arcep
autorité de régulation
des communications électroniques,
des postes et de la distribution de la presse

RÉPUBLIQUE FRANCAISE

RÉSEAUX DU FUTUR

Note de synthèse : la résilience des réseaux de communications électroniques

Mai 2025

ISSN n°2258-3106

La démarche « Réseaux du futur » de l'Arcep et son comité scientifique

Quels formats les réseaux du futur pourraient-ils adopter ? Quelles en seront les incidences sur le métier de régulateur de l'Arcep ? Quels pourraient être les nouveaux acteurs ou l'évolution des modèles économiques dans les secteurs régulés par l'Autorité ?

Pour alimenter ce travail prospectif et disposer d'un regard à 360° sur ces évolutions, sur un horizon de 5 à 10 ans, l'Arcep a demandé à douze personnalités qualifiées du monde académique, entrepreneurial et industriel, dans divers domaines d'expertise, de se joindre à elle dans un comité scientifique. Et pour que la réflexion soit complète, les équipes de l'Arcep échangent également avec des acteurs spécialisés de l'écosystème : opérateurs, équipementiers, acteurs d'internet, fournisseurs de service, acteurs d'internet ou encore collectivités territoriales.

L'Arcep restitue au fil de l'eau ces travaux en produisant des notes thématiques, accessibles à tous sur son site, afin d'éclairer le débat public.

Jean-Luc Beylat
VP Ecosystem, Nokia

Eric Brousseau
Professeur, Université Paris-Dauphine

Giovanna Carofiglio
Senior Director, Cisco

Grazia Cecere
Professeure, Institut Mines Télécom

Mélanie Dulong de Rosnay
Directrice de recherche, CNRS

Serge Fdida
Professeur, Sorbonne Université

Yves Gassot
Consultant indépendant

Nolwenn Germain
Présidente fondatrice, HAIDO

Isabelle Hilali
CEO fondatrice, datacraft

Christian Licoppe
Directeur département, Institut Polytechnique Paris

Françoise Soulié-Fogelman
Conseillière scientifique, Hub France IA

Vous pensez pouvoir contribuer à ces travaux ?

Cette réflexion se veut « vivante », l'Arcep invite tous ceux qui le souhaitent à s'approprier ces analyses et à lui envoyer des contributions sur reseaux-du-futur@arcep.fr

Vous souhaitez être informé des prochaines présentations de notes thématiques ?

Demandez à être invité à com@arcep.fr.

Où lire les autres notes thématiques ?

A la date de publication de la présente note (mai 2025), une première note a déjà été publiée : « L'informatique au cœur des réseaux télécoms » (octobre 2024).

« La résilience des réseaux de communications électroniques »

Note de synthèse n°2 du cycle de réflexion « Réseaux du futur » – mai 2025

1 Contexte et enjeux

L'importance, toujours croissante, des réseaux de communications électroniques dans l'accès des Françaises et Français à la vie économique, sociale et citoyenne n'étant plus à démontrer, le bon fonctionnement des réseaux et la capacité des opérateurs à rétablir le service dans les meilleurs délais en cas de panne, sont essentiels. La résilience des réseaux constitue ainsi un enjeu majeur pour l'ensemble de notre économie et de la société dans son ensemble. L'Arcep l'a ainsi mentionnée parmi les objectifs de sa revue stratégique « Ambition 2030 » publiée en janvier 2025.[1]

Cette note a pour vocation d'exposer certaines menaces qui pèsent sur les réseaux de communications électroniques, qu'elles soient nouvelles, d'ampleur inédite ou de fréquence plus élevée. Son objectif est de pouvoir appréhender les enjeux associés en matière de résilience et permettre à chacun, opérateurs et autorités publiques, de prendre des décisions éclairées. Elle met en exergue un certain nombre de bonnes pratiques visant à améliorer la résilience des réseaux qui ont pu être recueillies lors des différents entretiens, lectures et participations à des conférences.

Elle se concentre sur trois grands types de risques qui ont des effets significatifs sur la résilience des réseaux et services de communications électroniques :

- les risques organisationnels avec, d'une part, une **chaîne de valeur qui se fragmente** – l'époque où les infrastructures étaient exploitées sur un périmètre national par un nombre réduit d'opérateurs étant désormais révolue – et, d'autre part, un probable **accroissement de la concurrence pour l'accès aux ressources stratégiques** nécessaires au bon fonctionnement des réseaux et donc à leur résilience ;
- les risques technologiques liés, d'une part, à la criticité des infrastructures **physiques de connectivité sous-marine,** qu'il convient de sécuriser, et, d'autre part, aux **changements structurels des réseaux induits** par la virtualisation et la programmation logicielle des réseaux ;
- les risques naturels avec le **changement climatique** (hausse de la température, montée des eaux, intensification et allongement des canicules, évolution des régimes des précipitations, évènements climatiques plus intenses, plus fréquents et plus longs) dont les conséquences sur les infrastructures de réseaux, notamment de communications électroniques, constituent un enjeu central de la résilience de nos sociétés.

Ces problématiques s'inscrivent dans la durée et supposent que les parties prenantes se dotent d'une stratégie de résilience, parfois sur plusieurs décennies, accompagnée de déclinaisons opérationnelles mises en oeuvre progressivement.

D'autres types de menaces pourraient avoir des conséquences notables en matière de disponibilité des réseaux et des services mais elles ne sont pas traitées dans cette note dans la mesure où elles font déjà l'objet de mesures ou d'études spécifiques par d'autres services de l'État. C'est notamment le cas des cybermenaces, des dégradations volontaires de réseau ou des risques de pénurie électrique.

