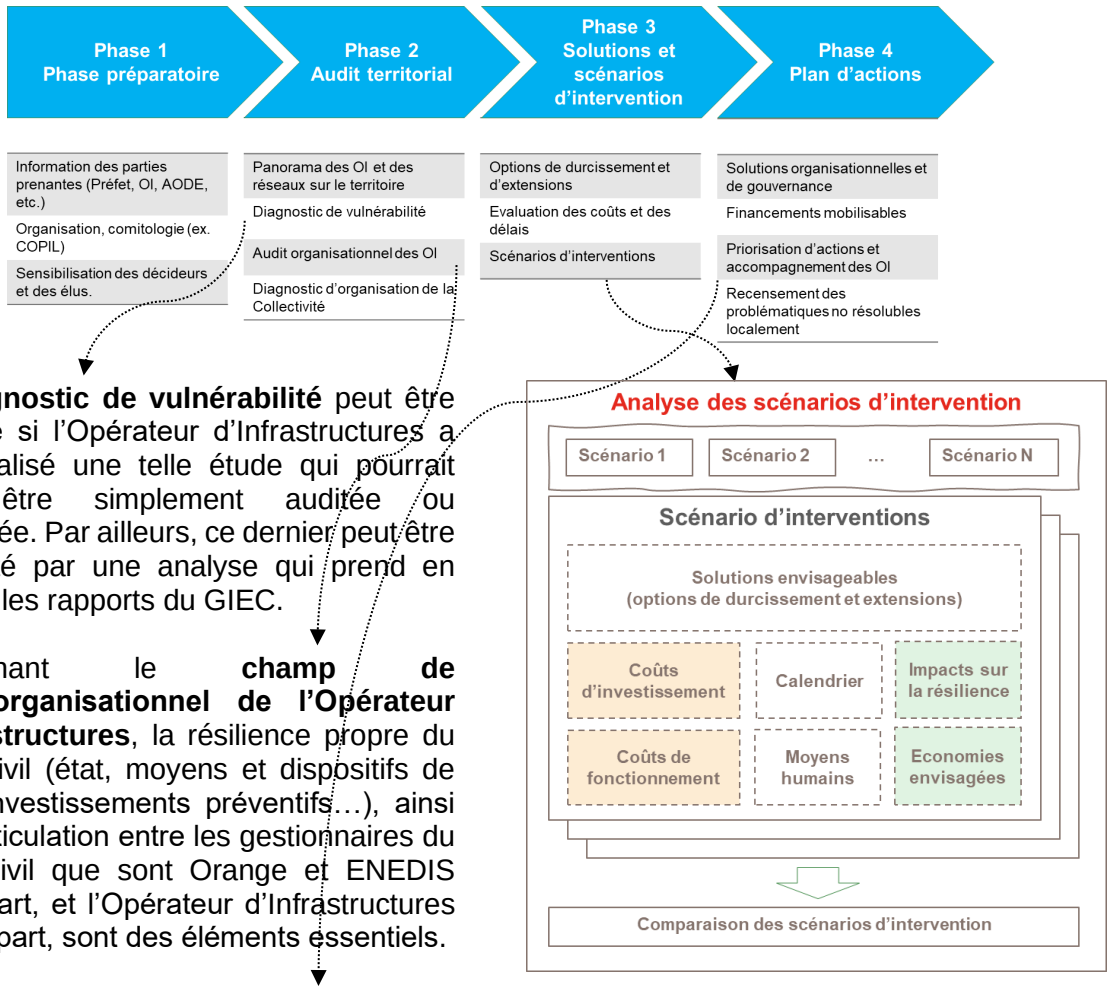
Pour autant, il ne serait pas judicieux d'attendre que le pouvoir réglementaire s'occupe de prendre en main ces sujets. Il est nécessaire d'initier un plan d'action au niveau local. En effet, les instances multilatérales réunissant les différents acteurs de la filière, contribuant activement à une « soft law » et permettant des avancées consensuelles, butent parfois sur l'absence de volonté de certains acteurs. Ainsi, la réalisation de schémas locaux permettra de favoriser l'émergence d'un consensus, de mobiliser la filière, de nourrir une réflexion au niveau national et de potentiellement permettre la mise en place d'une péréquation prenant compte la diversité des vulnérabilités des différents territoires.

Il existe donc une nécessité de réaliser des schémas locaux de résilience au plus vite. Ces derniers permettront d'identifier les risques pesant sur les infrastructures numériques pour ensuite passer à l'action. Il existe différents axes d'intervention :

- Une nécessité d'investissement :
    - Pour les anciens réseaux : limiter l'exposition aux risques et investir tant que les compétences de déploiement de réseaux sont encore disponibles
    - Pour les nouveaux réseaux : chaque fois que nécessaire, les adapter dès leur construction (en enfouissant directement les câbles par ex.) pour limiter l'inflation des coûts.
- Une nécessité d'organiser les compétences : à faible coûts, cette précision des responsabilités de chacun peut se révéler très efficace pour limiter les risques.
    - Sensibilisation des différents acteurs à leur rôle respectif
    - Insertion systématique de l'ensemble des réseaux fibres dans le cadre du dispositif ORSEC
    - Réforme de certains dispositifs juridiques : liens entre délégant et délégataire dans le cadre d'une DSP, relations entre l'Opérateur d'Infrastructures et les opérateurs commerciaux cofinanceurs, les liens de l'Opérateur d'Infrastructures d'une part avec Orange Wholesale France au titre de l'offre d'accès au génie civil souterrain et aux appuis de l'opérateur historique et d'autre part avec les Autorités Organisatrices de la Distribution d'Energie et les gestionnaires du réseau de distribution d'électricité (ENEDIS et les distributeurs non nationalisés)
- Une nécessité de réaction : prendre note des évènements passés et s'inspirer des schémas locaux déjà réalisés

La réalisation de « schémas locaux de résilience » par des territoires comme la Haute-Garonne, la Gironde et la Corse montrent que les schémas locaux sont des options considérées par les collectivités. Ces initiatives, pionnières en la matière, doivent être des sources d'inspiration dans la réalisation des futurs schémas. En outre, il est intéressant de se référer aux travaux d'ENEDIS dans lesquels certains éléments méthodologiques déployés pourraient être inspirants pour les télécoms.

Le présent guide a pour objectif d'aider les collectivités territoriales à réaliser leur schéma local de résilience en leur donnant un exemple de méthodologie à appliquer :




Le **diagnostic de vulnérabilité** peut être simplifié si l'Opérateur d'Infrastructures a déjà réalisé une telle étude qui pourrait alors être simplement auditée ou actualisée. Par ailleurs, ce dernier peut être complété par une analyse qui prend en compte les rapports du GIEC.

Concernant le **champ de l'audit organisationnel de l'Opérateur d'Infrastructures**, la résilience propre du génie civil (état, moyens et dispositifs de crise, investissements préventifs…), ainsi que l'articulation entre les gestionnaires du génie civil que sont Orange et ENEDIS d'une part, et l'Opérateur d'Infrastructures d'autre part, sont des éléments essentiels.

Bien que de manière pragmatique, concernant le **plan d'actions** de ces schémas locaux, l'heure apparait davantage aux négociations sur les coûts d'exploitation qu'à la résilience, la priorité doit être donnée à des investissements ciblés sur les parties en amont du réseau et/ou sur les segments les plus accidentés. Dans ce cadre, la hiérarchisation demeure une composante essentielle afin d'adapter ces schémas locaux de résilience aux différents budgets des collectivités.

Par ailleurs, certaines évolutions du cadre juridique sont suggérées dans ce guide et permettront sans doute d'améliorer le fonctionnement de l'écosystème dans son ensemble. Il apparait par exemple essentiel que l'ensemble des réseaux fibres soient systématiquement reconnus comme faisant partie du dispositif ORSEC. Par ailleurs, différents dispositifs juridiques sont mobilisables autant pour responsabiliser l'Opérateur d'Infrastructures d'un RIP que lui donner les moyens d'agir.

# INTRODUCTION

Le terme « résilience » désigne la « 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. »[3].

Le choc affectant l'objet peut être d'une nature très diverse. Pour ce qui est des réseaux de télécommunications, on peut, toutefois, mettre en évidence 3 types d'évènements majeurs mettant le système en péril : les aléas climatiques, les aléas de malveillance et les accidents. Face à ces derniers, il est clair que la résilience concerne à la fois des risques matériels et immatériels, physiques et digitaux.

Pour mener une stratégie de résilience, il est nécessaire de hiérarchiser ces risques pour prioriser les investissements à réaliser. Parmi les 3 types de risques évoqués ci-dessus, les risques climatiques apparaissent comme les plus importants à traiter et à endiguer. Deux raisons nous poussent à traiter spécifiquement ces risques climatiques dans le cadre de ce livre blanc : ces risques sont les plus spécifiques aux territoires et sont les plus importants[4] pour les territoires. Ils sont également voués à s'amplifier fortement dans le futur.

En effet, le 4 juillet 2023, selon l'Agence américaine d'observation océanique et atmosphérique, la Terre a connu le jour le plus chaud jamais enregistré : la température moyenne de la Terre a atteint 17,18°C. Cette statistique est encore un rappel de la responsabilité de l'Homme dans le réchauffement climatique. Le premier volet du 6ème rapport d'évaluation du GIEC[5], publié en août 2021, précise que le réchauffement climatique s'élève d'ores et déjà à 1,1°C. Pour autant, même en considérant le niveau actuel de réchauffement, les effets du réchauffement climatique se sont déjà fait sentir en France en particulier lors de l'été 2022 et ont provoqué une prise de conscience autant chez les décideurs politiques que chez les citoyens. Ils ont révélé la vulnérabilité de nos territoires. Les infrastructures numériques ne font pas exception : les incendies dans le Var ont nécessité la rénovation de 71km de fibre optique. Au-delà du risque financier pour les différents acteurs du numérique, les risques extra-financiers sont nombreux. Cette dépendance de la société dans son ensemble au réseau fibre doit s'apprécier au regard des alternatives qui peuvent se muer en solutions en situation de crise. Ce rapport apportera des conclusions concernant la complémentarité des réseaux mobiles et satellitaires vis-à-vis des réseaux fibres.

---

[3] https://infranum.fr/wp-content/uploads/2022/06/E%CC%81tude-re%CC%81silience-nume%CC%81rique.pdf

[4] Etude « Infrastructures Numériques : Essentielles C'est Une Évidence, Résilientes C'est Une Exigence » (https://infranum.fr/etude-infrastructures-numer/)

[5] 1er volet du 6ème rapport : https://www.unep.org/fr/resources/rapport/sixieme-rapport-devaluation-du-giec-changement-climatique-2022

Cette prise de conscience des risques actuels doit par ailleurs s'accompagner d'une prise de conscience des aléas futurs. Le rapport du GIEC alerte encore une fois sur l'aggravation exponentielle des aléas climatiques d'autant plus que, peu importe les efforts opérés, le niveau de réchauffement global de 1,5°C sera atteint dès les années 2030. Cette montée des risques sera concomitante de l'accroissement des vulnérabilités : de nombreuses initiatives de transformation numérique de secteurs sensibles comme la santé (à travers la télémédecine) augmenteront les risques liés à une rupture du service.

**1/ Guider les acteurs dans la réalisation d'un « schéma local de résilience »**

Pour absorber les chocs associés à ces risques, la prise de conscience ne suffit pas et doit s'accompagner d'une évaluation des risques associés.

Une étude pilotée par InfraNum[6] a chiffré le coût des actions permettant d'augmenter significativement la continuité de service des réseaux FttH, à la fois au quotidien et en termes de résilience. Il s'agit notamment de finir de boucler et d'enfouir les réseaux de collecte, déplacer ou réhausser les NRO qui seraient en zones inondables, enfouir les réseaux de transport et les lignes principales du réseau de distribution en aérien, sutout s'ils traversent des zones boisées, protéger les installations contre la malveillance, etc. Tandis que le scénario minimal est estimé à 6,9 milliards d'euros, une ambition forte nécessiterait de dégager 16,9 milliards d'euros. Dans tous les cas, ce sont des chiffres considérables quel que soit le scénario. Toutefois, ces scénarios sont à rapprocher des quarante années de vie de nos réseaux (et même bien au-delà pour le génie civil). Ils ont par ailleurs le mérite de poser le débat au niveau national pour trouver les financements.

De la même manière que pour les autres infrastructures qui composent le territoire national (transport, électricité etc…), cette mesure du risque demeure particulièrement délicate dans la mesure où les infrastructures numériques ont une couverture géographique étendue et des vulnérabilités diverses. Ainsi, au-delà de cette vision macroéconomique utile et pour mesurer les risques dans toute leur complexité, il revient à chaque territoire de mener des études locales, d'identifier des priorités voire des urgences. Ce diagnostic de vulnérabilité doit également être l'occasion pour les élus d'améliorer leur compréhension des infrastructures numériques. En effet, lorsque le terme de résilience est associé au secteur des télécommunications, il fait référence à la fois à la résilience des infrastructures mais aussi à celle du système dans son ensemble (notamment le système organisationnel de réponse au sinistre).

Le schéma local de résilience doit ainsi tâcher de hiérarchiser les vulnérabilités physiques du réseau mais aussi de préciser les modalités d'intervention en temps de crise. Concernant ces dernières, on distingue traditionnellement dans la littérature de la gestion de crise, 4 phases :

---

[6] Etude Infranum - Banque des Territoires : https://infranum.fr/wp-content/uploads/2023/07/Resilience-VF-1.pdf

- La prévention
- La préparation
- L'action
- La réaction

Les crises récentes ont permis de mettre en valeur d'importantes lacunes au niveau organisationnel, qui s'expliquent en grande partie par la jeunesse des infrastructures FttH en France :

- Pour la construction du réseau FttH, il a fallu faire pour l'essentiel avec l'état du génie civil disponible, à la fois pour des raisons financières et de délai. Ainsi, les problématiques que le réseau pourrait connaitre à long-terme n'ont pas été prioritaires dans la construction du réseau.
- La récente émergence du réseau FttH mais aussi l'ouverture à la concurrence des réseaux de télécommunications complexifient les chaines de responsabilités.

**Description du Schéma Local de Résilience**

Un schéma local de résilience (SLR) établi par une collectivité, en concertation avec les acteurs locaux, peut ainsi se donner pour objectif d'accompagner l'Opérateur d'infrastructure fibre afin que sa capacité de résistance aux crises soit en adéquation avec les besoins essentiels du territoire et ses aléas particuliers. Sa réalisation nécessitera un diagnostic territorial précis pour aboutir un plan d'action à court, moyen et long terme. Il aura vocation à être actualisé périodiquement en fonction de l'évolution des aléas et de l'évolution des usages du réseau.

### 2/ Préciser les responsabilités de chacun des acteurs locaux

Ces nouvelles problématiques sont d'autant plus préoccupantes qu'elles s'accumulent sur une organisation déjà complexe :

1. De fortes interdépendances avec d'autres secteurs comme celui de la distribution d'électricité ou encore du transport. Ces dépendances impliquent une nécessaire coordination avec les différents acteurs de ces filières.

2. Une répartition des responsabilités dans la mise en œuvre des politiques de résilience qui demeure floue : L'acteur central de la résilience d'un réseau FttH est l'Opérateur d'infrastructure (OI). Il a en main les outils opérationnels, tant en gestion courante qu'en cas de crise. Il est soumis aux obligations réglementaires générales de la sécurité civile et du cadre légal spécifique des réseaux de communications électroniques. Il arbitre et réalise les investissements préventifs et curatifs, est responsable contractuellement de la continuité du service autant vis-à-vis des utilisateurs du réseau que des opérateurs commerciaux qui sont généralement aussi ses cofinanceurs. Pour autant, l'OI agit dans un cadre contraint au niveau financier, avec ses cofinanceurs, et au niveau organisationnel, avec les gestionnaires du génie

civil sous-jacent. Déjà en 2016, le régulateur reconnaissait la complexité du sujet : « L'Arcep partage l'attention de la Cour en ce qui concerne les enjeux de sécurité et de résilience des réseaux. L'Arcep appelle de ses vœux la montée en puissance des mécanismes de surveillance et de gestion des risques, notamment au regard de la multiplicité d'acteurs impliqués dans le déploiement des boucles locales en fibre optique. L'Arcep est prête à travailler avec les services compétents de l'État pour participer à une démarche de structuration et formaliser les besoins liés aux enjeux de résilience des réseaux de communications électroniques »[7].

### 3/ Identifier les problématiques et inciter à des actions au niveau national

Bien sûr, des dispositions régaliennes nationales fixent des obligations de continuité de services aux opérateurs de réseaux de communication électronique. Pour autant, celles-ci, pensées pour les crises majeures et les opérateurs les plus puissants, ne tiennent évidemment pas compte de la diversité des territoires et des acteurs. Depuis peu, les préfets ont aussi la faculté d'imposer localement des obligations aux opérateurs afin de maintenir la satisfaction des besoins prioritaires de la population en cas de crises ; ce pouvoir n'a cependant jamais été mise en œuvre à ce jour. La pression réglementaire pourrait augmenter à la suite de catastrophes, mais il est bien sûr préférable de prendre les devants.

La réalisation de ces schémas locaux permettra à la filière de se mobiliser mais aussi de justement nourrir la réflexion au niveau national pour potentiellement mettre en place une péréquation prenant compte la diversité des vulnérabilités des différents territoires.

Le présent guide a été rédigé à partir d'entretiens réalisés avec les acteurs impliqués : collectivités, opérateurs d'infrastructure et commerciaux, administration centrale, régulateur, intégrateurs, distributeurs d'électricité, etc. Il a vocation à :

- Guider les collectivités territoriales dans la réalisation de leur « schéma local de résilience »
- Informer les acteurs du territoire et les préfectures sur les différentes responsabilités des acteurs des infrastructures numériques
- Nourrir une réflexion au niveau national en identifiant les freins réglementaires au déploiement de stratégies de résilience

Nul doute que la réalisation des premiers schémas locaux viendra enrichir les réflexions.

---

[7] Réponse à la Cour des Comptes https://www.arcep.fr/fileadmin/reprise/dossiers/fibre/avis-arcep-rapport-cour_des_comptes-310117.pdf

01

# Les risques des territoires

# 1. Panorama des aléas et risques pour le réseau

## 1.1 Rappel des forces et faiblesses des réseaux FttH

Comme pour le cuivre, la hiérarchie du réseau fibre s'impose du centre vers la périphérie pour assurer le service aux usagers, tant au niveau des segments que des locaux, armoires ou boitiers qui abritent les nœuds : liaisons longue distance, points de présence opérateurs (POP) et collecte, Nœuds de raccordement optique (NRO), transport et Points de mutualisation (PM), distribution et Points de branchements optiques (PBO), raccordements des usagers.

