# AVIS N° 2026-01 DU 19 JANVIER 2026

## SUR LA RESILIENCE ET LA ROBUSTESSE DES RESEAUX NUMERIQUES ET DE TELECOMMUNICATIONS

Les récentes catastrophes naturelles (inondations, incendies, tempêtes, neige) et les actes de vandalisme et de sabotage qui ont affecté les infrastructures numériques et de télécommunications ont démontré la très grande dépendance de notre société, de nos concitoyens et de notre économie à l'égard de ces phénomènes.

Les membres de la Commission supérieure du numériques et des postes (CSNP) considèrent qu'il est essentiel de s'assurer que notre pays a mis en place des plans de résilience solides et mobilise les moyens nécessaires pour faire face à ces menaces croissantes et multiples.

Dans cette perspective, les membres de la CSNP ont confié à Mme Lisa Belluco, députée de la Vienne, et Mme Patricia Demas, sénatrice des Alpes Maritimes, une mission portant sur la résilience des réseaux numériques et de télécommunications.

Naturellement, la résilience des réseaux repose, en premier lieu, sur la qualité et la robustesse des infrastructures qui ont été déployées initialement et sur leur entretien. La CSNP a eu l'occasion, à plusieurs reprises, d'alerter les opérateurs d'infrastructures et leurs sous-traitants ainsi que l'Arcep sur la nécessité de renforcer la qualité des réseaux numériques et de télécommunications sur l'ensemble du territoire. Les membres de la CSNP regrettent que ce ne soit pas encore complètement le cas.

La notion même de résilience recouvre une acception assez large[1] et porte sur la capacité des réseaux numériques et de télécommunications à mieux résister et à assurer une continuité de service minimale lors de la survenance d'évènements extérieurs tels que les catastrophes naturelles, les accidents, les actes de vandalisme ou de sabotage mais également les actes de cyber malveillance. Du point de vue de la CSNP, la notion de résilience inclut également la sécurisation de l'approvisionnement des composantes absolument nécessaires au fonctionnement de ces infrastructures (matières premières et composants de base tels que les semi-conducteurs).

Les membres de la CSNP ont donc porté leur attention sur l'état de préparation et les réponses apportées par l'ensemble des acteurs publics et privés à ces crises d'origines diverses liées notamment aux catastrophes climatiques ou aux incendies.

En réalité, plusieurs points critiques et pistes d'amélioration ont déjà été diagnostiqués. La CSNP constate cependant que la mise en œuvre des mesures pour y remédier est beaucoup trop lente. Cette lenteur s'explique par un manque de coordination et, sans doute, un manque de volontarisme des pouvoirs publics pour mettre en œuvre le plus rapidement possible les mesures nécessaires pour renforcer la résilience des infrastructures numériques et de télécommunication en cas de crise.

Au terme de ses travaux, le groupe de travail sur la résilience des réseaux propose des adaptations et des recommandations sur le pilotage national et local des plans de résilience, sur l'adaptation de notre droit, sur l'organisation des services de l'Etat et sur le financement d'infrastructures résilientes :

- **Renforcer le pilotage national et local de la résilience des réseaux de télécommunications**

**Recommandation n°1 : Coordonner au niveau ministériel le plan de résilience des réseaux de télécommunications**

[1] Plusieurs définitions de la résilience des réseaux numériques et de télécommunications co-existent, elles émanent d'institutions nationales ou internationales: l'Organisation internationale des télécommunications, l'Union européenne, l'Arcep ou l'ANCT notamment.

**Recommandation n°2 : Mieux informer les préfets des actions à conduire au niveau local pour renforcer la résilience des infrastructures de télécommunications**

**Recommandation n°3 : Communiquer aux préfets de département des annuaires opérationnels et actualisés des représentants locaux des opérateurs commerciaux et d'infrastructures des réseaux de télécommunications fixes et mobiles**

**Recommandation n°4 : Demander aux opérateurs commerciaux et d'infrastructures de communiquer aux préfets de département des plans de réponse aux crises conformes**

**Recommandation n° 5 : Intégrer les infrastructures de télécommunications dans les plans communaux de sauvegarde**

- **Mesures à prendre en urgence**

**Recommandation n°6 : Actualiser la doctrine du plan Orsec pour intégrer l'ensemble des opérateurs de télécommunications au cours du 1er semestre 2026**

**Recommandation n°7 : Mettre à la disposition des préfets un diagnostic en temps réel de la couverture mobile impactée en cas de crise**

**Recommandation n °8 : Mettre en place dès 2026 une itinérance en catastrophe ou « *disaster roaming* ».**

**Recommandation n°9 : Permettre aux opérateurs de télécommunication d'accéder aux réserves de carburant de l'Etat en cas de blocage des stations-services ou des raffineries**

- **Mieux connaitre et évaluer les risques pesant sur la résilience des réseaux numériques et de télécommunications**

**Recommandation n°10 : Identifier les infrastructures les plus critiques (Nœuds de Raccordement Optique et antennes mobiles) et renforcer leur robustesse et leur alimentation en énergie en cas de crise**

**Recommandation n°11 : Confier à l'Arcep le contrôle des plans de crise de ces points critiques, la redondance et la robustesse de ces infrastructures les plus critiques**

**Recommandation n°12 : Recenser et quantifier l'origine des pannes et des défaillances des infrastructures des réseaux numériques et de télécommunications et leur impact pour les usagers**

**Recommandation n°13 : Anticiper et adapter les réseaux au changement climatique à moyen terme**

- **Gérer l'interdépendance des réseaux de télécommunications et des réseaux électriques**

**Recommandation n°14 : Classer les infrastructures de communications électroniques comme des infrastructures de « service essentiel » et intégrer le secteur des télécommunications dans l'article 2 de l'arrêté du 5 juillet 1990 fixant les consignes générales de délestages sur les réseaux électriques**

**Recommandation n° 15 : Développer une interface Enedis permettant en situation nominale et en temps de crise aux opérateurs télécoms de récupérer en masse et en temps réel le statut électrique des Points de Livraison Energétiques**

**Recommandation n°16 : Réserver le spectre de basse fréquence 450 Mhz aux besoins des services publics**

- **Mesurer les risques liés à l'usage de technologies non souveraines**

**Recommandation n°17 : Identifier et mesurer la dépendance de nos infrastructures aux solutions numériques non souveraines**

**Recommandation n°18 : Etablir précisément les risques de dépendance liés à la virtualisation des réseaux télécoms**

**Recommandation n°19 : Initier au niveau européen la constitution de stocks stratégiques de métaux critiques**

- **Financement de la résilience des réseaux numériques et de télécommunications**

**Recommandation n° 20 : Sanctuariser sur le long terme les moyens budgétaires des services d'urgence et de l'ACMOSS**

**Recommandation n°21 : Mettre en place un fonds de résilience sur le modèle du fonds Barnier**

**Recommandation n°22 : Mobiliser les instruments financiers européens sur la résilience des réseaux et les infrastructures numériques et de télécommunications**

- **Anticiper les conflits d'usage liés au développement exponentiel de l'IA et du développement des centres de données**

**Recommandation n°23 : Mettre en place des mécanismes robustes pour mesurer les capacités et les consommations électriques liés aux usages de l'IA et des centres de données**

**Recommandation n°24 : Favoriser un débat public sur les usages critiques du numérique**

## I. Résilience des réseaux numériques et de télécommunications : une prise de conscience collective est en cours

Au cours de leurs travaux, les rapportrices ont pu constater qu'une véritable prise de conscience émergeait depuis quelques années sur la nécessité de mieux intégrer dans les dispositifs de crise nationaux et locaux les infrastructures numériques et de télécommunications.

Le sujet de la résilience est désormais systématiquement abordé par les acteurs du numérique et des télécommunications que ce soit au niveau des comités d'experts de l'Arcep, des groupes de travail de la Fédération française des télécoms et d'Infranum, par les collectivités locales notamment au sein de l'AMF, de l'AVICCA et de la FNNCR, au sein des comités locaux organisés autour des RIP, par l'ANCT et La Banque des Territoires, par le CREDO.

Face à la récurrence et la multiplication des crises diverses (incendies, tempêtes, actes de vandalisme), les pouvoirs publics ont pris en compte la nécessité de faire évoluer les outils de communication dont disposent les services de sécurité et de secours avec **la mise en place du Réseau radio du Futu**r qui bénéficiera à 300 000 utilisateurs en charge de la protection de nos concitoyens et avec **la création en 2023 de l'Agence des communications mobiles opérationnelles de sécurité et de secours (ACMOSS)[2].**

Pour autant, cette prise de conscience ne s'est pas encore traduite par une meilleure structuration de l'accompagnement et de la gestion de la résilience des réseaux numériques et de télécommunications.

## II. Un impératif : renforcer le pilotage national et local de la résilience des réseaux numériques et de télécommunication

Malgré la prise de conscience collective sur la nécessité d'améliorer la résilience et la robustesse des réseaux des télécommunications, le défaut de pilotage et le manque de coordination des cellules de préparation et de gestion de crise des réseaux de télécommunication sont constatés que ce soit au niveau national aussi bien qu'au niveau local.

**Pour les membres de la CSNP, il s'agit moins de désigner les responsables de ces carences que d'exiger un plus grand volontarisme pour que les mesures nécessaires et le plus souvent déjà identifiées soient mises en œuvre sans tarder. Certaines mesures n'appellent pas de crédits supplémentaires mais un effort organisationnel piloté au niveau national et local et surtout un véritable portage politique.**

### 1. Pilotage national de la résilience des réseaux numérique et de télécommunications : un portage politique est nécessaire

Si des progrès notables ont été réalisés avec la création de l'ACMOSS et du Réseau Radio du Futur qui coordonnent les moyens de télécommunications mis à disposition des services de secours, la résilience des infrastructures numériques et de télécommunications semble se heurter à des problèmes de pilotage au niveau national et local.

[2] Décret n°2023-225 du 30 mars 2023

Au niveau national, sur ce sujet, la compétence est partagée entre les acteurs traditionnels de la gestion de crise, le Secrétariat général de la défense et de la sécurité nationale (SGDSN) et la direction générale de la Sécurité civile et de la gestion des crises (DGSCGC) du ministère de l'intérieur d'une part, et les acteurs « sectoriels », familiers du secteur du numérique et des télécoms dans leurs champs de compétence respectifs : l'Arcep, la Direction générale des entreprises (DGE) et l'Agence nationale de la cohésion des territoires (ANCT), le Commissariat aux communications électroniques de défense (CCED) mais également le ministère de l'environnement.

**Force est de constater que cette multitude d'acteurs pèse sur l'efficacité du pilotage de la résilience des infrastructures numériques et de télécommunications au niveau national.**

D'un point de vue organisationnel et administratif, le SGDSN a compétence pour coordonner les actions de résilience.

Dans son rapport consacré aux « Soutiens publics en faveur du déploiement de la fibre optique » publié en avril 2025, la Cour des comptes constatait que « *l'impulsion nationale fait aujourd'hui défaut sur les problématiques de résilience. Des questions de fond demeurent non résolues quant à la place des réseaux fibre dans l'organisation de gestion des crises, aux responsabilités des acteurs et aux actions à conduire »* et relève « *un déficit de concertation ou résultent de l'absence de point de convergence entre les multiples instances de travail (comité des experts de l'Arcep, groupes de travail de la fédération françaises des télécoms et d'Infranum, comités locaux organisés autour des RIP, études financées par les territoires. Les orientations communes aux acteurs font défaut. ».*

La Cour des comptes propose qu'«*une réflexion soit conduite sous l'égide du secrétariat général de la défense et de la sécurité nationale* ».

**La Commission supérieure du numérique et des postes considère que le temps n'est plus à la réflexion mais à l'action : depuis 2022[3], la CSNP appelle l'écosystème du numérique et des télécoms et leurs autorités de tutelle à se saisir des enjeux de la résilience et de son financement.**

Les crises liées au changement climatique et les incidents d'origines diverses ont un impact avéré et immédiat sur le fonctionnement des réseaux de télécommunications. Il y a urgence à ce que le pouvoir politique s'empare du sujet, procède aux arbitrages nécessaires et que les services de l'Etat engagent des actions nécessaires dans les meilleurs délais.

**Pour les membres de la CSNP, une coordination au niveau administratif des acteurs concernés est nécessaire mais insuffisante, ils demandent une véritable coordination ministérielle de la résilience des réseaux de télécommunications.**

**Pour être opérationnel, ce portage politique doit clairement identifier un plan d'actions pour renforcer la résilience des réseaux numérique et de télécommunications en désignant les acteurs responsables et en précisant un calendrier d'actions ambitieux au vu de l'urgence des mesures qui doivent être prises.**

Les membres de la CSNP considèrent que le Ministère de l'Intérieur qui a autorité sur les préfets doit porter ces actions de coordination au plus près du terrain.

**Recommandation n°1 : Coordonner au niveau ministériel le plan de résilience des réseaux de télécommunications**

[3] Avis n°2022-05 du 27 juillet 2022 portant recommandations sur le financement et le modèle économique des infrastructures et des réseaux de télécommunications

### 2. Mieux informer les préfets en charge du pilotage local de la résilience

Il ressort des auditions conduites par les rapportrices que la résilience des réseaux fixes (cuivre et désormais fibre) mais également de téléphonie mobile sont encore méconnus des préfets, qui sont pourtant en charge de gérer les crises dans les territoires.

**Résilience des réseaux de télécommunication : un cadre juridique inapplicable et inappliqué ?**

Le cadre législatif et règlementaire de la gestion des crises dans le domaine des télécommunications, notamment le code des postes et communications électroniques (CPCE), reflète le monde des télécoms d'il y a 20 ans, lorsqu'un seul acteur, France Telecom, gérait l'ensemble des réseaux.

L'article L. 33-1 du CPCE impose une obligation de notification au ministère chargé des communications électroniques de tous incidents de sécurité ayant eu un impact significatif sur le fonctionnement du réseau.

Au titre de l'article D. 98-4 du CPCE, « *l'opérateur doit prendre les dispositions nécessaires pour assurer de manière permanente et continue l'exploitation du réseau et des services de communications électroniques et pour qu'il soit remédié aux effets de la défaillance du système dégradant la qualité du service pour l'ensemble ou une partie des clients, dans les délais les plus brefs*. ».

L'article D. 98-5 du CPCE précise que l'opérateur prend toutes les mesures appropriées pour assurer la sécurité de ses réseaux et garantir la continuité des réseaux fournis.

L'article L. 732-1 du Code de la sécurité intérieure (CSI) impose à tous les exploitants d'un service destiné au public ainsi qu'aux opérateurs des réseaux de communications électroniques ouverts au public de prévoir les mesures nécessaires au maintien de la satisfaction des besoins prioritaires de la population lors des situation de crise et de rétablir un fonctionnement du service dans des conditions compatibles avec l'importance des populations concernées pour assurer la sécurité de ses réseaux et garantir la continuité des services fournis.

L'article 732-2-1 du Code de la sécurité intérieure créé par la loi Climat et résilience du 22 aout 2021 permet au préfet de département de demander à tout exploitant de service ou réseau mentionné à l'article 732-1 dans les territoires où l'exposition importante à un ou plusieurs risques naturels peut conduire à un arrêt de toute ou partie du service ne permettant plus de répondre aux besoins prioritaires de la population , un diagnostic de vulnérabilité de ses ouvrages existants, les mesures qu'il prendra en cas de crise, les procédures de remise en l'état du réseau après la survenance de l'aléa et un programme des investissements prioritaires pour améliorer la résilience du réseau.