### Vulnérabilités intrinsèques du réseau

**Avantages du réseau FttH**

- **Un réseau neuf** dans toutes ses composantes (hors GC), et une architecture qui n'a pas eu à suivre les méandres de l'urbanisation des quarante dernières années
- Des performances permettant de **limiter le nombre de NRO** hébergeant les équipements actifs des opérateurs, par rapport aux NRA
- Un **risque de vol de câble non nul mais atténué** (sans valeur commerciale, mais qui peut être confondu avec un câble cuivre) ;
- Une **sensibilité nettement moindre aux perturbations électromagnétiques et à l'humidité.**

**Inconvénients du réseau FttH**

- Un découpage des zones de responsabilité des différents OI, stabilisé pour l'essentiel, mais compliqué au niveau de chaque département, et une **spécificité des Zones très denses** (un ou plusieurs opérateurs sur le segment de la distribution)
- **Une multiplicité des opérateurs d'infrastructure fibre par rapport à l'OI cuivre**, source d'émulation, mais aussi de complexité pour les interfaçages avec tous les autres acteurs
- Un **montage « en couches »**, avec deux gestionnaires de génie civil principaux, un OI et plusieurs Opérateurs commerciaux qui assurent le SAV de la partie raccordement
- Un **brassage au PM à chaque connexion d'un nouvel abonné** (création de ligne ou churn)
- Une **montée en charge rapide des raccordements, des intervenants en cascade et parfois mal ou pas formés**, ce qui multiplie les risques d'incidents (dont des dégradations), et peut être pénalisant à long terme (malfaçons, erreurs de documentation…)
- Une **dépendance au réseau électrique accrue**, avec la suppression de la télé-alimentation

*NB : Concernant la téléalimentation, cette dernière était déjà un lointain souvenir pour l'accès à internet via les box sur le réseau cuivre, mais était encore un atout pour les postes d'appels dans les Etablissements recevant du public par exemple.*

À noter que les RIP, non par leur nature, mais du fait qu'ils concernent les zones les moins denses du territoire, sont soumis à des aléas plus importants du fait, entre autres, de la part prépondérante du génie civil en aérien, de longueurs moyennes de réseau par prise multipliées et, en proportion, de plus grandes fragilités et distances à parcourir pour les réparations. De plus, les activités importantes peuvent moins facilement bénéficier d'une double adduction via le FttO. Certaines topologies (fonds de vallées par exemple) conduisent à des liaisons de collecte pendulaires non bouclées.

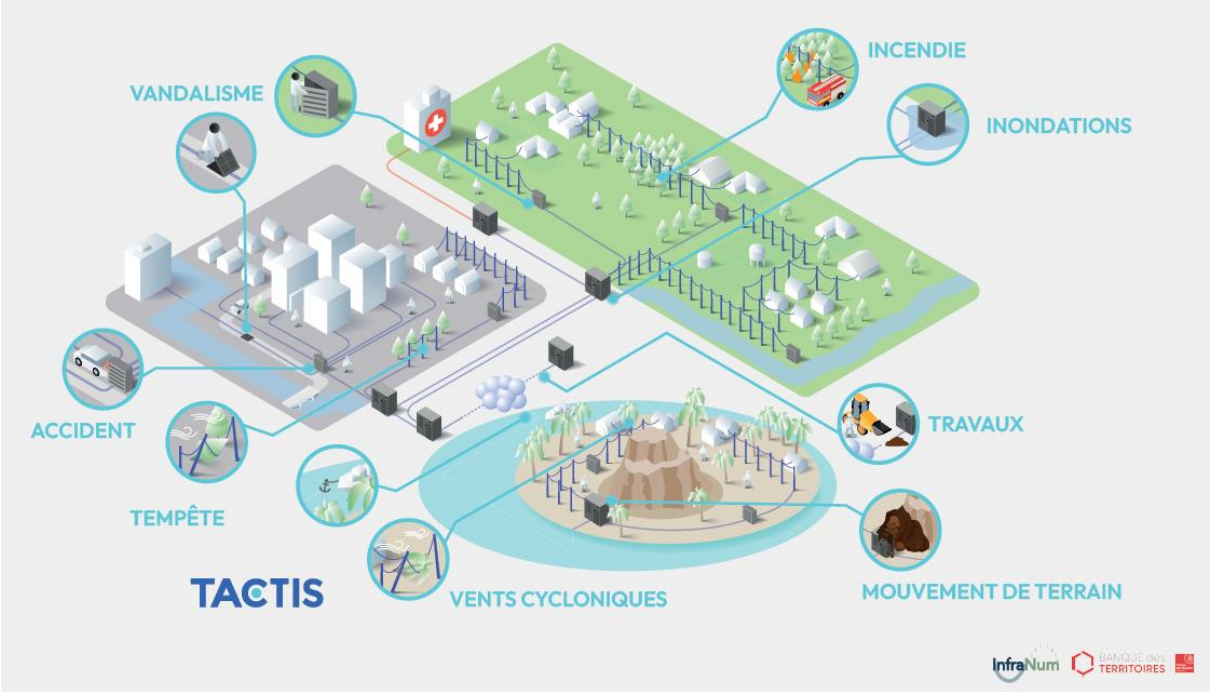
La complexification structurelle des réseaux fixes FttH par rapport au cuivre, et les inégalités de situation doivent être compensées par des mesures complémentaires tant au niveau national qu'au niveau local.

## 1.2 Quels risques pour les territoires ?

***Panorama des risques***

Les aléas peuvent être d'intensité et d'occurrence géographique ou temporelle variables ; ils peuvent porter atteintes à des personnes, à l'environnement ou à des biens. Les enjeux sont fonction des volumes impactés ainsi que de leur nature (vie humaine versus dommage matériel. Leur croisement forme une sorte d'équation avec : risque = aléa x enjeu.

Chaque territoire est différemment impacté par les aléas :




*Exemples d'aléas – Infographie issue de l'étude Infranum-Banque des Territoires sur la résilience des infrastructures numériques*

On distingue plusieurs familles de risques[8] :

- Technologiques
- Actes de malveillance
- Cybersécurité
- Naturels

Concernant les risques technologiques : ils semblent a priori de moindre impact, car les atteintes au réseau seraient probablement localisées.

[8] Cf Etude InfraNum - Banque des territoires : https://infranum.fr/elementor-9771/

Concernant le risque cyber :

1. Les réseaux de communications électroniques ouverts au public sont particulièrement sensibles au risque cyber.
2. Les réseaux d'infrastructure passive, comme le FttH, le sont moins mais n'y échappent pas puisqu'ils ont de nombreux dispositifs informatiques d'interfaçage OI/OC, une documentation sophistiquée, des centres de supervision, des équipements d'activation pour les opérateurs entreprise etc.

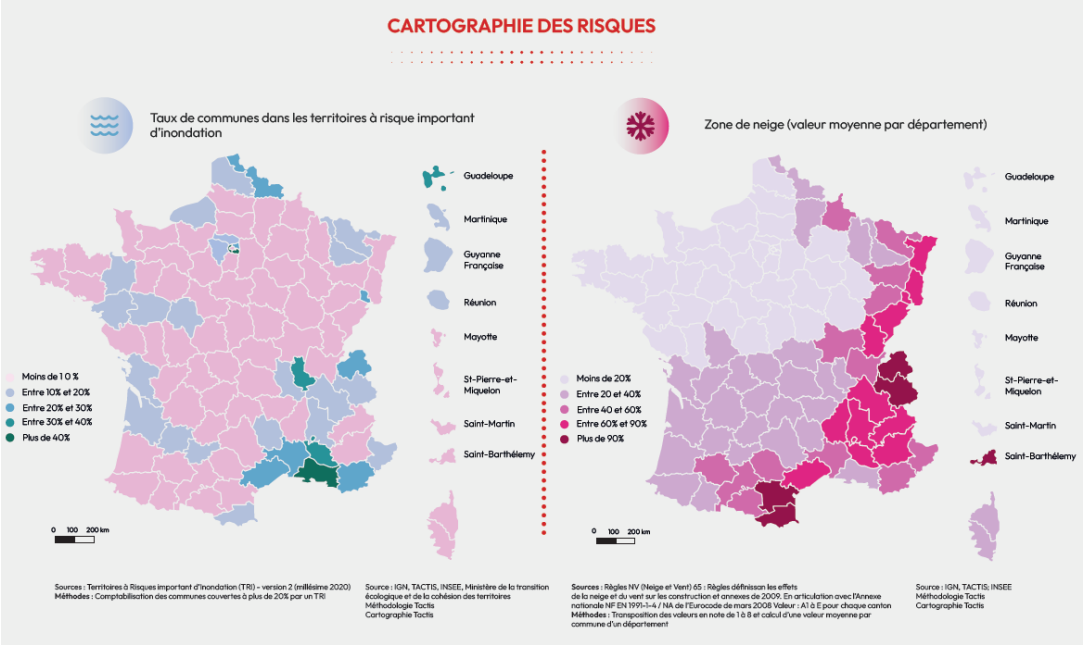
Comme toute infrastructure desservant massivement les territoires, ce sont les aléas naturels qui apparaissent comme les plus importants à traiter, et les plus spécifiques aux différents territoires.

## *Focus sur les risques naturels*

**L'inondation est le risque le plus important en France[9] :**

- 1/3 des communes disposent d'un Plan de prévention des risques naturels avec une dimension « inondation ».
- 1/4 de la population est située dans une enveloppe approchée d'inondation potentielle (EAIP, zone inondable de crue maximale).
  - 6 départements ont plus de la moitié de leur population dans un EAIP « débordement de cours d'eau » : Vaucluse, Haut-Rhin, l'Isère, Pyrénées-Orientales, Ariège et Savoie.
  - 2,3 % de la population française réside de manière permanente dans l'EAIP « submersion marine ». Cinq départements sont particulièrement exposés : le Pas-de-Calais, la Vendée, la Manche, la Charente-Maritime et la Gironde. 442 communes sont dotées d'un plan de prévention des risques littoraux.
- 271 plans de prévention du risque d'incendie de forêt PPRIF sont opposables ou prescrits (pour moitié en PACA, 22% en Nouvelle Aquitaine, 18% en Occitanie, 10% en Corse).

[9] Géorisque, Ministère de la transition écologique et de la cohésion des territoires
https://www.georisques.gouv.fr/minformer-sur-un-risque/inondation




*Exemples de cartographies de risques (cf. étude d'Infranum-Banque des Territoires sur la résilience des infrastructures numériques - juillet 2023)*

*Des risques plus élevés en outre-mer*

Beaucoup de territoires ultra-marins sont soumis à des risques naturels majeurs[10] (séismes, volcanisme, cyclones, submersion, tsunami…) et sont davantage vulnérables (insularité, sous-dotation en moyens matériels...).

Entre 1980 et 2021, 360 tempêtes ont touché la métropole. Lothar et Martin (décembre 1999) ont engendré à eux seuls des coûts estimés à 12 Md€ pour l'ensemble du marché de l'assurance. Les tempêtes touchent en moyenne 400 communes par an. **À la suite de l'ouragan IRMA qui a dévasté Saint Barthélemy et Saint Martin, des principes de résilience ont été appliqués pour la reconstruction du bâti et des réseaux, avec notamment un enfouissement systématique des infrastructures électriques comme télécom, financé pour partie par des fonds publics.**

**Alex et la Roya**

La Roya a été la vallée le plus touchée par la tempête Alex en octobre 2020. Il a fallu constituer une cellule spécifique sur les infrastructures au sein du Centre opérationnel de la Préfecture, afin d'améliorer la coordination. Au démarrage, la Préfecture n'avait pas pris en compte l'existence du réseau fibre, mais seulement du réseau cuivre. Le réseau FttH, en cours de déploiement, a été touché y compris dans le génie civil enterré, emporté avec des tronçons de route et des ponts. Un nœud optique et plusieurs points de mutualisation ont été emportés.

[10] Rapport sénatorial « Risques naturels majeurs : urgence déclarée outre-mer » (juillet 2018) https://www.senat.fr/rap/r17-688-1/r17-688-1_mono.html

Le réseau a pu être remis en état en mobilisant les équipes qui oeuvraient à la construction du réseau dans le département, et étaient donc sur place, avec des moyens et une certaine connaissance du terrain. Altitude Infrastructure avait mené les actions de court terme suivants[11] :

- Information régulière des OC de l'état de la situation ;

- Réparation provisoire des liens de collecte et de transports altérés ou détruits ;

- Analyse des clients activés coupés ;

- Audit du réseau de l'ensemble de la zone :

- Premières réparations, en tenant compte de l'état des autres infrastructures (routes, électricité notamment) ;

Dans un objectif de long terme, Altitude a ensuite mené de nouvelles études puis reconstruit le NRO et les PM détruits et tiré de nouveaux câbles. Ces opérations sont longues et doivent être menées en lien avec les services de la commune puisqu'au cas d'espèce il convenait de connaître le plan de reconstruction de la zone emportée pour finaliser le redéploiement.

La mission flash de l'Assemblée nationale qui a analysé la reconstruction des vallées, a constaté que certaines mairies avaient été dans l'impossibilité de joindre le Centre opérationnel départemental pendant 48h, les communications fixes et mobiles ayant été coupées. Elle recommande de doter les préfectures et communes isolées de téléphones satellitaires[12].

***Exemples de ressources pour recenser les aléas naturels***

- Le portail **Géorisque**[13] possède une entrée par commune, identifiant les principaux risques naturels ou technologiques. Il comporte une base de données permettant notamment de télécharger les plans de prévention des risques naturels. Il comporte également une entrée par parcelle pour les risques réglementés pour l'information des acquéreurs et des locataires (ERRIAL).
- Le site **Vigicrue**[14], doublé d'une application sur mobile paramétrable, informe en temps réel sur les risques de crues des principaux cours d'eau.
- **Météo France** publie des informations de vigilance[15] sur 9 phénomènes : vent, vagues-submersion, pluie-inondation, crues, orages, neige-verglas, avalanches, canicule et grand froid, disponibles sur son application pour mobile.

S'il n'est pas possible de déplacer ou surélever tous les ouvrages, suivant leur criticité, les principaux (NOC, POP, NRO…) doivent être hors d'atteinte, et les autres protégés ou remplaçables et réparables rapidement ; il faut évidemment croiser les implantations avec les différents scénarios (par exemple, pour les inondations, les évènements extrêmes de faible probabilité, le probabilité moyenne (centennale), et de forte probabilité). Pour les communes exposées, les scénarios minima à prendre en compte sont définis réglementairement[16].

---

[11] Extraits de la réponse d'AI à la consultation de l'Arcep sur le « bilan et perspectives » de juillet 2022

[12] https://www.assemblee-nationale.fr/dyn/16/organes/commissions-permanentes/developpement-durable/missions-de-la-commission/mi-flash-vallees-roya-tinee-vesubie-tempete-alex

[13] https://www.georisques.gouv.fr

[14] https://www.vigicrues.gouv.fr

[15] https://vigilance.meteofrance.fr/fr

[16] Article R. 563-31 du Code de l'environnement

Le Dossier Départemental sur les Risques Majeurs (DDRM), publié sur le site de la préfecture, est un document informatif et pédagogique centré sur le territoire. Il explique les phénomènes et les principes de la sécurité civile, recense les risques par commune et les communes couvertes par des mesures de prévention, donne des éléments clefs liés au territoire et à l'historique des crises. Un Dossier d'Information Communal sur les Risques Majeurs (DICRIM) peut préciser le document départemental.

**SYNTHÈSE DES RISQUES PAR COMMUNE[1]**

| COMMUNE | INONDATION COURS D'EAU[2] | INONDATION SUBMERSION MARINE | INCENDIE DE FORÊT | MOUVEMENT DE TERRAIN | SISMIQUE[3] | TEMPÊTE | RUPTURE BARRAGE | RUPTURE DE DIGUE | INDUSTRIEL OU SIS | MINIER | CANICULE | RADON | TMD |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| BEAULIEU | | | ● | ● | ● | ● | | | | | ● | ● | ● |
| BÉDARIEUX | ● | | ● | ● | | ● | ● | ● | ● | ● | ● | ● | ● |
| BÉLARGA | ● | | ● | ● | ● | ● | ● | | | | ● | ● | ● |
| BERLOU | | | ● | ● | | ● | | | | | ● | ● | |
| BESSAN | ● | ● | ● | ● | ● | ● | ● | | | | ● | ● | ● |
| BÉZIERS | ● | | ● | ● | ● | ● | ● | ● | ● | | ● | ● | ● |

**COMMUNES COUVERTES PAR LES DISPOSITIFS SUIVANTS[4] :**

| COMMUNE | SOUMISE À PPI Plan particulier d'intervention | COUVERTE PAR UN PPR Plan prévention des risques | ZONE DE SISMICITÉ | ZONE POTENTIEL RADON | CONCERNÉE PAR UN SIS Système d'information sur les sols | NOMBRE D'ARRÊTÉ CAT NAT Catastrophes naturelles |
|---|---|---|---|---|---|---|
| FRONTIGNAN | Industriel | Inondation - Technologique | 2 Faible | 1 | ● | 14 |
| GABIAN | | Inondation | 2 Faible | 3 | | 5 |
| GALARGUES | | Inondation | 2 Faible | 2 | | 8 |
| GANGES | | Inondation | 2 Faible | 2 | | 8 |
| GARRIGUES | | Inondation | 2 Faible | 1 | | 5 |
| GIGEAN | | Inondation | 2 Faible | 1 | | 6 |
| GIGNAC | Barrage | Inondation | 2 Faible | 1 | | 10 |
| GORNIES | | | 2 Faible | 2 | | 9 |
| GRABELS | | Inondation - Feu de forêt | 2 Faible | 1 | | 13 |

Extraits du DDRM de l'Hérault

## 1.3 Quelle évolution des risques ?

### *Un scénario d'adaptation à 4°C*

Une troisième version du Plan national d'adaptation au changement climatique (Pnacc) est attendue pour 2024. Elle prendra en compte l'hypothèse retenue par le Conseil national de la transition écologique en mai 2023 d'une trajectoire menant à une augmentation des températures moyennes en France métropolitaine de 4°C à la fin du siècle (à adapter pour les outre-mer), plus élevée que dans les deux plans précédents. **Le Ministre de la transition écologique a précisé qu'elle entraînerait notamment des conséquences sur les réglementations des infrastructures. C'est donc un signal clair qui est donné, même s'il n'est pas nécessaire d'attendre le durcissement de la réglementation pour s'engager dans des adaptations.**

**Ressources pour s'acculturer au risque du changement climatique**

Face à la difficulté de prendre des décisions, tout en évitant les « maladaptations[17]», de plus en plus d'outils d'information et de sensibilisation sont à disposition. Le portail DRIAS[18] (les futurs du climat) permet de visualiser et géolocaliser les projections climatiques suivant les scénarios les plus récents du 6ème rapport du GIEC. Climadiag[19] propose une entrée par commune, permettant de visualiser les conséquences des hypothèses basses, moyennes ou hausses d'évolution climatique sur les précipitations et températures. Une plateforme de The Shift Project[20] propose un outil d'autodiagnostic territorial de résilience. Il est également primordial de passer d'une conception verticale descendante à une « culture du risque » de tous les acteurs et de la population, comme le développe le CEREMA dans un dossier et un guide[21]

## 2. Des risques partagés avec d'autres types de réseaux

### 2.1 Interdépendance des réseaux

Si certaines crises peuvent toucher spécifiquement un réseau de télécoms, comme une cyberattaque, les crises les plus graves vont frapper à des degrés divers l'ensemble des réseaux d'un territoire. Par exemple, si le réseau routier est touché, avec des passages impraticables, la relève du réseau électrique sera ralentie, les réseaux de télécoms et ferrés tomberont en panne, engendrant de nouveaux problèmes d'encombrements de circulation etc. France Stratégie a récemment publié une note d'analyse[22] sur ce sujet, intitulée « le temps d'agir », pointant le fait que *« Le changement climatique n'est une réalité lointaine ni dans le temps, ni dans l'espace : ses premiers effets sont visibles dans le monde entier et vont fortement s'accentuer »*. La note pointe les vulnérabilités matérielles, mais aussi sur les personnes, par exemple sur les techniciens chargés de maintenir les réseaux en fonctionnement ou de les réparer, et souligne l'accroissement des risques liés aux interdépendances.

> *Connaître les interdépendances et organiser des liens avec les opérateurs locaux de tous les réseaux est une nécessité pour organiser la résilience d'un réseau télécom. Inversement, à titre d'exemple l'alimentation en eau potable peut faire appel à de la télésurveillance et de la télégestion, avec des flux dépendant localement d'une collecte en fibre optique.*
> **Extrait de la note d'analyse de France Stratégie**

[17] Le troisième rapport d'évaluation du GIEC définit la maladaptation comme « une adaptation qui échoue à réduire la vulnérabilité, mais au contraire, l'accroît ».
[18] https://www.drias-climat.fr/
[19] https://meteofrance.com/climadiag-commune
[20] https://theshiftproject.org
[21] https://www.cerema.fr/fr/actualites/developper-culture-du-risque-territoires-dossier

[22] https://www.cairn.info/revue-la-note-d-analyse-2022-3-page-1.htm

**Tableau 3 – Vision qualitative des interdépendances entre réseaux**


Note : la couleur indique le degré du lien de dépendance du réseau en colonne vis-à-vis de celui en ligne : le lien de dépendance est plus important dans le cas d'une case rouge que dans celui d'une case verte.