Plusieurs textes de nature administrative complètent ce corpus :

- L'instruction du Premier ministre n° 6600 du 7 janvier 2014 relative aux opérateurs d'importance vitale
- La convention nationale de lutte contre la malveillance visant les réseaux de télécommunications établie entre l'Etat et les opérateurs en 2021
- Le guide pour la déclaration des incidents affectant les réseaux d'infrastructures de communications électroniques publié par le service du haut fonctionnaire de défense et de sécurité du ministère de l'économie, des finances
- La décision n°2015-776 de l'Arcep impose aux opérateurs commerciaux des obligations de garantie de temps d'intervention, de rétablissement et d'interruption maximale de service

Au niveau européen, la directive (UE) n°2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n°910/2014 et la directive (UE) 2018/1972 et abrogeant la directive (UE) 2019/1148 ; directive dite « NIS 2 » consacre les infrastructures numériques comme des infrastructures hautement critiques. La directive NIS 2 est entrée en vigueur en octobre 2024 et devrait être transposée à l'occasion de l'adoption du projet de loi résilience programmée à l'agenda de l'Assemblée nationale mi-novembre 2025.

**Les propositions de modification formulées par la Cour des comptes**

Dans son rapport publié en avril 2025, la Cour des comptes considère que le cadre juridique sur la résilience des réseaux fibres est « *sédimenté et imprécis* » et propose plusieurs pistes d'amélioration :

- Préciser par un arrêté les « besoins prioritaires de la population » au sens de l'article R. 732-2 du CSI
- Seules les dispositions L 33.1, D. 95-4 et D. 98-5 du CPCE peuvent être contrôlées par l'Arcep qui n'a jamais sanctionné un opérateur sur cette base,

- L'article L. 732-1 du CSI n'est assorti d'aucun dispositif de contrôle ou de sanction

**Avant de procéder à des modifications règlementaires et législatives, les membres de la CSNP recommandent de rappeler à l'Arcep et aux préfets leurs rôle dans l'application des dispositions des articles L 33.1 et D. 98-5 du CPCE et de l''article L. 732-1 du CSI.**

Pour les membres de la CSNP, pointer du doigt la responsabilité des services préfectoraux qui sont submergés par une masse d'informations et de requêtes n'est pas suffisant, **ils souhaitent que l'Etat exprime clairement les actions à conduire au niveau local et que les préfets disposent des informations utiles et nécessaires.**

### a. Clarification nécessaire des actions à mettre en œuvre

La Direction générale des entreprises a informé les rapportrices de la rédaction d'un guide par la Direction générale de la Prévention des risques (DGPR) établissant des lignes directrices à l'attention des services déconcentrés afin d'éclairer les préfets dans leurs décisions de demander un diagnostic de vulnérabilités à l'ensemble des opérateurs dont les infrastructures sont exposées à des risques particuliers et d'émettre des recommandations pour renforcer la résilience.

L'expérience passée a démontré que ces instructions sont parfois insuffisamment opérationnelles alors qu'il importe, au contraire, de clarifier les actions à conduite en priorité.

Sollicitée par l'ANCT pour l'actualisation de la circulaire du Premier ministre en date du 5 juin 2021 sur les comités locaux de concertations des réseaux fixes, la CSNP a proposé que **les circulaires soient claires et opérationnelles pour les services de la préfecture**, ce qui n'est pas le cas actuellement.

La CSNP a, par ailleurs, attiré l'attention des pouvoirs publics sur les risques liés à la fin des réseaux 2G et 3G, et a proposé que le sujet de la résilience des infrastructures numériques et de télécommunications soient intégré dans les comités locaux.

**Recommandation n°2 : Mieux informer les préfets des actions à conduire au niveau local pour renforcer la résilience des infrastructures de télécommunications**

### b. Communication aux préfets de département la liste des représentants locaux des opérateurs commerciaux et d'infrastructure et leur plan de gestion des crises

Le temps où Orange était le seul opérateur télécoms est révolu depuis plusieurs années et pourtant, dans certains départements, l'opérateur historique est parfois le seul opérateur associé aux exercices et cellules de prévention et de gestion de crise.

Cette situation s'explique par le très grand nombre d'acteurs qui interviennent à l'occasion du déploiement du Plan France Très Haut Débit qui ne sont pas clairement identifiés et identifiables par les pouvoirs publics départementaux.

L'ANCT finalise un annuaire des opérateurs d'infrastructures impliqués dans les RIP qui sera transmis aux préfets. Cet annuaire ne répondra qu'à une partie du problème.

**Ainsi que le soulignent plusieurs interlocuteurs dont l'Arcep, il parait essentiel de cartographier pour chaque département l'ensemble des acteurs du numérique et des télécoms et le périmètre de leurs responsabilités**.

**Pour les membres de la CSNP, il est absolument essentiel que les préfets disposent d'un annuaire complet et mis à jour régulièrement précisant les points de contact départementaux des opérateurs des réseaux fixes et mobiles, des opérateurs commerciaux et d'infrastructures.**

Pour les membres de la CSNP, ce document doit être un outil opérationnel : il s'agit de communiquer aux autorités publiques des points de contact qui répondent quand ils sont contactés et sont en mesure de répondre aux attentes légitimes des services de l'Etat. Sur ce sujet, le secteur des télécommunications pourrait s'inspirer des interlocuteurs privilégiés qu'Enedis désigne pour répondre aux attentes des autorités publiques.

Ces annuaires pourraient être également communiqués aux maires.

**La CSNP demande au Ministre en charge des télécommunications d'adopter un texte réglementaire en ce sens.**

**Recommandation n°3 : Communiquer aux préfets de département des annuaires opérationnels et actualisés des représentants locaux des opérateurs commerciaux et d'infrastructures des réseaux de télécommunications fixes et mobiles**

### c. Communication aux préfets par les opérateurs des diagnostics de vulnérabilité et des mesures envisagées en cas de crise

Alors que l'article 732-2-1 du Code de la sécurité intérieure créé par la loi Climat et résilience du 22 aout 2021 permet au préfet de département de demander aux opérateurs un diagnostic de vulnérabilité de ses ouvrages existants, les mesures qu'il prendra en cas de crise, les procédures de remise en l'état du réseau après la survenance de l'aléa et un programme des investissements prioritaires pour améliorer la résilience du réseau, aucun préfet ne semble avoir formulé une telle demande à un opérateur de réseau fibre.

En effet, dans son rapport publié en avril 2025, **la Cour des comptes indiquait que fin 2024 aucun préfet n'avait formulé une telle demande à un opérateur de réseau fibre**. L**a Cour des comptes relève que moins de la moitié des RIP a engagé des travaux visant à planifier la réponse opérationnelle en cas de crise.**

L'ANCT a prévu de communiquer la liste des opérateurs d'infrastructures des RIP aux préfets de département. Cette initiative ne répondra que partiellement aux exigences liées à la résilience des réseaux.

La CSNP propose que l'ensemble des opérateurs commerciaux et d'infrastructures communiquent sans tarder aux préfets le diagnostic de vulnérabilité de leurs ouvrages et leur plan de réponses aux crises.

Pour s'assurer de la qualité de ces plans de réponse aux crises, la CSNP propose que ce plan soit constitué sur un modèle unique et qu'un guide de rédaction soit élaboré et communiqué sous l'égide de l'Arcep à l'ensemble des opérateurs.

**Recommandation n°4 : Demander aux opérateurs commerciaux et d'infrastructures de communiquer aux préfets de département des plans de réponse aux crises conformes**

### d. Intégrer les infrastructures de télécommunications dans les plans communaux de sauvegarde

Selon l'ANCT et la Banque des Territoires, le schéma local de résilience permettrait d'établir une cartographie des opérateurs d'infrastructures et des réseaux présents sur un territoire et d'établir des diagnostics de vulnérabilité en s'appuyant sur ceux établis par les opérateurs d'infrastructures.

A date, une dizaine de schémas locaux de résilience (SLR) seraient mis en place et une vingtaine de SLR seraient en voie d'adoption. Selon l'ANCT, le cout moyen d'un SLR (environ 100 000 euros dont la moitié serait co-financée par la Banque des Territoires) n'est pas un obstacle à leur adoption par les collectivités locales.

En réalité, ce serait plutôt le financement des actions de résilience elles-mêmes qui pose une difficulté aux collectivités locales (cf. paragraphe VI).

La CSNP considère qu'une trentaine de SLR ne permet pas d'atteindre un seuil très significatif de résilience à l'échelle du territoire national. Pour un passage à l'échelle plus ambitieux de la résilience des infrastructures de télécommunications au niveau local, la CSNP propose d'intégrer les infrastructures de télécommunications dans les plans communaux de sauvegarde, ce qui permettrait de sensibiliser l'ensemble des élus locaux au sujet de la résilience des infrastructures de télécommunications et constituerait une incitation à établir un schéma local de résilience.

**Recommandation n° 5 : Intégrer les infrastructures de télécommunications dans les plans communaux de sauvegarde**

**Plan de gestion de crise : l'exemple de la Métropole Nice-Côte-d 'Azur à l'épreuve de la tempête Alex**

Dès le 16 octobre 2020, le Conseil Métropolitain a acté une démarche proactive pour se doter de solutions de communication de secours, souveraines et résilientes.

**Phase 1 - Réponse immédiate (2020-2022)** : La première action a été de garantir un canal de communication minimal pour les élus en première ligne. Chaque maire de la Métropole a été doté d'un téléphone satellitaire et formé à son usage.

**Phase 2 - Expérimentations (2022-2023)** : La Métropole Nice Côte d'Azur a testé en conditions réelles différentes technologies pour en valider la pertinence :

- En 2022, un réseau terrestre (technologie uMesh) : Un réseau expérimental de "bulles Wi-Fi" autonomes en énergie a été déployé, reliant 5 communes (Nice, Saint-Laurent-du-Var, Carros, Colomars, La Roquette-sur-Var). Ce réseau à la capacité de transporter des flux de données importants à très haut débit et des communications radio. Grâce au maillage, il a la capacité de continuer à fonctionner même si une ou plusieurs antennes sont coupées ou détruites, et cela sans intervention humaine.
- En 2023, des valises tactiques satellitaires : La Métropole Nice Côte d'Azur a mené des exercices de simulation de crise (séisme à Aspremont et Venanson, inondation à Drap et Gattières). Ces exercices ont été réalisés avec coupure totale des réseaux numériques et électriques, validant des fonctionnalités avancées comme la diffusion d'images de drones et les visioconférences entre le terrain et le PC de crise.

**Phase 3 - Déploiement opérationnel (à partir de 2024) :**

- En 2024 : Acquisition des 5 premières bulles tactiques mobiles, validées lors des exercices.
- À partir de 2025 : Déploiement du réseau résilient permanent, en commençant par les 21 communes du périmètre "Tempête Alex". Ce réseau est basé sur les technologies expérimentées en phase 2, mais également sur des technologies éprouvées. Il disposera d'une autonomie énergétique et sera entièrement maillé en s'appuyant sur tes liaisons fibre, faisceaux hertzien, wifi mesh et satellite. Il servira aux communications de crise, mais aussi à des besoins quotidiens (communication radio, remontée de données de capteurs comme les pluviomètres, pilotage

d'installations techniques). Ce double usage garantit son maintien en condition opérationnelle et justifie l'investissement.

La tempête Alex a directement nourri la rédaction du Plan Intercommunal de Sauvegarde (PICS), dont la réalisation est une obligation légale (Loi Matras) d'ici novembre 2026. L'enjeu n'est plus seulement de décrire le risque de coupure dans les plans, mais bien d'y intégrer les procédures concrètes d'activation de solutions

Concrètement, le PCIS prévoit :

- Des procédures d'activation claires : le PICS définit qui déploie les valises tactiques, comment et dans quelles situations, et comment les services de secours et les PC de crise communaux se connectent au réseau de secours.
- Un outil de coordination déjà opérationnel (depuis janvier 2024) : il s'agit d'une main courante numérique sécurisée qui permet l'interconnexion en temps réel entre les PC de crise des communes et celui de la Métropole.
- Au fur et à mesure du déploiement du réseau résilient permanent (pour lequel les premières antennes secourues électriquement sont en cours d'acquisition), le PCIS sera mis à jour pour prendre en compte l'utilisation de ce réseau comme l'outil principal de communication en cas de crise.

## III. Plusieurs mesures à adopter en urgence pour renforcer la résilience

### 1. Participation de l'ensemble des opérateurs en charge des infrastructures de télécommunications aux cellules de préparation et de gestion de crise

Au cours des auditions et des travaux, Mme Lisa Belluco et Mme Patricia Demas ont interrogé l'ensemble des parties prenantes sur leur retour d'expérience après les graves incendies qui se sont déroulés dans l'Aude cet été. Ces témoignages et contributions ont mis en lumière des dysfonctionnements qui avaient déjà été constatés lors des incendies en Gironde en 2022 ainsi qu'à l'occasion des tempêtes Ciaran et Alex.

Il a notamment été constaté que l'ensemble des opérateurs commerciaux et des opérateurs d'infrastructures ne sont pas systématiquement associés aux cellules de crise organisées par les préfets et que, dans certains cas, leurs agents ne sont pas autorisés à circuler dans les zones sinistrées pour réaliser les travaux nécessaires au rétablissement des lignes.

Par ailleurs, les opérateurs commerciaux et d'infrastructure indiquent qu'ils ne sont pas systématiquement associés aux démarches et comités de planification opérationnelle de préparation et de gestion des crises notamment dans le plan Orsec.

Pour mémoire, en 2015, la direction générale de la sécurité civile et de la gestion de crise (DGSCGC) a élaboré un guide ORSEC sur les nouvelles modalités de rétablissement et l'approvisionnement d'urgence des réseaux d'électricité, communications électroniques, eau, gaz, hydrocarbures, intitulé RETAP RESEAUX.

**Pour les membres de la CSNP, il est impératif de modifier sans attendre le guide ORSEC « RETAP Réseaux » afin d'intégrer systématiquement les opérateurs d'infrastructures dans les plans Orsec**

En effet, et en dépit des signalements effectués depuis plusieurs années, les préfectures fonctionnent sur des schémas anciens dans lesquels Orange était le seul opérateur d'infrastructures de télécommunications connu des services de la préfecture.

Déjà en 2023, lors du TRIP de l'AVICCA, des représentants de Gironde Numérique indiquaient qu'ils n'avaient pas été appelés par les services de la préfecture de Gironde lors des trois grands incendies qui ont détruit plus de 30 000 hectares dans le sud la Gironde à Landiras, Belin-Beliet et de La Teste-de-Buch.

Nous sommes en 2025, et rien ne semble avoir évolué : La FNCCR a ainsi signalé à la CSNP que lors des incendies dans l'Aude l'autorité délégante, SYADEN, et l'opérateur délégataire EMERAUDE (groupe ALTITUDE infra) n'ont été associés à la gestion des incendies seulement après que M. Régis BANQUET, président du SYADEN, ait été mobilisé par ses autres mandats. L'actualisation de la doctrine sur les plans Orsec pour intégrer pleinement les réseaux télécoms a pris du retard et sa publication est programmée pour fin 2026.

**Les membres de la CSNP considèrent que ce sujet doit être traité de manière prioritaire et appelle le Ministère de l'intérieur à actualiser la doctrine du plan Orsec au 1er semestre 2026.**

**Recommandation n°6 : Actualiser en urgence la doctrine du plan Orsec pour intégrer l'ensemble des opérateurs de télécommunications au cours du 1er semestre 2026**

### 2. Création d'une cartographie numérique en temps réel de la couverture mobile impactée en cas de crise mise à la disposition des préfets et des autorités

Le CCED recommande de mettre à disposition des préfets un outil cartographique de la couverture mobile en temps réel. Cette cartographie suppose de pouvoir obtenir des opérateurs les données relatives à leur réseau antennaire de qualité.