Lecture : le réseau ferroviaire, le réseau de télécommunications et le réseau de distribution d'électricité sont fortement dépendants du réseau de transport d'électricité (cases en rouge). En revanche, le réseau routier n'est que peu dépendant des réseaux d'électricité, à l'exception d'interdépendances liées aux péages ou éléments de circulation (cases en gris). Des interdépendances géographiques existent entre de nombreux réseaux et en particulier avec le réseau routier, compte tenu de la présence des câbles électriques ou de télécommunications sous les routes ou le long de celles-ci (première ligne du tableau). Les réseaux d'électricité sont dépendants des télécommunications, notamment dans le cas du pilotage de la distribution par exemple (cases en orange).

Connaître les interdépendances et organiser des liens avec les opérateurs locaux de tous les réseaux est une nécessité pour organiser la résilience d'un réseau télécom. Inversement, à titre d'exemple l'alimentation en eau potable peut faire appel à de la télésurveillance et de la télégestion, avec des flux dépendant localement d'une collecte en fibre optique.

## 2.2 Focus sur le réseau électrique

Vu le degré de dépendance des télécoms au réseau électrique, il est utile de connaître les éléments-clefs de sa résilience[23]. De plus, si l'organisation ou les fragilités techniques sont très différentes, il est intéressant de s'en inspirer pour trouver sa propre voie concernant le FttH.

[23] Par souci de simplification, il n'est mentionné que ENEDIS. En pratique, la distribution électrique en France métropolitaine est assurée à 95% par ENEDIS, en lien avec les Autorités organisatrices de la distribution d'électricité (AODE), mais il existe aussi des distributeurs locaux pour les 5% restants dont il est indispensable de se rapprocher le cas échéant. De même, dans les systèmes électriques isolés (Corse et Outre-Mer) la distribution de l'électricité est assurée par EDF SEI (systèmes énergétiques insulaires) ou une SEM avec participation d'EDF à Mayotte.

### Quelle place pour les télécommunications dans les politiques de délestage ?

Il est nécessaire d'équilibrer en permanence la production et la consommation d'électricité ; ceci peut nécessiter **d'organiser des délestages**, par grandes zones géographiques, à la demande de RTE. Ce sont ensuite des paliers progressifs de délestage qui sont mis en œuvre, en commençant par suspendre les lignes derrière lesquelles les abonnés ne sont pas prioritaires. Le dernier palier concerne les lignes derrière lesquelles les priorités sont extrêmement fortes : hôpitaux, préfectures, sites SEVESO… Chaque préfecture désigne la hiérarchie des sites permettant de définir, à froid, les paliers, en sa basant sur des instructions générales.
Solutions pour le secteur des télécommunications :

- Les opérateurs de télécoms entretiennent des **équipements de secours électriques** pour leurs nœuds de réseaux fixes et mobiles, permettant de prendre le relai pour deux à quatre heures en cas de coupure. Cependant l'état des batteries et les aléas des bascules et redémarrages poseraient de sérieux problèmes si les délestages devenaient fréquents et massifs. La solution, parfois évoquée dans la presse, de délester plus finement, au niveau des compteurs Linky, est impossible techniquement, car la remontée des informations ne se fait pas en temps réel, contrairement au pilotage nécessaire pour équilibrer l'offre et la demande.
- D'autres pistes qui permettraient de tenir compte des nœuds de réseau de télécoms dans les délestages sont à l'étude. Le Ministre en charge des communications électroniques en a fait l'annonce au TRIP de l'Avicca[24] : « Les récents enjeux climatiques et géopolitiques (avec les coupures d'électricité probables en hiver) nous obligent à garantir un niveau de fiabilité des réseaux importants pour ne pas impacter la vie économique et la sécurité de nos concitoyens. C'est la raison pour laquelle **une mission inter-inspections vient d'être lancée afin d'identifier les mesures à prendre pour formuler des principes organisationnels dans une vision de renforcement de la résilience** des réseaux numériques à court, moyen et long terme, afin de garantir pour l'avenir la continuité de la vie économique et sociale de la Nation en toutes circonstances. »

## ***Investissements préventifs***

Des risques différents en fonction du type d'ouvrage

Les politiques d'investissements du distributeur du réseau publique d'électricité sont orientées sur les risques climatiques les plus prépondérants en fonction des différents types d'ouvrages :

- Les réseaux aériens sont sensibles aux épisodes de vent, givre ou neige collante, et à la proximité de zones boisées
- Les réseaux souterrains sont sensibles aux épisodes de fortes chaleurs et aux épisodes de crues.

De multiples nécessités d'investissements pour la filière

Pour se prémunir des aléas climatiques, le distributeur procède à de nombreux investissements, lesquels peuvent se traduire par :

- L'enfouissement ciblé de réseaux aériens

[24] Discours de Jean-Noël Barrot, 16 mai 2023 http://www.avicca.org/actualite/trip-de-printemps-2023-discours-de-jean-noel-barrot-ministre-delegue-charge-de-la

- Le remplacement de technologies « fragiles » (réseaux aériens fils nus par du réseau aérien torsadé, réseau souterrain « CPI » par des câbles de nouvelle génération, série de matériaux sujets au vieillissement prématuré par des matériaux plus modernes)
- La restructuration et la modernisation de son réseau pour limiter les conséquences d'un incident électrique (bouclage du réseau, pose de matériaux permettant de limiter l'impact clients et faciliter le rétablissement rapide de l'alimentation).

En parallèle, pour répondre à des défis majeurs autres que la résilience, notamment la prise en compte du développement des Énergies renouvelables (ENR) et des Infrastructures de Recharge des Véhicules Electriques (IRVE), le distributeur doit réaliser des investissements considérables[25]. Les investissements, ayant une incidence directe sur le prix de l'énergie via le TURPE, sont encadrés par la Commission de régulation de l'énergie (CRE).

Les ambitions de résilience des acteurs du réseau électrique

**Forte ambition sur la haute tension :** sur la haute tension, ENEDIS projette d'enfouir 28 000 km de réseau HTA identifiés comme étant « à risque avéré au regard du référentiel climatique et de la présence des zones boisées » d'ici 2032, mais l'utilisation du réseau HTA par les télécoms est extrêmement marginale.

**Sur la basse tension, les Autorités organisatrices de la distribution d'énergie (AODE) sont confrontées aussi aux multiples nécessités d'investissement.** Elles peuvent être plus ou moins volontaristes pour les programmes d'enfouissement, en fonction de leurs moyens, de l'exposition de leurs territoires aux aléas (notamment sur les façades maritimes) et de leur vision stratégique. En ordre de grandeur, environ 1% du réseau est enfoui chaque année, le plus souvent à la demande des communes qui veulent enfouir tous les réseaux aériens (télécom, éclairage, électricité) et participent au financement. De plus, la basse tension étant par définition en bout de réseau, un segment à enfouir aura un impact moindre qu'une intervention sur l'amont du réseau électrique ; à cela s'ajoute la complexité du raccordement chez les usagers en cas d'enfouissement en domaine public. **Il ne faut donc pas s'attendre en général à des plans massifs d'enfouissement à ce niveau.** Néanmoins, un groupe de travail FNCCR-Orange doit se constituer pour examiner l'intérêt d'enfouissements coordonnés pour des raisons de fragilité de certaines lignes aux aléas climatiques.

**On ne peut écarter l'hypothèse que l'augmentation des aléas entraîne des inflexions stratégiques des acteurs de l'électricité, mais au total il semble qu'aujourd'hui il y ait globalement assez peu à attendre d'économies pour des enfouissements coordonnés avec les réseaux télécom dans la dimension « résilience ».** Cela n'empêche pas, bien au contraire, d'explorer des opportunités locales, et d'instituer un dialogue régulier.

[25] Document préparatoire d'ENEDIS au « Plan de développement du réseau » https://www.enedis.fr/presse/transition-ecologique-enedis-devoile-les-travaux-preparatoires-son-futur-plan-de

**Exemple de la méthodologie déployée par ENEDIS**

Bien que les réseaux soient très différents, certains éléments méthodologiques[26] déployés progressivement par ENEDIS pourraient être inspirants pour les télécoms, ou même donner lieu à des synergies :
- cartographie des zones de fragilité électrique, basée sur les scénarios hydrographiques recensant les ouvrages et les clients impactés suivant les hauteurs de crues ;
- projet de détection des hauteurs d'eau par des capteurs communicants pour la gestion de crise en temps réel ;
- remplacement des ouvrages qui présentent des taux de défaillance anormalement élevés (détection à partir d'un traitement de big data sur l'incidentologie : « L'objet du machine learning est de déterminer la meilleure loi de corrélation entre des données d'entrée massives (description du réseau, historique et localisation des incidents, données environnementales...) et des données de sortie connues (incidents survenus sur les années d'apprentissage que le modèle cherche à reproduire ».

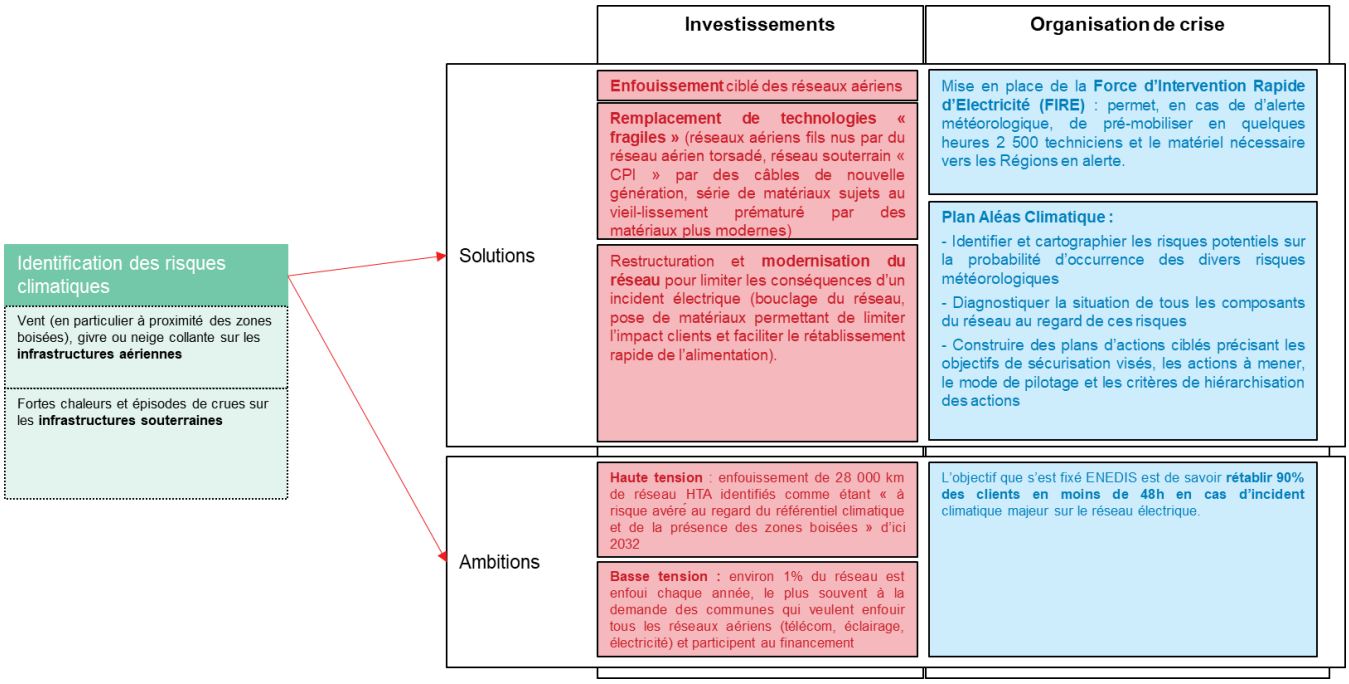
## ***Organisation de crise***

Au chapitre curatif, le traitement des crises par le distributeur du réseau publique d'électricité ENEDIS s'appuie sur sa **Force d'intervention rapide électricité (FIRE), mise en place suite à la tempête de 1999.** Elle permet, en cas de d'alerte météorologique, de pré-mobiliser en quelques heures 2 500 techniciens et le matériel nécessaire vers les Régions en alerte. Le dispositif de gestion de crise peut également s'appuyer sur un parc important de groupes électrogènes, ainsi que sur un Plan Aléas Climatique présenté aux pouvoirs publics dès 2006. Ce dernier est réactualisé régulièrement et s'appuie sur 3 grands principes :

- Identifier et cartographier les risques sur la probabilité d'occurrence des divers risques météorologiques
- Diagnostiquer la situation de tous les composants du réseau au regard de ces risques
- Construire des plans d'actions ciblés précisant les objectifs de sécurisation visés, les actions à mener, le mode de pilotage et les critères de hiérarchisation des actions

[26] Document préparatoire d'ENEDIS au « Plan de développement du réseau » p 92 à 96

**L'objectif que s'est fixé ENEDIS est de savoir rétablir 90% des clients en moins de 48h en cas d'incident climatique majeur sur le réseau électrique.**




## 3. Quelles alternatives en cas d'incident ?

### 3.1 Les usagers du fixe sauvés par le mobile en cas de crise ?

Dans une certaine mesure, le réseau mobile peut prendre le relai de pannes du réseau fixe pour les usagers. Mais il en est tout autrement en cas de crise générale (multiréseaux) touchant massivement les usagers.

**Limites de la substitution du réseau FttH par le réseau mobile**

- La collecte d'une partie des sites mobiles est assurée par les réseaux FttH ;
- Le réseau mobile sera déjà extrêmement sollicité ; des pannes importantes du réseau fixe ne feraient qu'aggraver les risques de saturation ;
- De nombreux usages du réseau fixe ne pourraient pas être assurés, en particulier pour les professionnels (monétique…), les petites entreprises sans sécurisation, des GFU de collectivités si la collecte est touchée, etc.
- 5% des ménages n'ont pas de téléphone mobile, un chiffre qui peut sembler marginal, mais qui montre que pour certains, parmi lesquelles sans doute une bonne part de personnes âgées, le téléphone fixe est le seul moyen de contacter les urgences.

Une importance croissante de la fibre optique

Il est incontestable que le rétablissement des réseaux du mobile sera prioritaire par rapport au fixe en situation de crise, ne serait-ce que pour les services qu'ils rendent en mobilité. Mais le paradoxe, c'est que **les réseaux mobiles seront de plus en plus dépendants des réseaux en fibre optique pour la collecte, et non l'inverse**. Identifier les émetteurs potentiellement impactés par une interruption des réseaux fixes devrait logiquement faire partie du recensement des priorités en cas de crise.

De plus, il est certain **que les usages des réseaux FttH ne feront qu'augmenter, en particulier dans les territoires de RIP où celui-ci servira plus qu'ailleurs à collecter des flux de services publics** (IoT, vidéoprotection, GFU…), aussi les réseaux FttH doivent-ils assurer leur propre résilience et se faire reconnaître par l'ensemble des autres acteurs pour entrer dans les priorités de rétablissement.

## 3.2 Certains usagers finaux doivent contribuer à leur propre résilience

Un réseau de masse, du fait de son nombre d'usagers finaux, d'opérateurs usagers et de son architecture, ne peut pas assurer une disponibilité parfaite en cas de crise.

Pour les entreprises et les principaux services publics, les sites dont le fonctionnement est très affecté par les indisponibilités doivent disposer de solutions de secours (4 ou 5G, satellite, double adduction FttO/FttH, liaisons de secours FH…) leur permettant de basculer en cas de problèmes, éventuellement en mode dégradé amenant à prioriser les flux.

L'État dispose de réseaux propres pour ses usages les plus critiques et en développe de nouveaux, via la création d'une Agence des communications mobiles opérationnelles de sécurité et de secours, et du **Réseau radio du futur[27] qui doit être opérationnel en 2024**, pour connecter les utilisateurs du terrain (policiers, gendarmes, SAMU, sapeurs-pompiers) entre eux et avec les salles de commandement. De plus, la guerre en Ukraine a accéléré les décisions au niveau européen, avec le **lancement d'une constellation de satellites en orbite basse, baptisée IRIS 2** (Infrastructure de Résilience et d'Interconnexion Sécurisée par Satellite). Centrée sur les applications gouvernementales pour des communications cryptées, elle pourrait aussi contribuer à assurer la continuité d'Internet en cas de crash des infrastructures terrestres par cyberattaque ou catastrophe naturelle. **Les premiers satellites sont attendus à partir de 2024, et la zone de couverture s'étendra aux régions ultrapériphériques de l'Union.**

[27] https://www.interieur.gouv.fr/actualites/communiques/lancement-du-projet-reseau-radio-du-futur-rrf-reseau-tres-haut-debit

02

# La répartition des responsabilités

# 1. Panorama des acteurs et des dispositifs

## 1.1 La gestion de crise

On distingue classiquement 4 phases dans la gestion de crise, qui sont toutes nécessaires pour minimiser les impacts des aléas :

- Prévention (investissements de sécurisation, identification des aléas locaux…)
- Préparation (plans de continuité d'activité, stocks mobilisables…)
- Réaction (déclenchement de la procédure de crise, activation de cellule de crise et cellule de communication…)
- Adaptation (retours d'expérience pour améliorer la résilience…).

Par définition, la crise peut prendre des formes extrêmement variées, en ampleur, durée, origine etc. Le scénario d'une pandémie avec confinement comme le COVID n'était guère envisagé en dehors des autorités sanitaires, et fait aujourd'hui l'objet de Plans de continuité d'activité spécifiques chez les opérateurs. Au moment de la crise, on s'appuie donc sur des éléments préparés (annuaires internes et externes de contacts à jour et à disposition permanente du personnel…) et on « débranche » aussi certaines procédures qui deviennent inapplicables. Ce sont aussi des moments où jouent la mobilisation, la solidarité et l'entraide, au sein des territoires, mais aussi au niveau national. Le retour à la normale se fait souvent par phases (rétablissement du service sur des installations provisoires, reconstruction…).
*La sécurité civile distingue la crise, qui touche spécifiquement un opérateur, de la crise généralisée, qui en touche plusieurs et nécessite une organisation collective de réponse (typiquement un évènement climatique important).*

## 1.2 Le dispositif ORSEC pour les réseaux

En 1952, la France se dote du dispositif ORSEC qui vise à organiser sous l'autorité du préfet « la mobilisation, la mise en œuvre et la coordination des actions de toute personne publique et privée concourant à la protection générale des population » (selon l'article R741-1 du Code de la Sécurité Intérieure). En 2015, la Direction générale de la sécurité civile et de la gestion des crises (DGSCGC) élabore un guide ORSEC sur les nouvelles modalités de rétablissement et l'approvisionnement d'urgence des réseaux électricité, communications électroniques, eau, gaz, hydrocarbures, intitulé « RETAP RESEAUX »[28]. Il est destiné à donner des éléments méthodologiques pour l'établissement des dispositifs ORSEC territoriaux.