Les membres de la CSNP appuient cette demande du CCED qui constitue une base minimale indispensable à une meilleure gestion des crises et s'étonnent que cette solution ne soit pas encore opérationnelle.

Le CCED propose de créer une obligation légale pour les opérateurs mobiles de fourniture de données en temps réel. Ce coût serait pris en charge par l'Etat en juste rémunération.

Les membres de la CSNP proposent qu'une proposition de loi instaure cette obligation assortie de sanctions financières dissuasives pour les opérateurs en cas de non-fourniture ou de transmission de données de mauvaise qualité. La simple "juste rémunération" proposée ne pourrait, selon les membres de la CSNP, suffire à garantir leur coopération.

**Recommandation n°7 : Mettre à la disposition des préfets un diagnostic en temps réel de la couverture mobile impactée en cas de crise**

### 3. Mise en place d'une itinérance en catastrophe ou "Disaster Roaming"

L'itinérance en catastrophe est une procédure technique mise en œuvre en cas de crise majeure affectant les réseaux mobiles des opérateurs télécoms. Elle permet à un abonné d'un réseau est devenu hors service d'être pris en charge par un autre réseau. Le CCED considère que ce mécanisme présente un intérêt notamment dans les départements maritimes et d'outre-mer soumis à des risques climatiques accrus. La CSNP considère que le "*Disaster Roaming*" n'est pas un service commercial mais une contribution obligatoire à la sécurité nationale, au même titre que d'autres réquisitions. L'impulsion de l'État est nécessaire et il revient à l'Arcep d'en définir le cadre technique et le modèle de compensation financière juste et obligatoire entre opérateurs dans les meilleurs délais.

**Recommandation n °8: mettre en place dans les meilleurs délais une itinérance en catastrophe ou « *disaster roaming* ».**

### 4. Accès des opérateurs aux réserves de carburant de l'Etat en cas de crise

Les représentants de la Fédération française de télécoms ont fait valoir en audition qu'ils ne disposaient pas d'un accès aux réserves de carburant de l'Etat en cas de problème d'accès au carburant (grève des raffineries ou des stations d'essence) comme cela est le cas pour Enedis.

Les membres de la CSNP considèrent que cette demande relève du bon sens et qu'elle est légitime.

**Recommandation n°9 : Permettre aux opérateurs de télécommunication d'accéder aux réserves de carburant de l'Etat lorsque cela est nécessaire pour le rétablissement des réseaux de télécommunication**

## IV. Mieux connaitre et évaluer les risques pesant sur les réseaux de télécommunications

### 1. Identifier et renforcer la robustesse des nœuds de raccordement optiques et des sites mobiles prioritaires

Les Nœuds de Raccordement Optique (NRO) de même que les antennes de téléphonie mobile sont les pierres angulaires des réseaux de télécommunication :

- Le NRO est le point central de raccordement d'un réseau fibre optique local. Il agrège les lignes optiques de milliers de foyers ou d'entreprises dans un quartier ou une ville. Il contient des équipements actifs (commutateurs, multiplexeurs) qui transforment et distribuent le signal. Si un NRO tombe, c'est toute une zone géographique qui perd son accès Internet fixe (fibre).
- Les sites Mobiles (Antennes) gèrent la couverture, la capacité et le transfert des communications mobiles. S'ils sont hors service, il est impossible de téléphoner, d'envoyer des SMS ou d'utiliser l'Internet mobile dans la zone qu'ils couvrent.

La Métropole Nice Côte d'Azur, confrontée à la tempête Alex, a été conduite à expérimenter un réseau résilient, maillé et autonome en énergie, pour permettre à ses services de pouvoir continuer à communiquer pendant 48 heures dans l'hypothèse où les réseaux numériques et électriques seraient hors service.

En cas de délestage électrique généralisé ou de coupure électrique, le système mis en place garantit que les sites stratégiques ne s'éteindront pas et permettront la liaison pour les fonctions essentielles.

**En complément, et pour sécuriser les NRO et les antennes identifiés comme prioritaires, il convient de mettre en œuvre la redondance des réseaux**.

Ce maillage signifie que chaque équipement stratégique est raccordé au réseau principal par au moins deux chemins physiques totalement distincts (double adduction géographique) afin de permettre une protection contre les coupures accidentelles ou malveillantes.

Le rôle de l'Arcep pour contrôler la conformité et la solidité de ces plans de crise mais également les données, parfois sensibles, des opérateurs est déterminante.

**Recommandation n°10 : Identifier les infrastructures les plus critiques (Nœuds de Raccordement Optique et antennes mobiles) et renforcer leur robustesse et leur alimentation en énergie en cas de crise**

**Recommandation n°11 : Confier à l'Arcep le contrôle des plans de crise de ces points critiques, la redondance et la robustesse de ces infrastructures les plus critiques**

### 2. Evaluer plus précisément l'origine des pannes affectant les réseaux numériques et de télécommunications

Il ressort également des auditions conduites dans le cadre du groupe de travail que les données métriques ou cartographiques sur la résilience des réseaux numériques et de télécommunications sont encore parcellaires, morcelées ou très ponctuelles.

Les membres de la CSNP préconisent de mettre à disposition des acteurs publics et privés, sur une base annuelle ou biennale, des études métriques sur la typologie des incidents affectant les réseaux numériques et de télécommunications, pour discerner ce qui relève d'un mauvais entretien ou d'une mauvaise gestion des réseaux numériques et de télécoms ou d'une crise d'origine externe aux réseaux.

Un guide a été publié par le CCED[4] pour accompagner les opérateurs relevant du Code des postes et des communications électroniques dans leur obligation réglementaire instaurée par l'article D. 98-5 du Code des postes et des communications électroniques et définir les seuils de déclaration.

Le CCED a mis en place depuis juin 2025 un outil pour recenser l'origine des incidents les plus significatifs : ce document n'est pas encore rendu public mais constituerait une base solide pour recenser la typologie des incidents affectant les réseaux de télécommunications.

Selon une étude de l'ENISA[5] à laquelle ne contribue pas la France, en 2024, la part de pannes dues aux défaillances- système représentait 60% (548 millions d'heures perdues) de l'ensemble des incidents, la part des incidents liés aux erreurs humaines représentait 19% des incidents et 402 millions d'heures perdues, la part des incidents liés à des phénomènes naturels représente 25% et 605 millions d'heures perdues pour les utilisateurs.

Les actes de malveillance représentent 10% des incidents et 214 millions d'heures perdues pour les utilisateurs.

Les réseaux mobiles, téléphonie et internet, sont les plus impactés avec respectivement 57% et 49% des incidents contre 26% pour les réseaux internet fixes.

Au final, et en tendance, la progression des incidents ne se traduit pas systématiquement par une augmentation du nombre d'heures perdues pour les usagers à l'exception des incidents liés aux catastrophes naturelles.

**Recommandation n°12 : Recenser et quantifier l'origine des pannes et des défaillances des infrastructures numériques et de télécommunications et leur impact pour les usagers**

[4] https://www.entreprises.gouv.fr/la-dge/publications/guide-pour-la-declaration-des-incidents-affectant-les-reseaux-et-les

[5] ENISA_Telecom_Security_Incidents_2024_en_1.pdf

### 3. Préciser la cartographie des zones à risque à moyen terme

Les membres de la CSNP considèrent qu'un exercice de projection est nécessaire pour adapter les infrastructures numériques et de télécommunications aux chocs et au réchauffement climatique.

Pour préparer la France aux chocs climatiques qu'elle pourra rencontrer à l'horizon 2100, le troisième plan national d'adaptation au changement climatique (PNACC) a été lancé le 10 mars 2025[6]. Ce plan prévoit des mesures pour développer une stratégie de long terme pour les réseaux de télécommunication afin d'assurer la continuité et la qualité du service.

Plusieurs mesures sont envisagées sans qu'un budget soit précisé ou alloué.

Des indicateurs ont été identifiés pour quantifier :

- le nombre de coupures de communications électroniques affectant plus de 1 000 foyers par rapport à une zone géographique à déterminer pendant plus de 4 heures,
- le nombre de coupures des services support des appels d'urgence affectant plus de 100 foyers par rapport à une zone géographique à déterminer pendant plus de 4 heures,
- le temps de rétablissement moyen des services support des appels d'urgence et le temps de rétablissement moyen des services de communications électroniques.

Les membres de la CSNP proposent qu'une cartographie soit établie sur la base de ces critères et mise à jour régulièrement pour constituer un outil opérationnel pour l'ensemble des parties prenantes (citoyens, préfets, collectivités locales, opérateurs).

**Recommandation n°13 : Anticiper et adapter les réseaux au changement climatique à moyen terme**

## V. Interdépendance des réseaux électriques et de télécommunications

Le retour d'expérience a démontré la très grande interdépendance entre les réseaux électriques, les réseaux de télécommunication fixes et mobiles et les réseaux d'eau.

Plusieurs pistes d'amélioration se dégagent pour renforcer la robustesse et l'autonomie des ces réseaux essentiels pour la population française.

### 1. Dépendance des réseaux de télécommunications au réseau électrique

Les réseaux fibres et mobiles sont plus dépendants du réseau électrique que le réseau cuivre qui est en voie de démantèlement.

Le retour d'expérience des tempêtes et des incendies récents démontre que ce sont essentiellement les problèmes de fourniture d'électricité qui ont entrainé une rupture de fonctionnement des réseaux mobiles notamment.

Globalement, les opérateurs télécoms reconnaissent que la coopération avec Enedis s'est sensiblement améliorée ces dernières années.

[6] Mesure32 - Services essentiels - Telecom.pdf

Sur la dépendance des opérateurs télécoms à la fourniture électrique, la mesure 32 du PNACC « Assurer la résilience des services de communications électroniques » prévoit de permettre aux opérateurs de communications électroniques d'obtenir des fournisseurs d'électricité :

- une mise à jour annuelle des références de points de livraison énergétique et
- en temps réel, l'état de fonctionnement de ces points de livraison.

Lors de l'audition des représentants de la FFT, la solution apportée par le PNACC ne semblait pas encore répondre aux attentes des opérateurs télécoms ou n'auraient pas encore été mises en oeuvre.

Dans son avis n°2023-07 du 18 octobre 2023 « Renforcer la couverture et la qualité des réseaux de télécommunications », les membres de la CSNP recommandaient de rendre prioritaires les raccordements électriques des infrastructures télécoms.

L'arrêté du 5 juillet 1990 prévoit en son article 2 que « lorsque, …, des délestages sont nécessaires, la satisfaction des besoins essentiels de la nation est assurée par le maintien d'un service prioritaire, compte tenu des obligations résultant des accords entre réseaux.

Ce service prioritaire doit permettre le maintien de l'alimentation en énergie électrique des hôpitaux, cliniques et laboratoires, des Installations de signalisation et d'éclairage de la voie publique jugées indispensables à la sécurité, des installations industrielles « *qui ne sauraient souffrir, sans subir de dommages, d'interruption dans leur fonctionnement, particulièrement celles d'entre elles qui intéressent la défense nationale.* »

**Recommandation n°14 : Classer les infrastructures de communications électroniques comme des infrastructures de « service essentiel » et intégrer le secteur des télécommunications dans l'article 2 de l'arrêté du 5 juillet 1990 fixant les consignes générales de délestages sur les réseaux électriques**

**Recommandation n° 15 : Développer une interface Enedis permettant en situation nominale et en temps de crise aux opérateurs télécoms de récupérer en masse et en temps réel le statut électrique des Points de Livraison Energétiques**

### 2. Dépendance d'Enedis aux réseaux de télécommunications

Dans un contexte de fin du réseau cuivre, Enedis s'appuie sur les réseaux cellulaires pour le contrôle de son réseau au niveau des postes moyennes/basses tensions. Dans un livre blanc publié en avril 2025[7], il est constaté que « *les réseaux cellulaires sont moins résilients dans un contexte de pannes électriques (multipliées par la crise climatique) que les réseaux fibres et cuivres, un enjeu partagé par les opérateurs télécom, cherchant à minimiser les temps d'indisponibilité de leurs infrastructures.* »

Après avoir étudié différentes solutions (cellulaire public 4G/5G, cellulaire privé 4G/5G, LoRA, Nb-IoT, Fibre FttO :FttH, Satelitte GEO et orbite basse), Enedis s'oriente avec ses partenaires vers le déploiement d'un réseau privé avec des antennes dédiées utilisant une fréquence basse pour permettre une couverture nationale avec un minimum de points hauts.

Pour l'opérateur électrique, la meilleure solution est à ce stade un réseau cellulaire basse fréquence résilient (bande de fréquence des 450 MHz) comme cela est le cas en Allemagne. A ce stade, le principal obstacle serait d'ordre financier. Selon les auteurs du Livre blanc, l'utilisation de la technologie sans fil 4G/5G avec 410-450 MHz devient le principal choix des entreprises de services

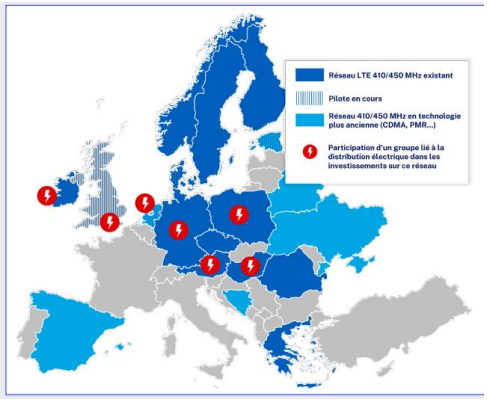
[7] Enedis_LB_012.pdf

publics à travers l'Europe. Certains pays ont déjà alloué cette partie du spectre aux besoins des services publics.

**Sans interférer avec les négociations sur les prix, les membres de la CSNP recommandent à l'Arcep de réserver le spectre 410-450 MHz aux besoins des services publics.**

**Recommandation n°16 : Réserver le spectre de basse fréquence 450 Mhz aux besoins des services publics**

CARTOGRAPHIE DES RESEAUX 410/450 MHZ EUROPEENS - (SOURCES : 450 MHZ ALLIANCE & WAVESTONE)



## VI. Résilience et enjeux posés par notre dépendance aux technologies non européennes

Selon une étude du cabinet Asteres commandée par le Cigref et rendue publique en avril 2025, 80% du total des dépenses liées aux logiciels et services cloud à usage professionnel en Europe est passé auprès d'entreprises américaines, soit un marché de l'ordre de 265 Mds d'euros.

Ce phénomène de dépendance aux solutions américaines est sans doute comparable ou encore plus importants pour les usages individuels.

### 1. Ultra-dépendance aux solutions numériques non souveraines

Cette ultra dépendance n'est pas nouvelle mais les tensions géopolitiques croissantes observées entre les Etats-Unis et le reste du monde depuis l'arrivée au pouvoir du Président Trump posent avec plus d'acuité la question du fonctionnement de nos infrastructures numériques et de télécommunications en cas de mesures unilatérales prises par le gouvernement des Etats-Unis et/ou les entreprises américaines.

Par ailleurs, ce sujet se pose également à l'égard des solutions chinoises sur certains segments des infrastructures numériques et de télécommunications.