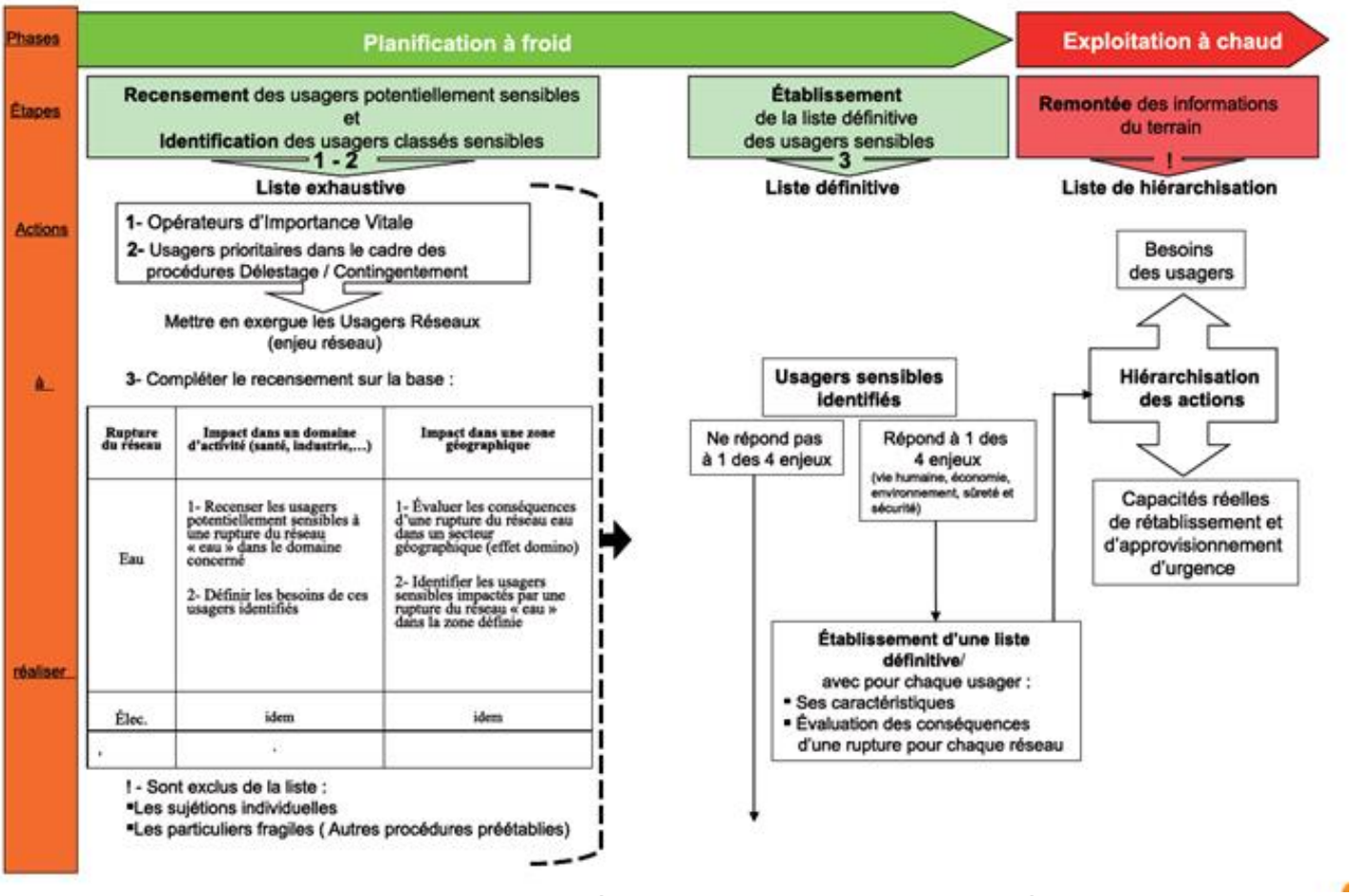
RETAP RESEAUX rappelle que les opérateurs de réseaux ont un point unique d'entrée suivant leur tutelle ministérielle ; ils doivent également être représentés dans les centres publics de décision. Le guide précise des notions importantes :

- Distinction entre « crise » (touchant un opérateur) versus « crise généralisée » (multiples opérateurs concernés)
- Définition des usagers prioritaires (à servir en cas de délestage ou de contingentement) et des usagers sensibles (dont les ruptures d'alimentation ont des conséquences importantes en matière de vie humaine, d'impact sur d'autres réseaux etc.)
- Hiérarchisation des usagers pour les rétablissements ou l'approvisionnement d'urgence

[28] https://www.interieur.gouv.fr/content/download/86317/668662/file/Guide%20ORSEC%20RETAP%20RESEAUX.pdf

- etc.

Il précise également que des panels d'information à échanger sont définis au niveau national, réseau par réseau, afin de disposer des informations utiles.

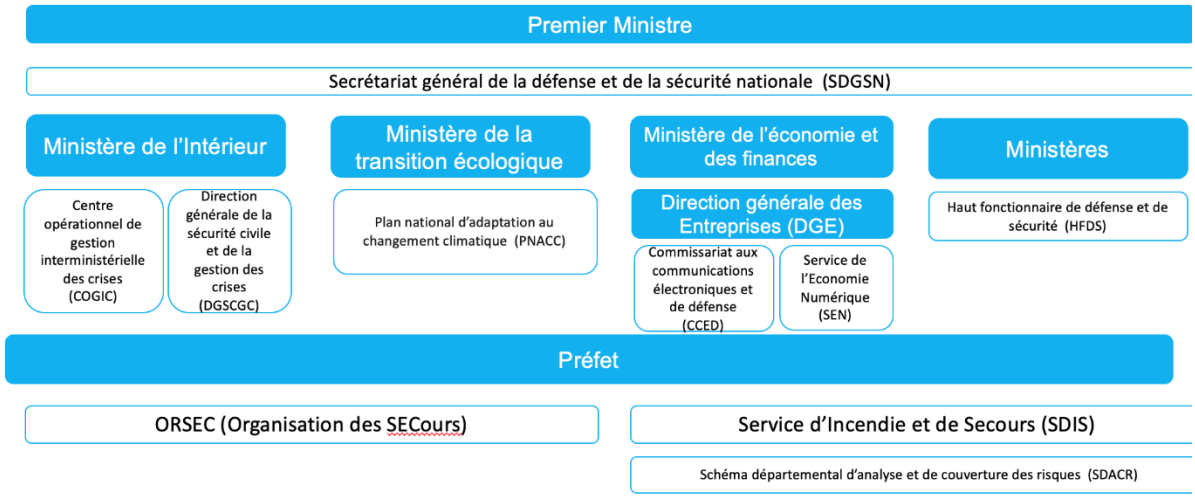



*Extrait du guide ORSEC RETAP sur la hiérarchisation des usagers pour le rétablissement ou l'approvisionnement d'urgence*

> *« Aurez-vous du carburant en cas de pénurie pour maintenir votre réseau ? Serez-vous dans les priorités de rétablissement du réseau électrique ? Sûrement pas si vous n'êtes pas inclus dans le dispositif ORSEC. »*
> Extrait du guide ORSEC RETAP sur la hiérarchisation des usagers pour le rétablissement ou l'approvisionnement d'urgence

## 1.3 Les acteurs et le cadre réglementaire

***Les acteurs institutionnels***




Le Secrétariat général de la défense et de la sécurité nationale (SGDSN), placé auprès du Premier ministre, est l'organe interministériel en charge pour « anticiper, prévenir, protéger ». Des questions de pandémie aux cyberattaques (via la désormais bien connue ANSSI), ses missions ne manquent pas.

Au quotidien, le ministère de l'Intérieur a la charge de la sécurité civile, pour les personnes et les biens, notamment via la Direction générale de la sécurité civile et de la gestion des crises (DGSCGC). Le Centre opérationnel de gestion interministérielle des crises (COGIC), est l'instance de commandement de gestion des crises de la sécurité civile, sous la tutelle du ministère de l'Intérieur. Il analyse et gère les catastrophes naturelles et technologiques, assure la remontée d'informations ainsi que l'interface avec les centres opérationnels des autres ministères.

Certains ministères[29] ont un Haut fonctionnaire de défense et de sécurité (HFDS), qui, dans son périmètre, veille notamment sur les plans de continuité d'activité, la gestion des crises, l'application de la réglementation relative aux Secteurs d'activité d'importance vitale (SAIV). Plus spécifiquement pour les télécommunications, la Direction générale des entreprises comporte un Commissariat aux communications électroniques et de défense (CCED[30]), rattaché au service de l'économie numérique.

Un réseau de 12 centres opérationnels assure les rôles de veille et d'alerte à l'échelle nationale.

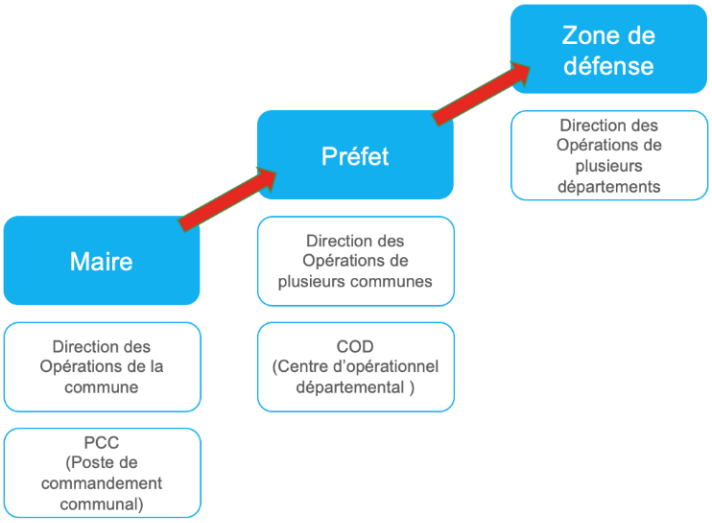
[29] Ministères en charge de la santé, de l'économie et des finances, du travail, de l'éducation nationale, de l'enseignement supérieur et de la recherche, de la culture, de la transition écologique…

[30] https://lannuaire.service-public.fr/gouvernement/06251b9f-b17e-4122-8315-d97b8f0e8e7f

## ***Les acteurs locaux***

Le niveau régional ou interrégional est structuré en 7 Zones de défense et de sécurité.

Les collectivités qui déploient des réseaux se sont approprié le Code des Postes et Communications Electroniques (CPCE), mais sont moins familières avec le Code de la Sécurité Intérieure (CSI). Au niveau des grands principes, ce code précise que *« Les exploitants d'un service, destiné au public, d'assainissement, de production ou de distribution d'eau pour la consommation humaine, d'électricité ou de gaz, ainsi que* ***les opérateurs des réseaux de communications électroniques ouverts au public*** *prévoient les mesures nécessaires au maintien de la satisfaction des besoins prioritaires de la population lors des situations de crise »*[31]. Le préfet peut, en outre, solliciter un programme d'investissements prioritaires d'un opérateur donné[32]. La réponse de la sécurité civile est effectuée en fonction de l'émergence de la crise.




Le maire est le premier échelon de la réponse de sécurité civile :

- Il possède des responsabilités « à froid » : l'élaboration d'un Plan communal de sauvegarde (il existe également des Plans intercommunaux de sauvegarde[33]. Ces plans comprennent une analyse de l'ensemble des risques connus auxquels la collectivité est exposée et des risques propres aux particularités locales.
- Il possède des responsabilités « à chaud » : en cas de crise, le maire active un Poste de commandement communal (PCC) qui centralise les informations et coordonne les actions. En cas de crise, il assure la direction des opérations dans la limite de sa commune, jusqu'à ce que, si nécessaire, le préfet assume cette responsabilité. En outre, il est en relation avec le Centre opérationnel départemental (COD) dirigé par le préfet.

Les pouvoirs du préfet (analysés en détail au cours de la sous-partie suivante) :

- « A froid », le dispositif ORSEC (Organisation des SECours) permet la préparation des acteurs, notamment via un recensement des risques et des exercices de crise (voir supra

[31] Article L.732-1 du CSI
[32] Article L.732-2-1 du CSI
[33] L'obligation pour les communes et intercommunalité de se doter d'un plan de sauvegarde a été étendu par la loi du 25 novembre 2021 et son contenu a été précisé par le décret 2022-907 https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045940284

et annexe). Sous l'autorité du préfet, le Service d'Incendie et de Secours (SDIS)34 élabore le Schéma départemental d'analyse et de couverture des risques (SDACR) qui analyse les moyens nécessaires.

- « A chaud », le préfet peut mobiliser les organes de sécurité (police, gendarmerie, sapeurs-pompiers, SAMU…), mais aussi le secteur privé, dont les opérateurs de réseaux.

Le Code de la sécurité intérieure donne aussi la possibilité au préfet d'imposer localement des actions de prévention et de réaction dans les territoires où l'exposition importante à un risque naturel peut conduire à l'arrêt de tout ou partie du service. Il peut demander par arrêté aux exploitants de réseaux, après avoir recueilli l'avis de leur autorité délégante, de réaliser, sous peine de sanction, un diagnostic de vulnérabilité, les mesures prises en cas de crise pour prévenir les dégâts et pour assurer un service minimal pour satisfaire les besoins prioritaires de la population, les procédures de remise en état du réseau ou encore un programme des investissements prioritaires pour améliorer la résilience des services prioritaires pour la population en cas de survenance de l'aléa.

Sans attendre une injonction préfectorale explicite, la connaissance des obligations et de leurs conditions et modalités de mise en œuvre (rappelées en annexe) est donc utile pour que chaque maillon de la chaîne se prépare.


[34] Pour certains territoires, la dénomination exacte est Service d'incendie et de secours (SIS) ou Service territorial d'incendie et de secours (STIS).


## 1.4 Le rôle central du préfet

***Le rôle du préfet dans le cadre du dispositif ORSEC pour les réseaux***

Les réseaux FttH ne sont pas insérés systématiquement dans le dispositif ORSEC. Cette inclusion est pourtant nécessaire au regard des interdépendances que le réseau FttH partage avec d'autres réseaux en particulier le réseau électrique (comme discuté dans la partie sur les risques partagés). En attente d'instruction ministérielle qui permettra de systématiser l'insertion des réseaux FttH dans le dispositif ORSEC, il convient de solliciter officiellement le préfet à cet effet.

***Les pouvoirs conférés par la loi « Climat et Résilience »***

La loi dite « Climat et résilience », précisée par décret en 202235, a donné de nouveaux pouvoirs au préfet. Cette loi liste les territoires concernés, en fonction des divers risques (inondation importante, sismicité, vents violents cycloniques, incendies de forêts) et les scénarios de référence à prendre en considération.
Elle donne la possibilité à l'autorité compétente de l'Etat (généralement le préfet) de prescrire par arrêté à tout exploitant

[35] Loi du 22 aout 2021, et décret n° 2022-1077 du 28 juillet 2022 relatif à la résilience des réseaux aux risques naturels, codifiés dans le Code de la sécurité intérieure

de réseau, après avis de l'autorité qui a délégué le service, la fourniture :

- d'un diagnostic de vulnérabilité, comprenant une cartographie des points de vulnérabilité du réseau et les zones potentiellement impactées ;
- d'un programme des investissements prioritaires détaillant les travaux nécessaires pour améliorer la résilience du réseau et réduire les zones potentiellement impactées.

L'autorité compétente de l'Etat fait part de ses observations à l'exploitant sur ces documents, ainsi qu'à l'autorité qui a délégué le service. Enfin, une demande d'actualisation du document peut être formulée au cas où une interruption du service due à un évènement naturel aurait conduit à « ne plus pouvoir répondre aux besoins prioritaires de la population ».

**En pratique**

À notre connaissance, aucun arrêté préfectoral basé sur ce dispositif législatif et concernant un réseau FttH n'a été pris à ce jour. Il n'est cependant pas inutile de se préparer pour cet exercice sans attendre une contrainte, ou simplement de se caler sur ce dispositif. Ainsi, même en l'absence d'arrêté, le Syndicat Mixte Haute-Garonne numérique a pu utilement s'appuyer sur la référence à ce cadre pour entrer en dialogue avec les autres exploitants de réseau du territoire et avancer la réflexion avec ses partenaires. À noter toutefois que seuls les risques naturels sont visés, et que la prescription ne porte pas sur l'organisation de crise de l'exploitant, qui doit aussi être traitée.

## 2. Quelles responsabilités des opérateurs télécoms ?

### 2.1 Les obligations générales des opérateurs télécoms

En vertu de **l'article L. 33-1 du Code des postes et communications électroniques (CPCE)**, les opérateurs sont débiteurs d'obligations qui tiennent à des conditions de permanence, de qualité, de disponibilité, de sécurité et d'intégrité du réseau et du service. A ce titre, il leur est demandé de :

- Notifier à l'autorité compétente des incidents de sécurité ayant eu un impact significatif sur le fonctionnement du réseau et du service de communications électronique
- Mettre en œuvre toute mesure permettant de garantir la continuité de l'acheminement des communications d'urgence

Une coupure de la continuité optique entraîne notamment l'impossibilité de joindre les numéros d'urgence pour les usagers situés en aval.

Un guide pour la déclaration des incidents affectant les réseaux et infrastructures de communications électroniques[36] et de l'internet ouverts au public a été publié par le service du Haut fonctionnaire de défense et de sécurité en charge du secteur. Il définit notamment les seuils à partir desquels cette notification est obligatoire (par exemple une indisponibilité totale du service d'accès à internet ou de téléphonie fixe touchant plus de 50 000 abonnés grand public ou 2 000 entreprises pendant 2 heures). À date, il n'est pas prévu d'abaisser ces seuils pour tenir compte des OI de petite taille, afin que seulement les incidents très significatifs, à l'échelle nationale s'entend, soient signalés. Bien entendu, des dispositifs de signalement à

[36] https://www.entreprises.gouv.fr/files/files/secteurs-d-activite/numerique/politique-numerique/communications-electroniques/communications-d-urgence/guide-operateurs-declaration-incidents-reseaux.pdf

l'échelle locale, sur des seuils beaucoup plus bas, sont nécessaires, en particulier pour les délégants.

## 2.2 La responsabilité des OC en tant qu'exploitants d'un service « destiné au public »

**L'article L.732.1 du Code de la sécurité intérieure** impose des obligations génériques aux exploitants d'un service « destiné au public », tels que les opérateurs de réseaux de communications électroniques ouverts au public. En tant que tels, les Opérateurs d'infrastructure ne fournissent pas de services au public.

Ce sont donc les Opérateurs commerciaux qui doivent notamment :

- « protéger leurs installations contre les risques, agressions et menaces prévisibles »
- « élaborer un plan interne de crise » qui permette de « pallier les conséquences les plus graves des défaillances, de la neutralisation ou de la destruction des installations »
- réaliser « à chaque révision du plan Orsec, une étude des conditions dans lesquelles ils satisferont aux obligations fixées[37] ».

Cependant, un OC ne va pas protéger un NRO contre une inondation ou une intrusion, qui est de la responsabilité de l'OI. De même, l'OI ne peut pas décider de dimensionner le stock de poteaux nécessaire à Orange ou ENEDIS pour intervenir en cas de destruction d'un volume important de lignes aériennes par un ouragan, il ne les gère pas.

**Evolutions possibles**

**Concernant les obligations sur les fournisseurs de service au public :** les obligations qui pèsent sur les fournisseurs de service au public devraient donc en toute logique descendre toute la chaîne de responsabilité spécifique aux réseaux FttH. En pratique, les clauses contractuelles idoines, les process et la prise en compte des coûts afférents sont sans aucun doute à améliorer, dans un cadre qui ne peut être que collectif.

**Concernant le dispositif réglementaire :** le dispositif réglementaire n'est pas complet non plus, puisqu'aucun arrêté n'est encore venu préciser quels sont les niveaux spécifiques de satisfaction des « besoins prioritaires » attendus, selon les services et les populations en cause. Reste que si une fibre optique est coupée, un OC ne saura pas satisfaire le moindre « besoin », essentiel ou non. À noter également que le caractère prioritaire se détermine aussi par « la continuité des services publics ». Or de plus en plus de RIP collectent le trafic de GFU de services publics (administrations territoriales, SDIS etc.).