**Pour les membres de la CSNP, la résilience des infrastructures numériques et de télécommunications passe par une diversification des sources d'approvisionnement en solutions IT, afin de garantir la disponibilité, l'intégrité et la confidentialité des systèmes et des données dans la durée en investissant dans des solutions européennes crédibles.**

A cet égard, les membres de la CSNP saluent l'initiative Eurostack[8] portée par L'Allemagne, les Pays-Bas et la France en faveur d'une politique industrielle du numérique permettant à l'Union européenne de réduire sa dépendance à l'égard des fournisseurs non européens de technologies et notamment le renforcement des infrastructures numériques européennes, une stratégie d'achat public « Europe d'abord » et une orientation open-source pour renforcer la collaboration au sein des communautés européennes.

**Mais, cette initiative ainsi que les plans d'investissement et de soutien aux écosystèmes français et européens pour faire émerger des champions européens dans le domaine de l'intelligence artificielle et du quantique s'inscrit sur le moyen voire le long terme.**

S'agissant plus particulièrement de **la virtualisation croissante des réseaux de télécommunications**, l'utilisation de réseaux définis par logiciel (SDN) et de virtualisation des fonctions réseau (NFV) permet aux opérateurs de virtualiser leurs fonctions et services réseau, les rendant ainsi plus agiles et efficaces et leur permet de rationaliser les opérations et à réduire les coûts.

**Les membres de la CSNP notent que l'Arcep suit cette évolution avec attention et souhaiteraient disposer d'une étude détaillée sur la dépendance des opérateurs d'infrastructures critiques aux solutions numériques non souveraines.**

### 2. Des solutions satellitaires européennes face à la concurrence avec Starlink

**Dans le domaine satellitaire**, le cyclone Chido à Mayotte a démontré notre dépendance aux solutions proposées par les satellites en orbite basse de Starlink. L'audition de la Fédération française des

[8] The White Paper - EuroStack

télécoms à laquelle participait un représentant d'Eutelsat a permis d'éclairer les membres de la CSNP sur le niveau de préparation du groupe européen pour offrir des solutions alternatives à Starlink.

### 3. Dépendance aux métaux rares et critiques

Sur la dépendance de notre pays aux métaux rares et critiques, les membres de la CSNP demandent au Ministre en charge de l'intelligence artificielle et du numérique d'étudier la faisabilité et la mise en œuvre du projet French Met' qui propose une solution de stock stratégique de métaux à destination des industriels français et d'étudier les différents scénarios qui pourraient répondre à une décision unilatérale ou un incident majeur qui priverait le secteur des télécommunications et plus largement du numérique.

**Recommandation n°17 : Identifier et mesurer la dépendance de nos infrastructures aux solutions numériques non souveraines**

**Recommandation n°18 : Etablir précisément les risques de dépendance liés à la virtualisation des réseaux télécoms**

**Recommandation n°19 : Initier au niveau européen la constitution de stocks stratégiques de métaux critiques**

## VII. Le financement de la résilience des réseaux numériques et de télécommunications

Les membres de la CSNP considèrent que **la dotation budgétaire du Réseau radio du Futur qui a pour objet d'offrir une connectivité très haut débit via un accès 4G et 5G aux services de sécurité en s'appuyant sur des réseaux de référence et des réseaux tactiques projetables doit être préservée des coupes budgétaires.**

Dans un rapport rendu public le 22 juin 2022, la fédération Infranum a fait un certain nombre de propositions pour renforcer le niveau de résilience des infrastructures existantes et le niveau de sécurité des sites très sensibles (Datacenters, points de présence, nœuds de raccordement optique). Face à la fragilité des infrastructures aériennes, l'enfouissement d'une partie significative des lignes apparait à la fédération comme une solution qui doit être étudiée. Le coût de ces opérations estimé par la filière est de l'ordre de 10 Mds €[9].

**Sur l'enfouissement des lignes aériennes, les membres de la CSNP observent qu'il n'y a pas de consensus sur ce point et qu'en cas d'incendie, de glissement de terrain, d'inondations, l'enfouissement des lignes ne constitue pas nécessairement une solution pour rétablir les réseaux de télécommunications.**

A l'évidence, **le choix de l'enfouissement des lignes est un sujet qui doit s'apprécier au niveau local en fonction des particularités climatiques et topographiques.**

De ce point de vue, le témoignage de M. Nicolas Tarbes, vice-président du Syndicat mixte Gironde numérique, au cours du TRIP d'automne 2023 de l'AVICCA est très éclairant sur les options et les enjeux qui se présentent en réalité aux collectivités locales et aux entités délégantes :

- Un premier scénario de sécurisation des sites clés (3 à 4 millions d 'euros) permet de traiter un tiers de la résilience du réseau local de fibre optique d'une valeur vénale de 2 Mds d'euros.

[9] Dans une étude plus récente, Infranum a évalué entre 6,9 Mds d'euros et 16,9 Mds d'euros les besoins en financements de la résilience des réseaux.

- Un deuxième scénario qui permet l'enfouissement des câbles de desserte notamment permet de traiter la moitié de la résilience pour un investissement de 64 millions d'euros, un investissement qui n'est plus à la portée du syndicat mixte
- Un troisième scénario (enfouissement des câbles de desserte, double adduction électrique des NRO, etc) représente un investissement de 240 millions d'euros à lisser sur 10 ans mais toujours hors de portée du syndicat mixte
- Une quatrième option correspondant à 100% d'enfouissement représente 1 Md d'euros pour un RIP dont le cout total s'est élevé à 740 millions d'euros pour raccorder 510 000 raccordés.

En 2022, la Banque des Territoires avait annoncé qu'elle serait en mesure de mobiliser des financements avec un amortissement sur le long terme (30 à 50 ans).

**Dans son avis du 27 juillet 2022, la CSNP appelait l'Etat et l'ARCEP, en liaison avec les opérateurs d'infrastructures et de génie civil, à lancer au plus tôt des travaux d'évaluation reposant sur des études solides et indépendantes.**

La CSNP considérait qu'il était essentiel d'anticiper les coûts d'entretien et de sécurisation des réseaux et des infrastructures télécoms. La CSNP appelait déjà à la mise en place d'un mécanisme de péréquation nationale (Recommandation n°6).

**Cette position constante de la CSNP, encore récemment rappelée dans un avis du 9 octobre 2025, rejoint la position de l'AVICCA et de la FNCCR sur la création d'un fonds d'aménagement numérique du territoire.**

Dans la contribution communiquée à la CSNP, la FNCCR estime que le financement de la résilience doit passer :

- soit par un plan de cofinancement succédant au Plan France Très Haut Débit qui présenterait l'avantage de structurer et unifier la procédure de « mise en résilience » des réseaux FTTH,
- soit par un fonds de péréquation sur le modèle du Fonds d'aménagement numérique des territoires (FANT) introduit par la loi n°2009-1572 du 17 décembre 2009 et qui n'a jamais vu le jour, faute de volonté politique et de décret d'application.

En tout état de cause, les membres de la CSNP souhaitent que les atermoiements sur le financement de la résilience des réseaux et la péréquation financière qu'ils jugent absolument nécessaire soient levés au plus tôt.

**Recommandation n° 20 : Sanctuariser sur le long terme les moyens budgétaires des services d'urgence, du réseau radio du futur et de l'ACMOSS**

**Recommandation n°21 : Mettre en place un fonds de résilience sur le modèle du fonds Barnier**

**Recommandation n°22 : Mobiliser les instruments financiers européens sur la résilience des réseaux et les infrastructures numériques et de télécommunications**

## VIII. Le développement exponentiel de l'intelligence artificielle et des centres de données : anticiper les conflits d'usage

L'intensification des usages liés à l'intelligence artificielle, et singulièrement de l'intelligence artificielle générative, mais également le déploiement des centres de données sur le territoire national posent à moyen terme des conflits d'usage dans l'accès aux sources d'énergie mais également à l'eau.

C'est notamment ce qu'il ressort des auditions des représentants de l'ADEME et du Shift Project, mais également de la publication du rapport « Intelligence artificielle, données, calculs : quelles infrastructures dans un monde décarboné ? » publié par le Shift Project le 1er octobre 2025[10].