## 2.3 Le rôle central de l'OI

***Les obligations génériques fixées par l'ARCEP qui encadrent les contrats d'accès entre les OI et les OC***

[37] Articles R 732-3, R 732-4 du CSI

Les obligations générales des opérateurs visent essentiellement la continuité de service vis-à-vis de l'utilisateur final, grand public, entreprises etc. Compte-tenu de la spécificité des Opérateurs d'infrastructure, dont les utilisateurs sont des Opérateurs commerciaux qui s'adressent au grand public ou aux professionnels, l'Arcep a fixé des obligations génériques qui encadrent les contrats d'accès entre les OI et les OC[38].

**S'agissant de l'action :**
L'ARCEP estime que la performance de tout réseau est liée à la capacité de l'opérateur d'infrastructure à remédier rapidement aux dysfonctionnements qui relèveraient de sa responsabilité (décision 2015-776 de l'ARCEP). L'Autorité soulève plusieurs points qui s'appliquent à tout Opérateur d'infrastructure :

- Engagement contractuel sur les délais de résolution de dysfonctionnements du réseau qui relèveraient de sa responsabilité. Elle préconise la définition d'un délai maximum de rétablissement par l'opérateur d'immeuble à l'opérateur qui accède à la ligne.
- Possibilité pour l'opérateur commercial titulaire de la ligne d'ouvrir un ticket d'incident sur les lignes actives et engagement dans l'offre d'accès sur des délais de rétablissement en cas d'incident (le cas échéant avec un partage de responsabilités à définir) et qu'il prévoie le paiement de pénalités incitatives à défaut de respect des engagements stipulés.

**S'agissant de la maintenance du réseau (vise davantage à la qualité)** : l'ARCEP retient que « L'opérateur d'immeuble[39] doit prévoir dans son offre d'accès aux lignes une prestation de maintenance pour permettre le maintien en état de bon fonctionnement du réseau mutualisé sur l'ensemble de sa durée de vie, hormis les cas de force majeure » (souligné par nous). Cette prestation doit inclure des réparations ou remises en conformité nécessaires à la mise à disposition de la ligne à l'opérateur commercial.
NB : l'Arcep peut se saisir directement d'un problème constaté chez un opérateur et le mettre en demeure de corriger des manquements. L'autorité peut également être saisie par une partie au contrat d'accès en règlement de différend. Ce type de mesures ne peut répondre à une situation de crise, mais pourrait toutefois permettre d'en tirer les enseignements.

### ***Une responsabilité inachevée de l'OI***

L'OI est en principe responsable de la continuité optique du réseau FttH du NRO à l'usager final et la doit en conséquence aux opérateurs commerciaux. La réglementation lui impose, en particulier la décision n°2015-776 de l'ARCEP, des **contraintes de garanties de temps d'intervention, de rétablissement et d'interruption maximale de service**. Ces contraintes réglementaires sont traduites contractuellement dans ses offres d'accès au bénéfice des opérateurs commerciaux. Et les contrats de DSP d'exploitation de RIP conclus avec les collectivités peuvent, en outre, les conforter voire les compléter, au titre de la maintenance préventive et curative.

Tout évènement climatique conduisant à une rupture de continuité optique impliquera ainsi en principe une mobilisation de l'OI. Cette mobilisation n'est aujourd'hui ni contrainte ni effective, pour deux raisons :

- La première tient à la notion de force majeure (constituée, selon l'article 1148 du code civil applicable aux contrats publics, de tout évènement extérieur, imprévisible et irrésistible au

[38] Notamment précisées dans la décision 2015-776 https://www.arcep.fr/uploads/tx_gsavis/15-0776.pdf

[39] Synonyme d'opérateur d'infrastructure

comportement des parties à un contrat) : elle permet à l'OI d'écarter toutes ces contraintes réglementaires et contractuelles de maintenance curative dans un délai donné. La décision n°2015-776 de l'ARCEP le précise explicitement, comme les stipulations des offres d'accès et, le plus généralement, des contrats publics d'exploitation des RIP. Sans précision particulière dans les contrats d'accès et les contrats de DSP, l'OI invoquera la force majeure en cas de survenance d'un évènement climatique, neutralisant ainsi ses obligations, comme la crise sanitaire de l'épidémie de Covid-19 l'illustre. Une identification de tout ou partie des risques climatiques dans le schéma de résilience modifierait, s'ils se réalisaient, le débat sur l'opposabilité automatique de la force majeure le moment venu.

- La seconde tient à la chaîne d'intervenants concernés, à titre préventif comme curatif : l'OI ne sera pas le seul à intervenir pour prévenir ou rétablir une interruption de service. Il doit déjà s'interfacer avec les gestionnaires des infrastructures de génie civil et appuis aériens, OWF, ENEDIS et les AODE.

Le processus usuel voit l'OI rétablir en premier la continuité optique, parfois à titre temporaire en cas d'infrastructures dégradées (câble à terre, traversée de route sur poteaux provisoires…). Ensuite, le gestionnaire d'infrastructures répare ou reconstruit les infrastructures définitives, sur lesquelles l'OI reposera le réseau.

Les rôles des collectivités et des OC : les collectivités délégantes peuvent aussi être impliquées au niveau opérationnel comme financier sur tous les sujets de vie de réseau, en fonction des clauses de chaque DSP. Les opérateurs commerciaux peuvent aussi être concernés, car ils ont notamment la charge du SAV du raccordement.

### ***Les divers moyens dont disposent les OI pour affronter une crise***

A la suite de la crise sanitaire, face aux dérèglements climatiques, mais aussi au constat de la multiplication des détériorations des réseaux par des tiers, les OI ont d'eux-mêmes commencé à renforcer leurs mesures préventives et leurs moyens d'intervention.

1. Construction du réseau : la première des responsabilités des OI en termes de résilience est bien la conception du réseau lui-même. Plusieurs OI relèvent que des choix techniques faits en amont ont permis d'augmenter la résistance de leur réseau face aux aléas climatiques.
2. Exploitation du réseau :

➔ **Prévention**

- **Maintenance préventive** : la plupart des OI, dont ceux des RIP, tendent à renforcer leurs actions de maintenance préventive face à l'explosion des charges d'exploitation, notamment de maintenance curative. Il est observé des durées de vies d'équipements inférieures à celles prévues (PBO par exemple, détériorés par l'action du vent s'ils ne sont pas refermés par les raccordeurs). Ils ont, dans cette perspective, engagé des actions pour supprimer les SPOF en sortie de NRO, changé le mode de brassage au PM (de W vers M) pour faciliter le travail des techniciens, surélevé des armoires et des shelters, mis en place des tôles à l'arrière des armoires PM pour limiter les actions malveillantes d'intervenants bien informés sur les faiblesses du réseau, ou encore utilisent l'intelligence artificielle pour le traitement d'images en masse.
- Le **contrôle du stock par l'OI** comme ses sous-traitants est fondamental, afin de garantir la disponibilité de matériels rares (l'exemple de câbles 968 paires a été cité), mais de façon générale de garantir la disponibilité de la réserve en cas de crise, avec des contrôles de ce stock effectués régulièrement.

### Complémentarité de la phase d'exploitation et de supervision

En phase de supervision, les prestataires mobilisés par la construction du réseau ne sont plus aussi engagés à l'égard de l'OI qu'en phase exploitation, ou alors sans volume d'affaires garanti. Il sera donc de plus difficile pour ces prestataires de conserver des moyens matériels et humains réellement mobilisables en cas de crise. Une harmonisation de ces contrats d'exploitation pour qu'ils intègrent un dispositif propre à la résilience est nécessaire, le cas échéant en l'imposant via les conventions de DSP.

➔ **Préparation**

- **Plans de continuité d'activité (PCA) :** l'expérience de la crise sanitaire a incité les OI à élaborer des Plans de continuité d'activité (PCA) qui comportent des moyens mobiles mobilisables (de type NRO, groupes électrogènes etc.), des exercices de simulation pluriannuel et l'organisation des astreintes tant en interne que chez les sous-traitants, notamment pour les interventions sur le génie civil, avec la mobilisation d'équipes d'autres régions. De tels documents de gestion de crise peuvent être utilement stockés en version papier par les collaborateurs de l'OI (retour d'expérience remonté) afin de ne pas improviser en cas de crise ni d'être dépendants de serveurs eux-mêmes inaccessibles.

➔ **Action**

- **Détection :** une fois le réseau opérationnel, au niveau interne, l'OI dispose déjà de moyens de supervision et de détection des incidents, centralisés dans son NOC (network operating center). Ce NOC n'est en principe pas décentralisé à l'échelle d'un réseau local, mais unique pour l'ensemble des réseaux exploités par la maison-mère du groupe auquel appartient l'OI. Cette centralisation ne constitue pas une difficulté, l'important étant de pouvoir disposer parallèlement de moyens pour intervenir localement.
- **Priorisation :** le plus souvent, les NOC sont adressés par deux backbones distincts, avec des remontées d'alarme et éventuellement de la qualité de service (QoS) renforcée pour traiter des priorisations de flux sur les réseaux activés, notamment le flux de téléphonie en cas de crise, ou encore prioriser les dérangements collectifs. Il nous a été remonté la difficulté de faire reconnaître les NRO comme sites prioritaires pour mieux garantir la continuité de fourniture d'énergie.
- **Maintenance curative** : au niveau externe, les OI mobilisent aussi des prestataires pour réaliser la maintenance curative, via des contrats cadres avec des acteurs nationaux à forte empreinte géographique qui, localement, ont recours à de la sous-traitance locale qualifiée et ayant la connaissance du territoire. La nécessité de traiter avec des acteurs de rang 1 vient de la capacité pour l'OI de négocier en national mais aussi de la nécessité pour ce prestataire d'investir dans les matériels et les ressources en astreinte.

*Tous leurs contrats ne prévoient pas forcément de chapitre propre aux situations de crise (obligations de moyens, escalade, rémunération spécifique), alors que cela devrait constituer une obligation.*

<u>Des situations qui doivent être évaluées au cas par cas :</u>

- **Des risques divers :** il semble utile et efficient de lancer des études d'incidentologie sur la zone donnée. Ces études sur la durée sont représentatives des causes naturelles mais doivent aussi intégrer les causes de tiers, à commencer par l'accidentologie routière, pour les PM et poteaux notamment.

- **En réalité les modalités d'intervention sont très différentes :** les modalités d'intervention locales sont hétérogènes d'un réseau à l'autre, en fonction des architectures et de la fourniture d'une offre activée ou par l'OI. Les procédures d'escalade et de traitement évoluent en fonction de l'architecture support du service (FttH, FttE ou FttO) pour respecter les obligations contractuelles. Les collectes extra-départementales activées (back haul) sont souvent redondées au titre des conventions de DSP, mais ce n'est pas toujours le cas. De même, les points de fragilité des segments de collecte (SPOF, single point of failure) sont en principe exclus, ou en voie de l'être à la suite de difficultés déjà rencontrées.

Il est aussi relevé par les OI le caractère fondamental du SI et de la fiabilité de la base (SIG) par rapport au terrain, dans la résilience du réseau, tout en indiquant qu'**un certain nombre d'actions de renforcement du réseau devront attendre la fin des raccordements massifs pour être efficaces.**[40]

[40] *La fin des raccordements massifs pourrait coïncider avec la dépose du Cuivre qui constituera une opportunité pour repasser sur le terrain sur l'ensemble du réseau, et notamment sur les tronçons BLO aériens (mais la dépose du cuivre porte aussi des risques de détériorations).

## Un diagnostic de vulnérabilité en POC

Axione a lancé une démarche de Preuve de concept (POC) pour un diagnostic de vulnérabilité par rapport au changement climatique, en septembre 2022. S'inscrivant dans le cadre du décret de 2022 qui mentionne ce type de diagnostic, elle est menée avec les équipes de l'opérateur en faisant appel à une expertise externe, et concerne trois territoires aux caractéristiques différentes : Corrèze, Loire Atlantique et Vaucluse.

8 aléas sont pris en compte : vent fort, neige, fortes chaleurs, inondations, feux de forêt, retrait gonflement d'argile, retrait du trait de côte et corrosion. Il est attribué une note de sensibilité sur chaque composant et sous-composant du réseau suivant les aléas ; cette phase a été établie par une revue de littérature et de nombreux échanges avec les experts internes, ainsi qu'un examen des données d'incidents sur les réseaux de l'opérateur d'infrastructure. Le croisement avec le degré d'exposition à l'aléa permet ensuite de déterminer une note de vulnérabilité pour ces composants et sous-composants sur les différentes zones d'un territoire. On regarde par exemple le nombre de jours estimés où une ligne aérienne pourrait être affectée par de la neige collante. Les hypothèses retenues sont deux variantes des scénarios des climatologues du GIEC (4.5 et 8.5), et ce à deux échéances (2030 et 2050).

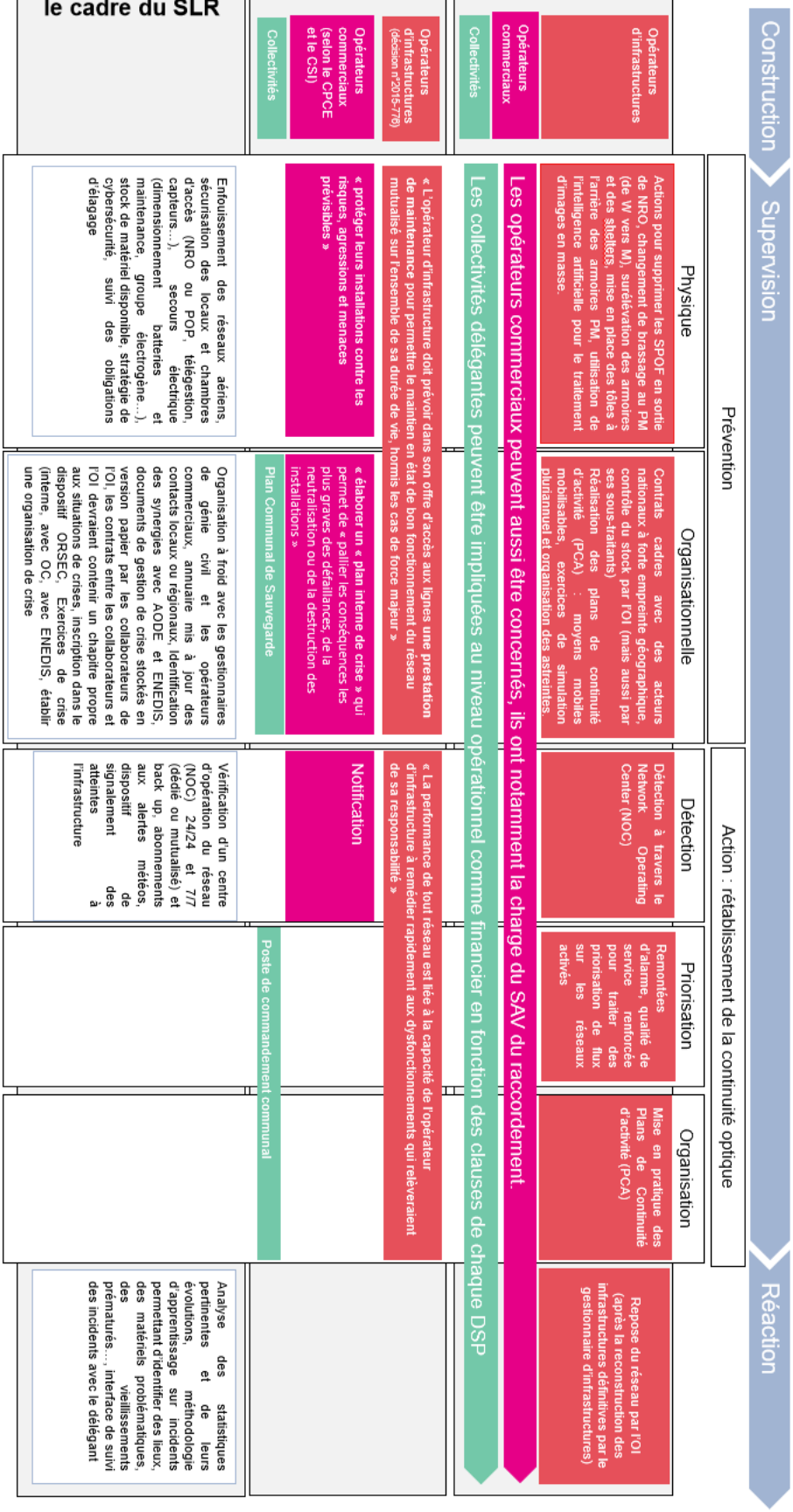
Les notes de vulnérabilité sont ensuite entrées dans le SIG afin d'obtenir une cartographie (implémentation en cours). Cela permet par exemple de visualiser les zones potentiellement inondables ou les lignes soumises à des risques de feux de forêt.

Cette vision globale permettra d'établir un tableau de bord pour prioriser les investissements à réaliser (par exemple priorités d'enfouissements…). Elle permettra aussi d'affiner la maintenance préventive, en adaptant par exemple la fréquence des passages d'inspection, en focalisant sur les endroits les plus à risques et en les allégeant ailleurs. En complément, une étude sur les données de végétalisation, menée à titre expérimental sur la Sarthe, doit permettre qu'un examen des données d'incidents sur les réseaux de l'opérateur d'infrastructure. Le croisement avec le degré d'exposition à l'aléa permet ensuite de déterminer une note de vul-nérabilité pour ces composants et sous-composants sur les différentes zones d'un territoire. On regarde par exemple le nombre de jours estimés où une ligne aérienne pourrait être affec-tée par de la neige collante. Les hypothèses retenues sont deux variantes des scénarios des climatologues du GIEC (4.5 et 8.5), et ce à deux échéances (2030 et 2050).

Les notes de vulnérabilité sont ensuite entrées dans le SIG afin d'obtenir une cartographie (implémentation en cours). Cela permet par exemple de visualiser les zones potentiellement inondables ou les lignes soumises à des risques de feux de forêt.

Cette vision globale permettra d'établir un tableau de bord pour prioriser les investissements à réaliser (par exemple priorités d'enfouissements…). Elle permettra aussi d'affiner la maintenance préventive, en adaptant par exemple la fréquence des passages d'inspection, en focalisant sur les endroits les plus à risques et en les allégeant ailleurs. En complément, une étude sur les données de végétalisation, menée à titre expérimental sur la Sarthe, doit permettre d'affiner les approches pour l'élagage réalisé par l'opérateur et le rappel des obligations d'élagage des propriétaires de terrain. Cette phase doit se terminer en septembre/octobre.

Après validation du POC, ce type de diagnostic de vulnérabilité serait étendu à tous les réseaux d'Axione, chaque territoire présentant ses propres caractéristiques.