### 1. Accélération de la progression de la consommation électrique des centres de données

Entre 2005 et 2024[11], la consommation électrique annuelle liée aux centres de données est passée de 120 TWh à 420 TWh. Cette dynamique est principalement alimentée par les Etats-Unis qui consacrent 4,5% de leur consommation électrique nationale aux centres de données.

Selon le Shift Project, sans évolution majeure dans les dynamiques actuelles, à l'horizon 2030, la consommation électrique des centres de données mondiaux pourraient atteindre 1250 TWh à 1500 TWh. A l'horizon 2035, cette plage pourrait encore s'étendre, entre 2250 TWh et 3000 TWh.

Cette évolution s'explique par la dynamique des usages numériques « conventionnels » (hébergement des sites web, jeux en ligne, réseaux sociaux, service cloud, vidéo à la demande, stockage et traitement des données d'entreprise, intelligence artificielle « traditionnelle ») mais également par l'émergence accélérée de l'intelligence artificielle générative et le développement des cryptomonnaies.

**La proportion de l'intelligence artificielle dans l'ensemble des usages des centres de données représenterait 15% en 2025[12] mais 55% en 2030, soit une progression exponentielle.**

Selon l'Arcep, cette progression de l'intelligence artificielle aura également des effets importants sur la saturation des réseaux à large bande passante et à faible latence.

Selon l'ADEME, en France, la consommation électrique du secteur numérique est estimée à 51,5 TWh pour l'année 2022, soit 11% de la consommation électrique française. En prenant en compte la consommation électrique des centres de données situés à l'étranger qui hébergent des usages français, la consommation totale serait de 65 TWh.

Force est de constater qu'il existe des différences notables entre les estimations de l'ADEME, de l'Arcep et de RTE.

**Comme le propose le Shift Project, il parait essentiel de mettre en place des mécanismes robustes pour mesurer et identifier avec précision les capacités et les consommations liés aux usages de l'IA et des centres de données selon une périodicité régulière.**

[10] Intelligence artificielle, données, calculs : le rapport final du Shift - The Shift Project
[11] Energy | IIEA
[12] Energy | IIEA

## 2. Anticiper les conflits d'usage : un débat de fond est nécessaire

- Conflits d'usage en matière de consommation électrique

La consommation électrique additionnelle des centres de données en 2035 par rapport à 2020 représenterait entre 10% et 23% supplémentaires d'électricité consommée en 2035 par rapport à 2020. En 2035, la consommation des centres de données pourrait atteindre 7,5% de la consommation totale d'électricité, contre seulement 2% aujourd'hui.

**Cette progression pose très clairement la question de la disponibilité de l'électricité consommée en France et donc les conflits d'usage entre les acteurs et les activités.**

- Conflits d'usage en matière de gestion de l'eau

Les centres de données nécessitent des circuits de refroidissement et le maintien d'un taux d'humidité constant pour maintenir la performance des serveurs. Ces systèmes de refroidissement entrainent une consommation directe ou indirecte d'eau (refroidissement par climatisation, *free cooling*, *indirect liquid cooling* et *direct liquid cooling*, *immersion cooling*).

L'usage majoritaire porte sur l'eau potable, et dans une moindre mesure sur des eaux grises ou de l'eau de mer, et entre donc directement en concurrence avec les usages domestiques, agricoles et industriels de ces ressources menacées par le stress hydrique.

A l'occasion des auditions et des travaux, les rapportrices ont pu mesurer les enjeux posés par les potentiels conflits d'usage du numérique et leurs conséquences sur la résilience des infrastructures des réseaux numériques et de télécommunications.

Sans entrer dans le champ direct de la résilience, pour les membres de la CSNP, ces sujets nécessitent **un débat et une meilleure information du public sur les usages.**

Que ce soit pour l'usage de l'IA mais également pour la vidéo à la demande, le streaming et les jeux vidéos, le grand public n'a pas pleinement conscience de l'impact de ses usages sur notre consommation d'énergie et en ressources naturelles.

Des campagnes d'information sont nécessaires et pourraient être organisées à grande échelle.

**Recommandation n°23 : Mettre en place des mécanismes robustes pour mesurer avec précision les capacités et les consommations électriques liés aux usages de l'IA et des centres de données**

**Recommandation n°24 : Favoriser un débat public sur les usages critiques du numérique**

**PERSONNES AUDITIONNEES**

**ACMOSS -** M. Guillaume LAMBERT, Directeur de l'Agence des communications mobiles opérationnelles de sécurité et de secours

**ADEME**

M. Mathieu WELLHOFF, Chef de service Sobriété numérique

Mme Julia MEYER, Ingénieure numérique responsable

**Association française des utilisateurs des télécoms (Afutt)**

M. Bernard DUPRE, Président

M. Alain GERARDIN, Vice-président

M. Pierre-Yves HEBERT, Vice-président

**ANCT**

M. Bastien COLLET, Directeur des programmes France Mobile et France Très Haut Débit

M. Florian TOLLET, Chef de projet - Programme France Très Haut Débit

**Arcep**

M. Ghislain HEUDE, Directeur de la direction « Fibre, infrastructures et territoires »

M. Valentin MUGNIE, Chef de l'Unité territoires connectés

**Avicca**

M. Ariel TURPIN, Délégué général

M. Thierry JOUAN, Délégué général adjoint

**Commissariat aux communications électroniques de défense (**CCED**)**

Mme Carine BEDUZ, Cheffe du pôle des communications d'urgence

Mme Anne-Sophie COLOMB, adjointe au pôle communications d'urgence, cheffe de projet Résilience

**ENEDIS**

M. Vincent DUFOUR, Directeur des affaires publiques

M. Laurent PERRAULT, Directeur Exploitation Systèmes et Chaînes Communicantes

**IELO** - Mme OLSZANSKI, Directeur marketing des ventes

**INFRANUM**

Mme Ilham DJEHAICH-MEZOUAR, Présidente

Mme Marlène KURZ, chargée d'affaires publiques et internationales

**Fédération française des télécoms**

M. Romain BONENFANT, Directeur Général

M. Arnaud BALLET, Directeur des affaires publiques

**Orange**

Mme Pauline CAYATTE, Directrice des relations institutionnelles

M. Antoine FAILLIE, Directeur Stratégie et Réseau Mobile

**SFR -** Mme Camille BALL, Responsable Affaires Publiques

**Bouygues Télécoms** – M. Corentin DURAND, Responsable Affaires Publiques

**Eutelsat** – M. Etienne LESOEUR, Directeur des affaires institutionnelles

**Green IT -** M. Frédéric BORDAGE, Fondateur

**Shift Project -** M. Hugues FERREBOEUF, Chef de projet Numérique

**CONTRIBUTIONS TRANSMISES A LA CSNP**

Agence nationale de la cohésion des territoires - ANCT
AXIONE
Commissariat aux communications électroniques de défense - CCED
Direction générale des entreprises - DGE
Direction générale de la sécurité civile et de la gestion des crises - DGSCGC
Fédération nationale des collectivités concédantes et régies - FNCCR

## BIBLIOGRAPHIE

ANCT et Banque des Territoires « Elaborer son schéma local de résilience » Novembre 2023

Arcep « Réseaux du futur - Note de synthèse : la résilience des réseaux de communications électroniques » Mai 2025

AVICCA « Définir une stratégie de résilience des réseaux FttH : un impératif face à la multiplication des risques »

Cour des comptes « Les soutiens publics en faveur du déploiement de la fibre optique » Communication à la commission des finances du Sénat – Avril 2025
CREDO

Enedis, Orange, Nokia, EDF et Wavestone « La résilience des réseaux cellulaires en soutien à la résilience des réseaux électriques » Avril 2025

ENISA - TELECOM SECURITY INCIDENTS 2024 – Juillet 2025

Infranum « Résilience des réseaux FttH »

SGDSN – Revue nationale stratégique 2025