Construction
Supervision
Réaction
Prévention
Action : rétablissement de la continuité optique
Physique
Organisationnelle
Détection
Priorisation
Organisation
Processus usuel
Opérateurs d'infrastructures
Opérateurs commerciaux
Collectivités
Actions pour supprimer les SPOF en sortie de NRO, changement de brassage au PM (de W vers M), surélévation des armoires et des shelters, mise en place des tôles à l'arrière des armoires PM, utilisation de l'intelligence artificielle pour le traitement d'images en masse.
Contrats cadres avec des acteurs nationaux à forte empreinte géographique, contrôle du stock par l'OI (mais aussi par ses sous-traitants)
Réalisation des plans de continuité d'activité (PCA) : moyens mobiles mobilisables, exercices de simulation pluriannuel et organisation des astreintes.
Détection à travers le Network Operating Center (NOC)
Remontées d'alarme, qualité de service renforcée pour traiter des priorisation de flux sur les réseaux activés
Mise en pratique des Plans de Continuité d'activité (PCA)
Repose du réseau par l'OI (après la reconstruction des infrastructures définitives par le gestionnaire d'infrastructures)
Les opérateurs commerciaux peuvent aussi être concernés, ils ont notamment la charge du SAV du raccordement.
Les collectivités délégantes peuvent être impliquées au niveau opérationnel comme financier en fonction des clauses de chaque DSP
Obligations
Opérateurs d'infrastructures (décision n°2015-776)
Opérateurs commerciaux (selon le CPCE et le CSI)
Collectivités
« L'opérateur d'infrastructure doit prévoir dans son offre d'accès aux lignes une prestation de maintenance pour permettre le maintien en état de bon fonctionnement du réseau mutualisé sur l'ensemble de sa durée de vie, hormis les cas de force majeur »
« protéger leurs installations contre les risques, agressions et menaces prévisibles »
« élaborer un « plan interne de crise » qui permet de « pallier les conséquences les plus graves des défaillances, de la neutralisation ou de la destruction des installations »
Plan Communal de Sauvegarde
« La performance de tout réseau est liée à la capacité de l'opérateur d'infrastructure à remédier rapidement aux dysfonctionnements qui relèveraient de sa responsabilité »
Notification
Poste de commandement communal
Suggestions dans le cadre du SLR
Enfouissement des réseaux aériens, sécurisation des locaux et chambres d'accès (NRO ou POP, télégestion, capteurs…), secours électrique (dimensionnement batteries et maintenance, groupe électrogène…), stock de matériel disponible, stratégie de cybersécurité, suivi des obligations d'élagage
Organisation à froid avec les gestionnaires de génie civil et les opérateurs commerciaux, annuaire mis à jour des contacts locaux ou régionaux, identification des synergies avec AODE et ENEDIS, documents de gestion de crise stockés en version papier par les collaborateurs de l'OI, les contrats entre les collaborateurs et l'OI devraient contenir un chapitre propre aux situations de crises, inscription dans le dispositif ORSEC, Exercices de crise (interne, avec OC, avec ENEDIS, établir une organisation de crise
Vérification d'un centre d'opération du réseau (NOC) 24/24 et 7/7 (dédié ou mutualisé) et back up, abonnements aux alertes météos, dispositif de signalement des atteintes à l'infrastructure
Analyse des statistiques pertinentes et de leurs évolutions, méthodologie d'apprentissage sur incidents permettant d'identifier des lieux, des matériels problématiques, des vieillissements prématurés…, interface de suivi des incidents avec le délégant

## 2.4 Les statuts spécifiques d'OIV et d'OSE

Les rôles et responsabilités des OI et des OC décrits précédemment se trouvent modifiés dans le cas où ces derniers seraient désignés comme Opérateurs d'Importance Vitale (OIV) ou Opérateurs de Services Essentiels (OSE).

*Description du statut d'OIV*

Pour se préparer aux crises majeures, le SGDSN pilote le dispositif des Activités d'importance vitale (AIV). Des Opérateurs d'importance vitale (OIV) sont désignés dans 12 secteurs d'activités par les Ministères concernés (alimentation, industrie, nucléaire, gestion de l'eau...). Chaque OIV doit remplir des obligations, parmi lesquelles :

- la désignation d'un délégué pour la défense et la sécurité ;
- la rédaction d'un Plan de sécurité opérateur (PSO) qui décrit son organisation et sa politique de sécurité ;
- l'identification des Points d'importance vitale (PIV) de ses réseaux et installations ;
- la rédaction d'un Plan particulier de protection (PPP) pour chaque PIV ;
- la rédaction d'un Plan de continuité d'activité (PCA) pour faire face à toutes sortes de crises ;
- l'obligation de s'organiser face aux menaces en termes de cybersécurité pour leurs Systèmes Informatiques d'Importance Vitale (SIIV) sous le contrôle de l'ANSSI.

Le préfet concerné localement élabore un Plan de protection externe comportant ces mesures de vigilance et d'intervention en faveur des PIV de sa zone. Il existe environ 250 OIV et 1400 PIV. Leurs listes ne sont pas publiées pour des raisons de sécurité.

Le statut d'OIV donne de fortes obligations relatives à la résilience contrôlées par l'Etat, et est plutôt orienté sur les menaces liées à la malveillance et à la défense nationale. Il est peu probable que ce statut soit donné à une collectivité exploitant directement un RIP sur un territoire ; dans le cas où un opérateur majeur est OIV, le périmètre de ses obligations ne s'étend pas nécessairement à ses filiales (sociétés de projets…), ni aux activités d'opérateur d'infrastructures. Il est néanmoins possible de s'inspirer de ce cadre, de manière proportionnée, sans en avoir l'obligation, d'autant que la directive européenne NIS 2[41] va élargir la quantité d'opérateurs soumis à des exigences. Les infrastructures numériques sont considérées comme une des 11 « entités essentielles ». NIS 2 doit être retranscrite en droit français avant le 17 octobre 2024, avec certainement une période d'adaptation pour les structures concernées.

*Description du statut d'OSE*

La réglementation distingue également les Opérateurs de services essentiels (OSE), qui vise plutôt les fournisseurs de service aux usagers et qui sont tributaires des réseaux et systèmes d'information, sur lesquels veille l'ANSSI[42].

[41] Network and Information Systems Directive https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

[42] https://www.ssi.gouv.fr/entreprise/reglementation/directive-nis/faq-operateurs-de-services-essentiels-ose/

# 3. Quelles perspectives pour le renforcement de la résilience ?

## 3.1 Positionnement des OI et des OC

Dans son « Bilan et perspectives » de juillet 2022, l'Arcep a souligné que *« la résilience des réseaux FttH face aux incidents exceptionnels et d'ampleur est un enjeu important, afin d'éviter que des interruptions de service prolongées ne viennent perturber la vie économique et sociale sur tout ou partie du territoire national ».*

L'Arcep a interrogé les acteurs sur les « mesures pertinentes pour assurer cette résilience ». L'ensemble des opérateurs d'infrastructures et commerciaux est partfaitement conscient des problématiques, des enjeux et des difficultés à surmonter. Quelques extraits de leurs contributions reprises ci-dessous montrent la diversité des sujets à traiter.

> *De façon générale, le réseau FttH repose sur des architectures qui peuvent être fragilisées par des aléas climatiques tels que tempêtes, incendies, etc. Cela pose la question de l'enfouissement de certains segments aériens à moyen terme dans les zones les plus sen-sibles. (…) (À propos d'un encadrement régulé des tarifs du GC) Un tel encadrement pluriannuel serait par ailleurs désincitatif pour Orange dans la perspective des nouveaux investissements à consentir pour assurer la résilience de ses infrastructures de génie civil, dans un contexte de plus en plus difficile s'agissant des incidents de réseaux consécutifs au change-ment climatique (inondations, incendies, tempêtes, etc.).*
>
> **Orange**

> *Altice France alerte les pouvoirs publics sur la recrudescence des actes de vandalisme ou les accidents subis ces deux dernières années sur les infrastructures des réseaux FttH, dont la liste est transmise à l'ARCEP (soumise au secret des affaires) et la nécessité d'une action conjointe des acteurs de la filière et de l'Etat pour lutter contre ces agressions, à l'instar des actions qui ont été menées pour prévenir et sanctionner les auteurs de dommages sur les antennes mobiles ces dernières années.*
>
> ***Altice France***

> *Concernant les réseaux FTTH, Altitude partage l'importance de travailler dès à présent sur la résilience et pérennité de ces réseaux mais souhaite mettre également l'accès sur la qualité d'exploitation et en particulier la bonne réalisation des raccordements. La réalisation du raccordement vient en effet achever le déploiement du réseaux FTTH et doit s'accompagner de garanties élevées en termes de qualité et de remontée d'informations afin de permettre aux OI de maitriser l'exploitation et la maintenance de leur réseau de bout en bout sur le long terme. Ce sujet est donc fortement lié à celui de la résilience qui ne concerne pas uniquement les épisodes de catastrophes naturelles. Sur ce sujet particulièrement, Altitude souligne l'importance des travaux du groupe Interop' et appelle l'Arcep à s'assurer de son bon fonctionnement. Interop' est un outil indispensable pour normaliser et assurer l'efficience des process et donc la commercialisation et l'exploitation des réseaux, aujourd'hui et pendant la phase de migration. Or, force est de constater que les OC, bien que demandeurs de la gestion de deux versions simultanées des protocoles, ne respectent pas les délais d'implémentation, au détriment de la qualité des raccordements ou de l'offre FttE par exemple (…) Compte tenu de la situation, Altitude invite l'Autorité à rester vigilante et à renforcer son implication afin de stimuler l'avancée des travaux et de veiller à maintenir des objectifs ambitieux en ligne avec l'importance et l'urgence des enjeux.*
>
> **Altitude Infrastructure**

*Deux types de mesures sont à mettre en œuvre pour renforcer la résilience des réseaux FttH, l'intégration des Opérateurs d'Infrastructures FttH dans les dispositifs de gestion de crise au niveau local et national ainsi que la préparation de Plans de Continuité d'Activités. (…) Pour assurer un niveau de résilience sur ses réseaux FttH, Axione a élaboré 6 Plans de Continuité d'Activité afin de limiter les effets directs négatifs des aléas externes d'une gravité particulière. Ils sont rédigés en fonction de la typologie des aléas : Plan crise Sanitaire, Plan de destruction des NRO, Plan tempête, Plan cyberdéfense, Plan disponibilité du SI, Plan séisme. La documentation associée détaille les différents scénarios et leurs impacts, les personnes et services mobilisés, leurs rôles et responsabilités, les critères de déclenchement et de clôture de la crise, la liste des outils et des modes opératoires. Les plans "tempête" et "destruction des NROs" intègrent notamment le pré-positionnement de NRO mobiles, de groupes électrogènes, d'équipements de secours sur les territoires, l'organisation d'astreintes et les dispositions contractuelles assurant la priorisation des moyens d'intervention en cas de crises.*
*A l'inverse, une mauvaise solution serait de laisser les opérateurs de détail réaliser directement des réparations en urgence sur le réseau de l'Opérateur d'Infrastructure FttH. En effet, les effets en termes de qualité, de mauvaise documentation des réparations et de manque de coordinations seraient bien plus important que l'éventuel gain de temps que pourrait apporter ce mécanisme.*

**Axione**

*En coordination avec les autorités nationales, en particulier le Secrétariat général de la dé-fense et de la sécurité nationale et Agence nationale de la sécurité des systèmes d'informa-tion, les opérateurs ont d'ores et déjà pris des mesures pour renforcer la résilience de leurs réseaux. Une partie des mesures publiques consistent en des réseaux auto-reconfigurables, des plans de résilience, une supervision 24/24 et la prise en compte des aléas climatiques lors de l'installation des équipements stratégiques. (…)la priorité en cas de crise majeure serait de garantir la sécurité des biens et des personnes et donc de maintenir le réseau mobile en état de fonctionnement : 95% des appels transitent aujourd'hui par le réseau mobile et non par le réseau fixe.*
*Ainsi qu'il a été exposé ci-dessus, les opérateurs ont d'ores et déjà pris des mesures pour faire face aux risques encourus d'une particulière gravité et assurer une résilience suffisante des réseaux. Les mesures proposées par certains opérateurs d'infrastructure ne relèvent absolu-ment pas de la « résilience des réseaux » mais de la « qualité de service des câblages client finaux » .*

**Bouygues Telecom**

*Nous estimons utile, que les opérateurs d'infrastructure de réseaux FttX qui accueillent des opérateurs commerciaux sur leur réseau ou dans leurs infrastructures puissent informer leurs clients des mesures et processus qui sont envisagés en cas d'aléas externes graves qui peuvent mettre en péril la continuité des services sur leur réseau. (…)*
*(A propos de l'éventualité de câbles en pleine terre) il nous semble important de prendre en compte l'évolution du contexte économique et sociétal sur le statut actuel des réseaux fixes (…) le FttH apporte des services numériques cruciaux (voire d'importance vitale) pour les utilisateurs et continue à remplacer d'autres réseaux (TNT, FM, RNT, etc.) sur les usages en position déterminée et soutient fortement l'activité économique (entreprises, télétravail, etc.).*

**Free**

> *Concernant l'enfouissement des lignes, l'ampleur des financements et des travaux à mobiliser nécessite d'établir des priorités et de commencer sans attendre qu'une catastrophe mette le dossier au-dessus de la pile. Dans le domaine de la couverture mobile, le régulateur a pu éta-blir des priorités et échéances pour les axes de transport. Afin d'assurer une meilleure résili-ence du réseau fibre mutualisé en tant qu'infrastructure de référence, l'Avicca demande que la régulation fixe un échéancier à Orange pour l'enfouissement (sites stratégiques, principales artères...) en tenant compte des zones davantage soumises aux aléas climatiques.*
>
> **Avicca**

Une lecture intégrale des contributions des acteurs est disponible[43].

## 3.2 Des dispositifs juridiques à adapter à la résilience

Afin d'appréhender globalement une politique volontariste de résilience, trois leviers juridiques sont mobilisables, autant pour responsabiliser l'OI d'un RIP que lui donner les moyens d'agir.

1. Le premier levier est le **contrat de DSP avec l'autorité délégante**. Ce contrat traite toujours de maintenance curative et préventive, d'enfouissement, de dévoiement comme de gros entretien et de renouvellement. La résilience couvrant pour partie des actions préventives (étude de vulnérabilité) ou prévisibles (moyens à mobiliser en cas de crise), y contribuer se rattache à ses obligations générales. La prise en charge des coûts induits incombe ainsi au délégataire, **mais des plafonds d'enveloppe annuelle peuvent résulter de son plan d'affaires avec pour effet de limiter son exposition pour les enfouissements et dévoiements.**
2. Le deuxième levier repose sur les **relations entre l'OI et les opérateurs commerciaux cofinanceurs**, qui devraient contribuer aux coûts d'entretien et de remplacement de 60 à 80 % des lignes FttH à très long terme.
    a. **Le cofinanceur supporte via le tarif récurrent les coûts de maintenance générale** (de l'ordre de 5,40 à 5,80 € HT/ligne cofinancée), lesquels inclut le coût d'utilisation générale et les seules opérations courantes de maintenance préventive et curative. Il doit aussi contribuer aux coûts de gros entretien/renouvellement à hauteur de son cofinancement, sans discussion avec l'OI en principe. Cet engagement de l'opérateur cofinanceur est la contrepartie de son droit d'usage de 40 ans, dans une logique proche de la copropriété.
    b. Cela étant, les offres d'accès des OI ne traitent pas de la problématique de résilience. Certaines évoquent une contribution de l'OI aux charges de dévoiement, voire d'enfouissement en les plafonnant (aux alentours de 1€/an/ligne, un volume qui correspond plutôt aux dévoiements et enfouissements à la demande de tiers), d'autres l'excluent implicitement. Leur **contribution à la reconstruction du réseau consécutive à un évènement climatique ne fait en revanche a priori pas débat.**
    c. Il n'en reste pas moins que le cofinanceur ne contribue qu'aux coûts de dépose et repose des câbles optiques, **le coût du génie civil étant couvert par son**

[43] https://www.arcep.fr/uploads/tx_gspublication/contributions-consult-bilan-perspectives-AdM-fixe-7eCycle.zip

**tarif récurrent.** Ce qui signifie que toute politique massive d'enfouissement induit une discussion entre l'OI et les gestionnaires de ces infrastructures.

3. Le troisième levier repose donc sur les **liens de l'OI d'une part avec Orange Wholesale France (OWF) au titre de l'offre d'accès au génie civil souterrain et aux appuis de l'opérateur historique et d'autre part avec les AODE (Autorité Organisatrice de la Distribution d'Energie) et les gestionnaires du réseau de distribution d'électricité (ENEDIS et les distributeurs non nationalisés).**
    a. **Prévention :**
        i. En théorie, s'agissant d'OWF, dans ses relations avec l'OI, celui-ci supporte seul les coûts des opérations d'enfouissement que lui imposent les gestionnaires de voirie, sans appeler l'OI ni les opérateurs commerciaux à y contribuer.
        ii. En pratique, ces opérations d'enfouissement mobilisent aussi des contributions des gestionnaires de voirie, le plus souvent des communes ou des EPCI qui entendent enfouir les lignes pour des raisons esthétiques. Des départements peuvent aussi l'imposer pour des impératifs de sécurité routière. La dimension de résilience des réseaux télécoms n'est jusqu'ici pas à l'origine de l'enfouissement.
        iii. En outre, ces opérations sont le plus souvent coordonnées avec « l'effacement » du réseau de distribution électrique, lui aussi sollicité par les communes le plus souvent. Ces opérations sont donc co-financées par plusieurs acteurs dans le cadre posé par le conventionnement AMF/Orange initié en 2005 et actualisé en janvier 2012, les coûts propres au génie civil télécom étant partagés entre la commune et Orange, en fonction de la propriété du génie civil créé. L'AODE comme le gestionnaire du réseau électrique sont rarement à l'origine de ces opérations d'effacement.
        iv. Il faut en retenir qu'il existe un dispositif d'enfouissement éprouvé des infrastructures supports des réseaux télécom qui mobilise financièrement les communes et OWF. L'OI et les OC y contribuent indirectement via le tarif de l'offre iBLO qu'ils supportent conjointement. Ce dispositif ne répond pas toutefois à la logique de résilience : il vise avant tout à enfouir des réseaux en centre-bourg et non de grands linéaires de tronçons de transport ou de collecte. Une politique d'enfouissement volontariste ne pourra pas reposer sur les seules enveloppes annuelles existantes. Par ailleurs, aucune politique d'enfouissement préventif d'OWF n'est attendue du 7ème cycle d'analyse de marché au titre des autres opérations de maintenance ne relevant pas de rénovation ou de réparation[44].
    b. **Action :** A titre curatif ensuite, s'agissant du réseau d'OWF, le process n'est pas adapté en cas de crise, notamment en termes de prévenance, de délais d'intervention, ou encore de périmètre de responsabilité entre l'OI et OWF**.** En cas d'urgence, l'OI ne peut intervenir lui-même pour réparer que si OWF dépasse son délai de réponse à la demande d'intervention de 5 jours ouvrés, réponse dans laquelle il doit indiquer les conditions et délais de réparation.

[44] ARCEP, Projet de décision d'analyse du marché de fourniture en gros d'accès aux infrastructures physiques de génie civil de boucle locale, 20 février 2023, p. 54.

L'analyse de marché en cours ne devrait pas substantiellement modifier ces conditions d'intervention de l'OI sur le génie civil d'OWF. En outre, la rémunération par OWF des interventions effectuées par l'OI pour son compte pourrait se traduire par une meilleure couverture des coûts de ce dernier, avec une mention du remboursement par OWF « des coûts efficaces », censés tenir compte du renchérissement du coût des opérations ponctuelles, surtout réalisées en urgence.[45]

## 3.3 Les travaux collectifs pour renforcer la qualité et la résilience

Par construction, les opérateurs de communications électroniques sont obligés de coopérer tout en étant concurrents. L'abonné de l'un doit pouvoir joindre celui d'un deuxième en passant peut-être par le réseau d'un troisième etc. Cette nécessité est renforcée sur les réseaux FttH, du fait qu'il y a plusieurs Opérateurs d'infrastructure et aussi une obligation de cofinancement. Concrètement plusieurs instances sont à l'œuvre :

- Les « multilatérales » organisées par l'Arcep sur des sujets au long cours, avec les opérateurs concernés ;
- Le Comité d'experts fibre, qui réunit opérateurs, équipementiers, associations de collectivités etc. Il est réuni sous l'égide de l'Arcep qui en publie les recommandations ;
- Inter'op fibre, qui réunit les opérateurs, a pour objectif de normaliser les échanges d'informations et d'harmoniser les processus entre opérateurs dans trois domaines de la mutualisation FTTH, l'infrastructure, l'accès et le SAV ;
- Objectif fibre, qui réunit notamment des fédérations professionnelles, s'est axée sur la publication de guides concernant la fibre dans les bâtiments et la formation professionnelle ;
- Les fédérations professionnelles, principalement la Fédération française de télécoms (FFT) et InfraNum, ainsi que les associations de collectivités Avicca et FNCCR, qui mutualisent les bonnes pratiques au sein de leurs membres et les représentent auprès des instances nationales (gouvernement, législateur, régulateur…) ;

[45] ARCEP, Projet de décision d'analyse du marché de fourniture en gros d'accès aux infrastructures physiques de génie civil de boucle locale, 20 février 2023, p. 52 à 53.

- Le CREDO, qui réunit des personnes expertes et impliquées, a publié de nombreux guides sur la qualité et la pérennité des réseaux.

Jusqu'ici les travaux ont porté sur la **qualité des réseaux, une base essentielle de la résilience.** A titre d'exemples, le comité d'experts fibre a recommandé un changement dans le lovage pour les Points de mutualisation, InfraNum met en avant la rémunération des intervenants pour assurer la qualité des raccordements et publie des études sur la résilience, l'Avicca a fait développer Grace THD, modèle conceptuel de données qui permet d'assurer l'interopérabilité des données d'informations géographiques concernant le référentiel de l'infrastructure de génie civil et des réseaux fibre optique déployés, Objectif fibre actualise régulièrement son guide sur les raccordements à destination des promoteurs et propriétaires etc.

**Ces instances contribuent ainsi activement à une « soft law » qui permet des avancées consensuelles, mais elles aussi butent parfois sur l'absence de volonté de certains acteurs pour participer ou d'obligations dans leur mise en œuvre effective.**

Si des retours d'expérience de gestion de crise ont fait occasionnellement l'objet d'échanges en « multilatérale FttH », **le sujet « résilience » n'est pas encore abordé dans toutes ses dimensions dans les instances d'échanges entre les acteurs.** À notre connaissance, aucun exercice de simulation de crise entre un OI, Orange pour son génie civil, ENEDIS pour le sien, et les différents OC, n'est en discussion.

03

# Le schéma local de résilience

**Des schémas locaux de résilience nécessaire :** si des travaux nationaux sont indispensables pour renforcer la résilience des réseaux FttH, des actions locales sont aussi nécessaires, y compris dans ce cadre encore imparfait. Des actions ne dépendent pas de la partie mutualisée du réseau, et sont déjà dans les mains des collectivités délégantes, comme des interconnexions de réseaux, bouclages de collecte, extension de FttO, organisation interne de crise etc. Certaines mesures sont extrêmement couteuses, d'autres peu tout en étant fondamentales, comme les améliorations d'organisation ; aussi est-il impératif de dégager une vue d'ensemble, se projeter dans le temps et établir des priorités. Ceci est d'autant plus vrai que les aléas, en particulier climatiques, augmentent, et que les usages du réseau croissent et se qualifient inéluctablement, multipliant ainsi les risques.

Diversité des plans locaux de résilience : au choix de la collectivité, le champ du schéma local de résilience peut couvrir les divers réseaux FttH de son territoire, publics et privés ou seulement ceux dont elle est délégante ou en charge directe. Il est bien évident que les outils à disposition pour diagnostiquer et améliorer la résilience ne sont pas les mêmes selon que la responsabilité dépende d'un service public géré directement, délégué, ou entièrement privé.

**La stratégie doit être coordonnée avec l'OI** : dans tous les cas, l'association, indispensable, des OI à la démarche sera d'autant facilitée que la collectivité se positionne pour accompagner les acteurs dans leur responsabilité propre (enfouissements coordonnés, appui à l'identification des risques etc.). Par commodité dans ce qui suit, il est fait référence à l'OI au singulier, la démarche devant se démultiplier auprès de chacun d'entre eux s'ils sont plusieurs, avec bien évidemment des degrés de précision différents suivant les cas de figure.

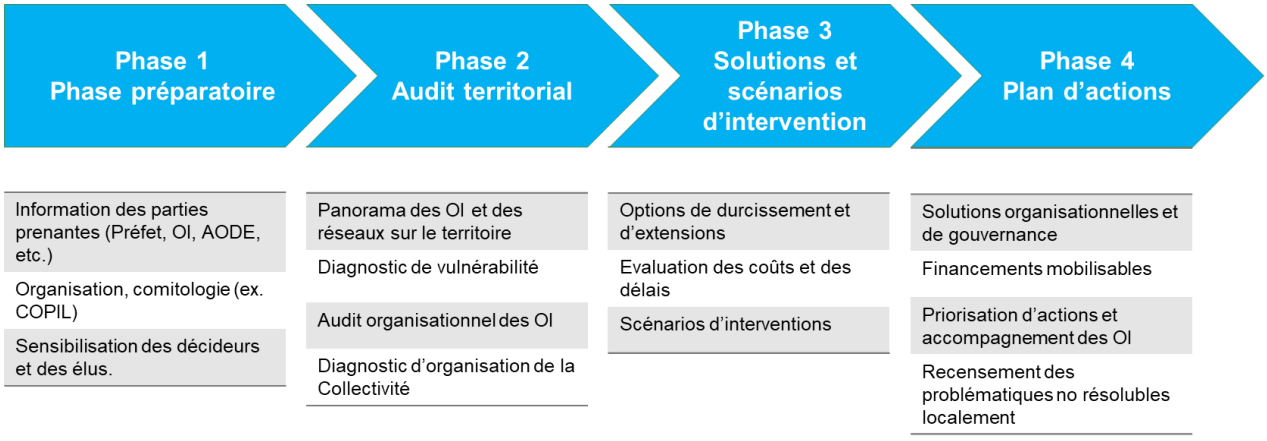
**Proposition de la Banque des Territoires**

Le département « Transition numérique » de la Banque des territoires peut accompagner financièrement la réalisation d'un schéma local de résilience, comme elle a aidé à des stratégies de développement des usages et services, ou des schémas directeurs territoriaux d'aménagement numérique.
Le schéma local de résilience peut être réalisé en interne, ou faire appel en tout ou partie à des prestataires. Certains chapitres ou certaines précisions devront en rester confidentielles, afin de ne pas créer de risques supplémentaires (malveillance, par exemple). Les éléments listés ci-dessous ne sont pas exhaustifs. Leur importance peut être variable suivant les territoires, dont certains sont sujets à des risques avérés récurrents par exemple (vents forts en zone littorale, cyclones, neige abondante…), ou doivent compter sur leurs propres forces (situation insulaire, éloignement de la métropole…).

**NB : la rédaction ci-dessous se base sur le cas le plus fréquent, à savoir que la collectivité n'est pas l'opérateur d'infrastructure (OI privé ou en délégation).** Les points d'attention sont bien entendu les mêmes, avec un basculement vers un diagnostic interne et l'interrogation des prestataires qui appuient la collectivité agissant en tant qu'OI dans certaines missions. Il est précisé que le cadre ci-dessous est général, et que les approches méthodologiques des bureaux d'étude qui effectueront ces schémas permettront sans aucun doute de répondre aux objectifs fixés.

Plusieurs collectivités se sont déjà lancées dans des schémas de résilience pour leurs réseaux FttH, notamment **Haute-Garonne Numérique** et Gironde Numérique. La **Collectivité territoriale de Corse** mène une réflexion plus globale concernant également le mobile, l'électricité et l'Internet des objets, en rapport avec son insularité et les discussions en cours sur son autonomie. Les apports des premiers travaux de terrain sur ces questions enrichiront sans aucun doute les présentes réflexions.

L'élaboration d'un schéma local de résilience peut se décliner différemment en fonction des territoires, elle peut se mener en phases successives :




## 1. Phase préparatoire

Afin de préparer et organiser la mission d'élaboration du schéma local de résilience, il convient d'identifier les personnes et organismes à **associer au comité de pilotage** ou ponctuellement (directions de la collectivité ou d'autres collectivités en rapport avec l'adaptation au changement climatique, direction des routes, AODE, etc.). Disposer d'une bonne vision des aléas du terrain justifierait d'impliquer **les EPCI**, qui disposent d'une vision fine du territoire via l'exercice de leurs compétences en matière d'urbanisme et de gestion des milieux aquatiques et de prévention des inondations. L'information sur les objectifs poursuivis et le déroulement doit cibler **les institutions et acteurs locaux** (préfet et ses services, collectivités concernées, opérateurs d'infrastructure, distributeurs d'électricité, etc.)., Il peut également être utile d'informer des **acteurs nationaux** de la démarche (Arcep, ANCT, etc.).

## 2. Audit territorial

### 2.1 Panorama des OI et des réseaux sur le territoire

Une **cartographie des OI et des réseaux** présents sur le territoire permet de rappeler les différentes entités responsables.

Pour le ou les OI concernés par le SLR, la volumétrie de lignes et abonnés et le recensement des principaux utilisateurs finaux permet de cerner les impacts potentiels de crises. Il est aussi utile pour informer les décideurs sur l'importance de la résilience du réseau, qu'ils soient en charge du réseau (ex. délégant), de la sécurité civile (préfet, maires, etc.), ou responsables politiques d'un territoire (président.e de Région, de Conseil départemental, etc.). A minima, il peut comporter des données à date et des prévisions à l'échéance de l'extinction du cuivre ou de projets de déploiements de services complémentaires :

- Nombre de lignes raccordables ;
- Nombre de clients grand public et professionnels ;
- Nombre de clients entreprise ou service public avec QoS ;
- Utilisateurs s'appuyant sur l'infrastructure de collecte (GFU mairies, collèges, lycées, hôpitaux, recherche ; backhaul objets connectés ; vidéoprotection ; sites mobiles, etc.).

Il peut s'accompagner utilement d'une cartographie de couverture et de synoptiques du réseau. Ces éléments seront d'autant plus parlants qu'ils permettront de hiérarchiser (par exemple nombre d'abonnés potentiels derrière un NRO ou classes de NRO…). Il est également utile d'identifier les réseaux FttO présents pour voir là où les établissements importants peuvent opter pour un double accès, et s'assurer des mécanismes de résilience de ces réseaux FttO s'ils sont utilisés par des services publics.

Cette récapitulation des enjeux peut s'avérer utile pour convaincre, si nécessaire, les autorités préfectorales d'inclure les opérateurs d'infrastructure et leurs autorités délégantes dans le dispositif Orsec. Le recensement peut permettre d'identifier des sites prioritaires, en relevant toutefois que ce sont les opérateurs commerciaux qui ont la connaissance de leurs clients ; un raccordement sur un site peut concerner aussi bien le logement du gardien que l'équipement informatique, rien n'obligeant l'OC à déclarer l'importance d'une liaison, ni même à souscrire une GTR sur la fibre pour vendre lui-même une GTR. Le dispositif préfectoral de crise comporte déjà l'identification de sites prioritaires dans le dispositif ORSEC. Il ne s'agit ni de le doublonner, ni de multiplier à l'infini les priorités qui du coup n'en sont plus, mais de voir s'il est possible de compléter la liste par les éléments connus de l'OI et de la collectivité (par exemple GFU, vidéoprotection…).

**Demande des informations des réseaux aux OI**

En plus des informations de volumétrie et de qualification sur leurs utilisateurs, les OI détiennent les informations sur leurs réseaux, la gestion des crises et la stratégie sur la résilience. La collectivité aura d'autant plus de facilité à obtenir ces documents qu'il s'agira de réseaux d'initiative publique. La collectivité sera particulièrement intéressée par la connaissance de l'existance et la communication par les OI des documents suivants :

- Architecture du réseau et de ses interconnexions
- Plans de continuité et de reprise d'activité (PCA, PRA)
- Etat et actions concernant la résilience (ex. diagnostic de vulnérabilité)

## 2.2 Diagnostic de vulnérabilité

Le diagnostic de vulnérabilité[46] doit permettre d'identifier les aléas, leurs occurrences et évolutions probables, et leurs impacts sur chaque élèment des réseaux. Il porte essentiellement sur le réseau FttH (ou FttO), et prend en compte les interdépendances avec les autres réseaux (principalement électrique). Un même réseau peut concerner des portions de territoires soumis à des aléas très différents.

Pour les aléas climatiques, au-delà des données existantes à prendre en compte, il peut être utile de se projeter sur le moyen terme en rapport avec des **scénarios du GIEC**.

Il s'agit ensuite de localiser les éléments de réseau qui pourraient être davantage impactés, via une notation de sensibilité en fonction des aléas (passage d'artère en aérien dans une zone boisée ou un couloir de vent, implantation d'un PM dans une zone fréquemment inondable, NRO sans vidéoprotection, chambres d'accès à des POP non sécurisées, absence de bouclage de collecte sur un NRO…), en hiérarchisant en fonction de l'impact potentiel (collecte, transport, distribution, lignes concernées, risques de durées d'indisponibilités).

[46] La loi Climat et Résilience donne aux préfets la possibilité d'imposer des diagnostics de vulnérabilité. Nous gardons ici le même terme pour l'ensemble des risques, et pas seulement ceux liés aux aléas climatiques.

Pour d'éventuels enfouissements sur la partie « distribution », il est utile de distinguer les parcours « interbourgs » des « intrabourgs », plus coûteux, davantage en antenne (embranchements multiples) et avec un impact complexe sur le raccordement des parcelles privatives. Une quantification approximative est possible avec la taille des câbles, mais compte-tenu de leur modularité granulaire, il est plus précis de raisonner en termes de nombre de locaux concernés (à savoir les prises, à terme, y compris, voire, si des données sont disponibles, sur des zones en cours de fortes urbanisations). Une approche plus qualitative peut compléter ces éléments, par le repérage de sites d'entreprises ou de services publics importants en aval, sites SEVESO, sites sensibles ANSII, de collecte de site mobile etc.

Ce **diagnostic de vulnérabilité peut être simplifié si l'OI a déjà réalisé une telle étude qui pourrait alors être simplement auditée ou actualisée** (voir ci-dessous).

Des visites sur place, sur les points principaux et/ou par échantillons, sont utiles. À titre d'exemples réels, des tournées d'inspection ont déjà montré des pratiques dangereuses (stockages de cartons vides dans des NRO…), des configurations à risque (NRO en shelter sans glissière de sécurité mais implanté dans un lieu avec risques forts de percussion par un véhicule, tuyau de climatisation passant au-dessus de baies…).

Il sera nécessaire de prendre en compte a minima l'évolution de l'état de l'art, qui aura pu évoluer depuis la construction du réseau (par exemple l'intérêt de serrures connectées testées actuellement sur des PM), ou des novations qui semblent pertinentes à l'initiative d'un OI ou d'une collectivité présentant des similarités.

**Des spécificités à actualiser pour chaque territoire**

Les caractéristiques de chaque territoire sont à prendre en compte. Exemples concrets :

- Haute-Garonne Numérique : la canicule de 2022 a montré les risques accrus d'incendie, mais aussi la température de portes métalliques de NRO montant à 60°, et les climatisations sollicitées en permanence, avec la question de leurs limites de capacités dans l'avenir, sans parler des difficultés humaines d'intervention en période longue de canicule.

- La Réunion : le déploiement du FttH engendre une augmentation considérable du transit longue distance. Il en résulte que la sécurisation qui semblait assurée par l'existence de deux câbles sous-marins distincts n'est plus garantie, car le plus ancien ne peut supporter la totalité du trafic. Or les câbles sous-marins peuvent être victimes d'arrachements, par exemple à cause d'ancres près des côtes africaines, ce qui arrive près d'une fois par an en moyenne, mais aussi être endommagés par des éruptions sous-marines, avec plusieurs occurrences en vingt ans, et un délai de réparation qui se compte en mois.

## 2.3 Audit organisationnel des OI

### ***Champ de l'audit***

**Pour les réseaux en Délégation de service public**, le respect des prescriptions contractuelles initiales qui pourraient avoir un impact sur la résilience est supposé avoir été acté dans le processus de réception du réseau par la collectivité concédante ou agissant en marchés de travaux (modulo les difficultés spécifiques des modalités de raccordement de l'usager final). De même, un éventuel audit technique du réseau peut être un préalable dans certains cas, mais ne fait pas à proprement parler partie d'un schéma local de résilience.

**<u>Dans le cas des RIP</u>, l'audit et ses conclusions ont des limites, car si la collectivité a un pouvoir de contrôle, le délégataire conserve une autonomie dans son fonctionnement.**

Ainsi que développé plus haut, en ce qui concerne particulièrement les risques naturels, **la résilience propre du génie civil** (état, moyens et dispositifs de crise, investissements préventifs…), **ainsi que l'articulation entre les gestionnaires du génie civil souterrain et aérien que sont Orange et ENEDIS d'une part, et l'OI d'autre part, sont des éléments essentiels.** Cependant, ils ne peuvent pas être audités directement par une collectivité, et ne seront appréhendés que dans les limites de la relation contractuelle avec l'OI, et via celui-ci.

Le SLR s'intéresse à ce qui se passe avant, pendant et après les crises au niveau de l'OI. **Tout ou partie des items suivants peuvent être déjà traités dans les rapports annuels.**

## ***<u>Préparation aux crises</u>***

Le SLR peut passer en revue tous les éléments qui concourent à diminuer les impacts d'une crise en s'y préparant, notamment :

- Organisation « à froid » avec les gestionnaires de génie civil (Orange, ENEDIS GC, procédures standards ou précisées localement), avec les opérateurs commerciaux, annuaire mis à jour des contacts locaux ou régionaux (ENEDIS, direction des routes…), etc.
- Diagnostics de vulnérabilité et Plans de continuité d'activité (PCA) ;
- État d'avancement de l'inscription de l'OI dans le dispositif ORSEC (dont liens avec les opérateurs d'autres types de réseaux, autorités locales…) ;
- Centre d'opération du réseau (NOC) 24/24 et 7/7 (dédié ou mutualisé) et back up ;
- Secours électrique (dimensionnement batteries et maintenance, groupe électrogène…) ;
- Sécurisation des locaux et chambres accès NRO ou POP (badges, vidéoprotection, autorisation d'accès à distance…), télégestion, capteurs…
- Ingénierie (tubes dédiés…) et documentation du réseau permettant de prioriser des sites, les abonnés avec QOS ;
- Abonnements aux alertes météo et crues, capteurs etc.
- Moyens disponibles : stocks de matériels de remplacement localement ou régionalement via l'OI ou les gestionnaires de génie civil en contrat avec l'OI (poteaux, attaches, câbles, armoires PM, PBO, activation, NRO mobile…), matériels d'intervention (nacelles, groupes électrogènes…), astreintes, moyens humains internes mobilisables, contrats de prestataires mobilisables ;
- Exercices de crise (internes, avec les OC, avec Orange et ENEDIS…) ;
- Organisation de crise (cellule locale ou régionale, procédures d'escalade vers le national, dispositif de communication, articulation avec le délégant…) ;
- Projets d'investissements préventifs (en propre et avec les cofinanceurs) ;
- Assurances.

## ***<u>Dispositifs et pratiques concourant à la résilience</u>***

Les dispositifs qui améliorent la qualité de service au quotidien et le traitement des incidents courants seront évidemment utiles en cas de véritable crise. Ils peuvent donc entrer éventuellement dans le scope d'un audit, par exemple :

- Analyse des statistiques de QoS pertinentes et de leurs évolutions (taux de non-délai de rétablissement par segment, délai moyen de rétablissement, taux de respect des

interruptions, maximum de services pour les offres avec QoS, interruption maximum de service annuelle…) ;

- Stratégie de cybersécurité (protection de l'infrastructure et des données, surveillance des anomalies, formation du personnel…)
- Dispositif de signalement des atteintes à l'infrastructure47 (site, application mobile…) ;
- Méthodologie d'apprentissage sur incidents permettant d'identifier des lieux (carrefour accidentogène sur PM, traversée aérienne de route …), des matériels problématiques (attaches…), des vieillissements prématurés…
- Suivi des obligations d'élagage ;
- Interface de suivi des incidents avec le délégant.

## 2.4 Diagnostic organisationnel de la Collectivité

Une analyse des clauses contractuelles de la délégation de service public est indispensable pour évaluer les obligations de moyens, les possibilités d'utilisation de fonds de gros entretien/gros renouvellement, la clause de retour à meilleure fortune, les possibilités de contrôle, etc.

La collectivité, surtout s'il s'agit de la collectivité délégante, est partie prenante, tant en aval qu'au moment des crises et après. Il n'est pas besoin de rappeler que la population se tourne toujours vers ses élu.e.s de proximité, et ils le feront d'autant plus qu'il s'agit d'un réseau d'initiative publique. L'aspect « communication de crise » rend indispensable une articulation étroite avec celui qui sera au centre des informations et des actions, l'Opérateur d'infrastructure. Comment est-elle actée, avec quelles cibles (mairies, presse…), quel.le(s) porte-parole(s), au sein de quelle cellule de crise, toutes ces questions peuvent être abordées « à froid ».

**Identification des synergies avec les acteurs du territoire**

Comme dans toute bonne analyse SWOT[48], outre les forces, faiblesses et menaces, le territoire recèle des opportunités à identifier et utiliser.

Les Régions et Départements peuvent mener des politiques d'adaptation au changement climatiques. Certaines collectivités et groupements mettent en place des dispositifs de suivi et d'alertes sur les crus complétant ce qui est centralisé au niveau national.

Les Autorités organisatrices de la distribution d'énergie (AODE) et ENEDIS sont des partenaires incontournables en matière d'enfouissement, et d'identification de sites prioritaires. Côté malveillance, une convention a été signée en 2021 entre le ministère de l'Intérieur et les opérateurs, pour favoriser les échanges avec les acteurs de la sécurité (police, gendarmerie) ; elle est précisée à l'échelle des départements, via les préfectures. La connaissance fine du territoire permet de signaler à l'OI des opportunités complémentaires à ses moyens propres ou à ses prestataires, par exemple l'existence d'un loueur de camion-nacelle etc.

[47] Voir par exemple https://nathd.fr/declarer-un-dommage-reseau/

[48] Strenghts Weaknesses Opportunities Threats, ou forces, faiblesses, opportunités, menaces.

**De multiples initiatives**

Vendée Numérique suit la constitution du jumeau numérique de la Vendée, et envisage de l'utiliser pour suivre l'évolution de la végétation, afin d'affiner sa gestion de l'élagage. Le suivi de la croissance de la végétation pourrait permettre de cibler les actions, en géolocalisant les sections, et en croisant avec le volume de locaux impactés. Lié aussi à ce futur jumeau numérique, le SDIS est partenaire d'un projet européen « resil coast », qui vise à étudier les risques submersion ; il est possible que cela concerne la préservation des réseaux FttH également.
La Corrèze a formé ses agents d'entretien des routes pour détecter des problèmes sur le réseau FttH aérien et les signaler précisément[49] sur le site mis en place par Nouvelle Aquitaine THD notamment en direction des collectivités[50].
Des outils d'identification des besoins d'élagage et de l'état des poteaux, faisant appel à des caméras embarquées sur des véhicules parcourant le territoire et une modélisation d'intelligence articielle, ont été développés par des sociétés françaises et utilisées par certains OI.

# 3. Solutions et scénarios d'intervention

## 3.1 Options de durcissement et d'extensions

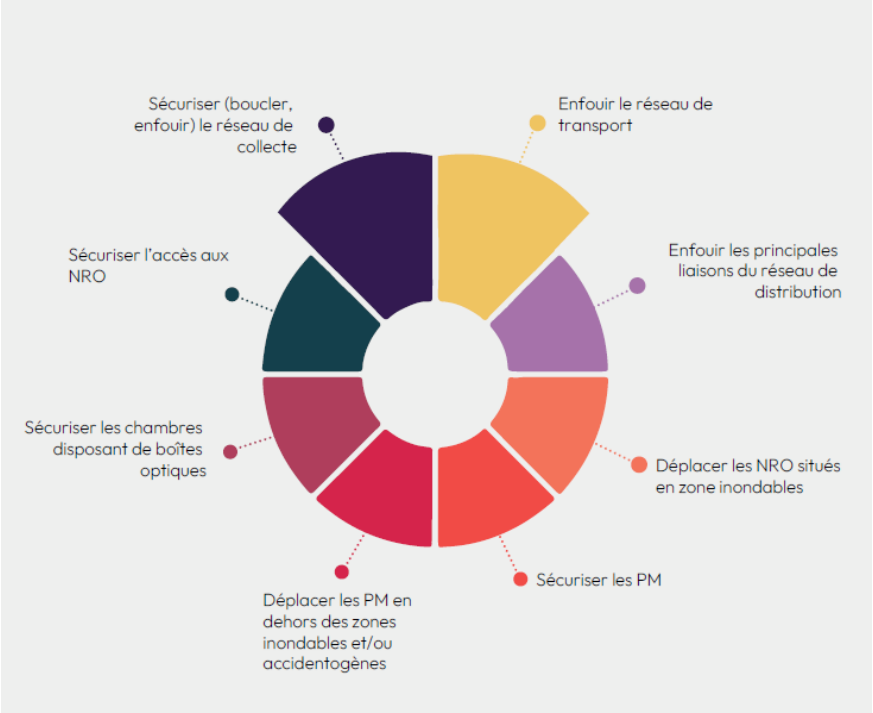
Afin de présenter des éléments aux décideurs pour les choix à effectuer, il est bien entendu nécessaire d'établir un **catalogue chiffré estimatif des mesures qui apparaissent pertinentes**.

Si cela est possible, l'analyse **s'appuie sur l'incidentologie du réseau** (voir ci-dessus dans l'audit de l'OI) qui peut pointer sur des zones à risque du fait de conditions environnementales particulières ou de fragilités de matériel (vétusté, composants inadéquats, usure prématurée due à une mauvaise utilisation par des intervenants sur le réseau…).

**Types d'investissement** : il peut s'agir d'opérations globales (vidéoprotection de tous les NRO…), sélectives par seuils (enfouissement des artères de transport de plus de x ou y lignes), balancées (traiter 20% des cas permet d'atténuer 80% des problèmes, suivant le principe empirique dit de Pareto), ou carrément ponctuelles (réhausse d'un NRO, déplacement d'un PM en zone avec forte probabilité d'inondation, bouclage de collecte en fond de vallée…).

**Cadre des investissements :** les éventuels investissements concernent autant que nécessaire la partie proprement FttH au sens du réseau mutualisé, mais aussi les autres segments en amont (collecte, interconnexions avec d'autres réseaux de collecte, POP, éventuellement longue distance), voire les extensions de RIP FttO. Le cas échéant, suivant la commande de la collectivité, cette partie du diagnostic identifie des sites publics prioritaires et chiffre leurs coûts de raccordement de ses sites publics par un accès distinct du FttH.

[49] https://www.correze.fr/actualites/centre-dentretien-des-routes-des-batiments-et-de-la-fibre-de-beynat/print
[50] https://nathd.fr/declarer-un-dommage-reseau/.




*Exemples de solutions de durcissement des réseaux*
*(cf. étude Infranum-Banque des Territoires sur la résilience des infrastructures numériques)*

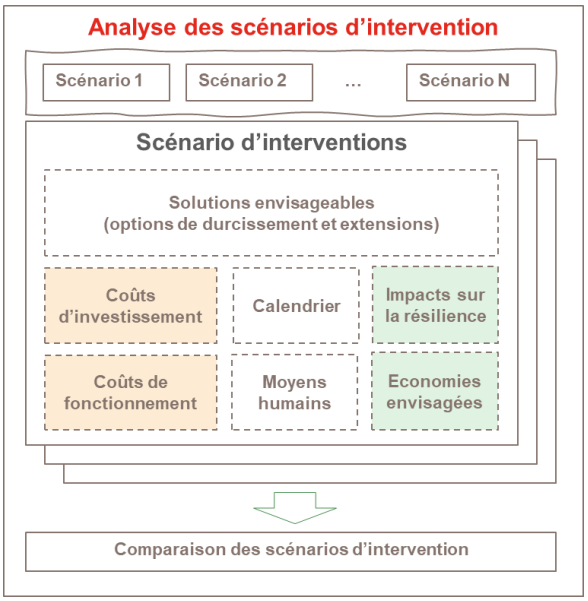
## 3.2 Evaluation des coûts et des délais

Les coûts d'investissement et de fonctionnement seront estimées pour les différentes mesures analysées. Il ne s'agit pas à ce stade d'avancement de devis précis mais des évaluations permettant de comparer les différentes solutions entre elles et de procéder à une hiérarchisation des actions qui aura lieu respectivement dans l'analyse des scénarions d'intervention et dans l'établissement du plan d'actions.

Il convient également d'estimer d'éventuelles économies engendrées (propriété du GC ou collecte versus location…), ou les revenus de services qui pourraient enrichir le catalogue de l'OI si la résilience était améliorée (par exemple possibilité d'étendre les zones où il est possible de proposer des offres de constitution de GFU). Autant que possible, en face de chaque groupe de dépenses doit figurer l'amélioration attendue (NB sur la résilience en cas de crise, mais sans doute d'abord sur la qualité de service au quotidien).

## 3.3 Scénarios d'interventions

Sur la base des diagnostics effectués, le SLR établit un ou plusieurs scénarios d'investissements suivant différents degrés d'ambition, le cas échéant par itérations.




# 4. Plan d'actions

Des phases de pédagogie et de concertations, éventuellement itératives, doivent permettre d'effectuer des arbitrages sur les scénarios retenus, les problèmes et solutions diagnostiquées, aboutissant à des décisions de court, moyen et long terme.

Le plan d'actions comporte des mesures d'investissement et d'organisation.

## 4.1 Solutions organisationnelles et de gouvernance

Les décisions peuvent porter notamment sur :

- La gouvernance de crise (seuil de déclenchement, composition de la cellule de crise et de la cellule de communication, fonctionnement avec l'OI, porte-parolat, outils de communication avec le grand public, la presse, les maires, le Conseil départemental ou régional, les AODE…) ;
- L'insertion dans le dispositif Orsec ;
- Le suivi périodique des aléas (ils sont régulièrement réévalués, 5 ans pour les PPRI par exemple), à croiser avec l'actualisation régulière des enjeux (quantification et qualification des utilisateurs, schéma du réseau…) ;
- La mise à jour régulière des contacts, suivi de la réglementation, des bonnes pratiques, des retours d'expérience et expérimentations d'autres OI et collectivités ;
- Le montage d'exercice de crise ;
- Les partenariats (anticipation des enfouissements avec les AODE, contrat local avec les forces de l'ordre…) ;

- Actions sur les sites critiques de la collectivité (redondance des accès, etc.) ; sensibilisation des utilisateurs du territoire sur le sujet (via CCI, SM, etc.).

## 4.2 Financements mobilisables

La structure qui peut supporter les coûts est variable suivant les montages (concession, affermage ou régie) et les segments de réseau (partie mutualisée ou non), joue sur les financements mobilisables :

- Fonds propres du délégataire ou du délégant ;
- Aides d'une collectivité tierce ;
- Cofinancement éventuel sur la partie mutualisée du RIP ;
- Marges de manœuvres du contrat de délégation (réserves employables, allongement de la durée…) ;
- Prêts[51]

Éventuels fonds spécifiques pour faire face aux changements climatiques, régionaux, nationaux, européens.

**Des mécanismes nationaux pour financer la résilience ?**

La solidarité nationale et européenne a déjà joué pour contribuer à l'enfouissement et la reconstruction des réseaux, comme à Saint-Martin, dévastée par l'ouragan Irma[52]. L'Avicca, la FNCCR et InfraNum réclament la mise en place effective d'un Fonds d'Aménagement Numérique du Territoire dont l'une des priorités serait de contribuer à l'augmentation de la résilience des réseaux.
Au chapitre financièrement important de l'enfouissement des réseaux, des réflexions sont en cours autour de la création d'un véhicule financier national permettant d'agir sur les lignes prioritaires et d'en répartir les coûts via les mécanismes existant d'utilisation du génie civil d'Orange, ce qui permettrait ainsi une péréquation nationale.

## 4.3 Priorisation d'actions et accompagnement des OI

En fonction des possibilités de financements qui peuvent être réunies, il en résulte, a minima, un arbitrage de la collectivité sur une priorisation des travaux de durcissement à financer et à réaliser, **en distinguant ce qui est à la charge de la collectivité et/ou de l'OI, en spécifiant d'éventuelles urgences.**

L'exercice peut aller jusqu'à un Plan d'investissements à moyen terme sur les financements qui sont établis. Plus probablement ou de surcroit, l'objectivation des risques, avec leurs conséquences (coûts de rétablissement, pertes de recettes…) ainsi que la hiérarchisation des investissements à réaliser doivent permettre d'engager un dialogue avec

[51] Voir notamment https://www.banquedesterritoires.fr/resilience-securisation-physique-des-reseaux

[52] SAS Tintamarre, opérateur de fourreaux créée à l'initiative de la collectivité, de la Banque des Territoires et de Dauphin Telecom Infrastructure pour construire 72 km de génie civil, avec une aide de l'État de 5 M€ et du FEDER de 1,5 M€.

l'OI et/ou entre l'OI et ses cofinanceurs pour aboutir à programmer les investissements nécessaires.

Les clauses génériques des délégations de service public et les contrats signés donnent déjà un cadre permettant de suivre la problématique de la résilience, par exemple avec les rapports annuels, suivis d'incidents etc. Le SLR peut élaborer des précisions à négocier (actualisation de diagnostics de vulnérabilité, etc.). La mise en place de moyens d'intervention d'urgence relève en principe des obligations d'OI.

En complément des financements mobilisables (cf. section précédentes), il est intéressant d'explorer la possibilité d'orienter des enveloppes non consommées (gros entretien/renouvellement, opérations de dévoiement, etc.) voire une clause de retour à meilleure fortune aux fins d'investissement dans les priorités de la résilience, en concertation avec l'OI. La recherche de financements peut aller jusqu'à envisager un allongement de la durée contractuelle si cela permet des investissements nécessaires et conséquents (en rapport avec le Plan d'affaires initial, et dans les limites de la jurisprudence bien entendu).

La proposition d'un **plan d'actions techniques et organisationnelles**, listant les actions, les moyens nécessaires (humains, techniques, financiers) et le calendrier associé est un livrabl essentiel du schéma local de résilience. Toutefois des actions estimées souhaitables peuvent ne pas être priorisées dans une première version du SLR faute de financements suffisants ou dans l'attente de projets techniques au niveau national ou d'évolutions réglementaires.

## 4.4 Recensement des problématiques non résolubles localement

Les éléments recueillis lors de l'établissement du schéma local de résilience ne peuvent pas tous donner lieu à une action locale (par exemple sur les possibilités d'articulation OI/OC ou OI/gestionnaires de génie civil en cas de crise, la solidarité des cofinanceurs en prévention, d'éventuelles difficultés juridiques ou administratives à s'intégrer dans un plan Orsec…). Suivant la nature des sujets et leur gravité, et au choix de la collectivité, les constats dressés peuvent utilement contribuer à la réflexion des diverses autorités et partenaires pouvant concourir à améliorer le cadre global : ANCT, Arcep, préfet et comité de concertation sur les télécoms fixes départemental ou régional, CCED, DGSCGC, ministre en charge, parlementaires, associations de collectivités, fédération professionnelle des opérateurs et intégrateurs, etc. Il en est de même pour faire part de retours d'expériences de crise dont il sera toujours essentiel de tirer les leçons.

# CONCLUSION

Les préoccupations de résilience n'ont pas été absentes lors de la construction des réseaux en fibre optique, dans la limite des considérations budgétaires diverses du moment. Avec l'approche de la fin de la phase de construction, et la montée des risques, notamment climatiques, s'ouvre un nouveau chapitre. Comme dans toute l'histoire du très haut débit en France, il s'écrira à la fois au niveau local et au niveau national, en interaction.

Les mesures les moins onéreuses tout en étant efficaces sont de l'ordre de l'organisation : avec les autorités locales et les autres gestionnaires de réseaux dans les dispositifs ORSEC, entre l'OI et les gestionnaires de génie civil, l'OI et les OC, les délégants et les délégataires, etc. Elles paraissent indispensables, pour tenir compte de la stratification des responsabilités.

Autre point d'attention, nous sommes encore dans une phase de construction des réseaux fibre ; les OI ont des équipes locales pour encadrer les prestataires, ceux-ci ont des compétences disponibles, des matériels et équipements, et tout ceci est mobilisable en cas de destructions importantes, comme cela a été le cas pour La Roya. Demain, avec la fin des constructions en masse, toutes ces conditions favorables auront radicalement changé. Les équipementiers ne maintiendront pas non plus toutes leurs lignes de production. Il sera nécessaire de garder du personnel compétent in situ, pour l'OI comme pour les intégrateurs, et des stocks mobilisables, en face d'aléas importants. Là aussi, en comparaison avec le temps du réseau unique hérité du monopole, la fragmentation des acteurs, à la fois dans les couches et dans l'espace géographique, nécessitera pour chacun d'eux d'inventer de nouvelles réponses, ou, pourquoi pas, par mutualisation.

Qu'en est-il d'investissements massifs, tels que des enfouissements des artères aériennes les plus importantes et exposées ? Des obligations réglementaires pour assurer les services essentiels existent et se renforceront, mais ce n'est probablement pas sous cette pression que les opérateurs seront rapidement tenus d'augmenter la résilience des réseaux - sauf à ce qu'une série d'incidents majeurs ne vienne en démontrer l'impérieuse nécessité. On peut espérer plutôt que la communauté des opérateurs dégage un consensus pour cette augmentation au profit des abonnés, avec les investissements nécessaires. En parallèle, des mécanismes d'enfouissements sélectifs sont à l'étude, avec une péréquation des coûts de génie civil élargie par rapport au cadre actuel, mais encore incertains à date, sans parler des hypothèses de mise en place de fonds nationaux dédiés pour partie à la résilience.

A défaut d'investissements massifs, certains, ciblés sur les parties amont du réseau ou des segments très accidentogènes, sont davantage à la portée des budgets existants. Ils seront utiles en cas de crise mais également pour améliorer la qualité de service en réduisant l'impact d'incidents courants. Les Schémas locaux de résilience sont là pour les identifier.

Enfin la réalisation de ces schémas locaux nourrira aussi les réflexions des acteurs industriels et institutionnels au niveau national, par une approche concrète, liée à la diversité des territoires.

# REMERCIEMENTS

L'Agence nationale de la cohésion des territoires (ANCT) a soutenu d'emblée notre ambition de procurer aux collectivités territoriales un guide méthodologique sur la résilience des réseaux. Nous tenons à remercier les équipes de l'ANCT pour leur accompagnement et leur participation tout au long de l'élaboration de ce guide.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

agence nationale de la cohésion des territoires

Nous adressons nos sincères remerciements aux acteurs institutionnels, opérateurs, collectivités territoriales et associations télécoms pour leurs témoignages et contributions dans le cadre de l'étude :

- Altitude Infrastructure
- Arcep
- Avicca
- Axione
- Bouygues Telecom
- Commissariat aux communications électroniques de défense
- Cercle CREDO
- Collectivité de Corse
- Direction générale des Collectivités locales
- ENEDIS
- Fédération nationale des collectivités concédantes et régies
- Gironde Numérique
- Haute-Garonne Numérique
- Iliad / Free
- Nouvelle Aquitaine THD
- Orange
- Orange Concessions
- Régie Réunion THD
- Sogetrel
- TDF
- Vendée Numérique
- XP Fibre
- Willis Towers Watson

Ce guide méthodologique a été rédigé par la Banque des Territoires à partir de l'étude pilotée par Patrick Vuitton avec l'appui de Martin Tissier du cabinet BERSAY et de Pierre Borda du cabinet SETICS.

BERSAY

Setics

BANQUE des TERRITOIRES

Caisse des Dépôts GROUPE

**banquedesterritoires.fr**

@BanqueDesTerr

Direction de la communication du groupe Caisse des Dépôts - Août 2023