2 La résilience des réseaux

Quelles que puissent être les obligations de permanence et de disponibilité attachées à l'exploitation des réseaux de communications électroniques, ces réseaux peuvent être confrontés à des événements exceptionnels susceptibles de dégrader très fortement leur fonctionnement.

[1] https://www.arcep.fr/actualites/actualites-et-communiques/detail/n/voeux-arcep-2025-janvier2025.html

Si, par le passé, les réseaux de communications électroniques ont globalement réussi à surmonter les crises auxquelles ils ont été soumis pour retrouver un fonctionnement normal, il est toutefois indispensable de se projeter dans l'avenir, d'anticiper l'évolution des risques (leur nature, leur fréquence et leur intensité) et de s'y préparer pour en atténuer les effets.

C'est le but des travaux sur la résilience des réseaux qui visent à améliorer leur capacité à résister, à absorber et à corriger les effets de perturbations ponctuelles de natures diverses et à revenir à une situation de fonctionnement nominal le plus rapidement possible.

Cette résilience se fonde notamment sur :

- **une sécurisation du réseau** : mise en place des redondances, bouclages, reconfiguration automatique du réseau en cas d'incident, etc.
- **l'anticipation des risques et leur atténuation** : à partir d'une analyse des risques susceptibles d'impacter l'infrastructure, il est opportun d'identifier les vulnérabilités de leurs équipements, de définir et de mettre en œuvre des plans de renforcement adaptés ;
- **une gestion de crise adaptée à ces risques** : outre le renforcement des infrastructures, il est indispensable de se préparer aux crises avant qu'elles ne surviennent et d'établir une organisation efficace : identifier les acteurs et répartir les rôles ; définir des processus, une gouvernance et un fonctionnement adaptés ; diffuser cette planification auprès des personnels ; instaurer une culture de la gestion de crise au sein de l'organisation ; mettre en place des tests et des exercices de simulation ; prévoir les procédures de restauration ou de remplacement des équipements ; dresser les retours d'expérience adaptés afin d'améliorer lesdites procédures.

Mandaté par le cabinet de la Première ministre, le secrétariat général de la défense et de la sécurité nationale[2] (SGDSN) a conduit fin 2021 les travaux interministériels de préparation de la stratégie nationale de résilience « SNR ».

La SNR est une démarche opérationnelle qui vise à mieux préparer la France, ses entreprises et ses citoyens aux divers chocs, à « tenir dans la durée, collectivement et en profondeur face aux crises » quelle qu'en soit l'origine. Elle vise à mettre en cohérence l'ensemble des actions publiques déjà mises en œuvre et à identifier les nouvelles actions à mener. Elle a notamment pour objectif de décliner les objectifs, les indicateurs associés et les éventuelles difficultés des actions identifiées.

Elle érige le secteur des communications électroniques comme l'une des 12 activités clés[3] de la résilience nationale.

Par ailleurs, le troisième Plan d'adaptation au changement climatique (PNACC-3) soumis à consultation public fin 2024 identifie une mesure spécifique visant à « Assurer la résilience des services de communications électronique ».[4]

[2] https://www.sgdsn.gouv.fr/files/files/1.%2020220315_NP_SGDSN_Document%20cadre_SNR_FR_0.pdf

[3] Poste et communications électroniques, numérique, énergies, international, économie, social et sociétal, alimentation et eau, sécurisation, transports, justice, sanitaire, défense militaire du territoire.

[4] PNACC-3, mesure 32 https://consultation-pnacc.ecologie.gouv.fr/sites/default/files/2024-10/Mesure32%20-%20Services%20essentiels%20-%20Telecom.pdf

3 Risques organisationnels

3.1 Fragmentation des acteurs impliqués dans l'exploitation des réseaux de communications électroniques

L'ouverture à la concurrence du secteur des télécoms a vu la création de nombreux opérateurs commerciaux dont les offres reposaient essentiellement sur les infrastructures nationales d'un nombre réduit d'opérateurs. Ces derniers étaient responsables de l'exploitation, de la maintenance, de la sécurisation et des stratégies de résilience de leurs infrastructures.

Ce modèle est fortement remis en question tant sur les réseaux d'accès fixes, mobiles que sur le cœur de réseau. L'écosystème des infrastructures de réseaux connaît ainsi des évolutions qui doivent être pleinement intégrées dans l'élaboration et la mise en œuvre des politiques de résilience.

3.1.1 Tendances observées

a) Concernant les réseaux d'accès fixe, l'unique réseau national d'accès cuivre cède la place à une multiplicité d'opérateurs locaux d'infrastructures en fibre optique

Par le passé, la principale technologie d'accès utilisée en matière de réseaux fixes de communications électroniques était le réseau de cuivre : ce réseau était géré par un unique opérateur, Orange, qui y donnait accès à ses concurrents, mais en était l'unique exploitant.

Avec les objectifs nationaux et européens de transition vers le très haut débit, et le lancement du Plan France Très haut Débit (ci-après « PFTHD »), a été acté le déploiement massif de la fibre optique en tant que technologie d'accès en raison de ses meilleures performances. Le réseau cuivre a, quant à lui, vocation à être fermé à l'horizon 2030.

Compte tenu des investissements nécessaires, le cadre de déploiement de la fibre optique a été élaboré pour favoriser la mutualisation de la partie terminale des réseaux et pour articuler investissements privés et investissements publics dans le respect des règles relatives aux subventions publiques.

Dans les zones les plus denses, plusieurs opérateurs d'infrastructure privés coexistent pour raccorder l'ensemble des utilisateurs.

Dans les zones dites « AMII[5] » ou « AMEL[6] », un seul opérateur d'infrastructure privé déploie et exploite, sur fond propre, un réseau fibre.

Enfin, dans la grande majorité du territoire le déploiement de la fibre relève d'un mixte d'investissements publics et privés au travers de réseaux d'initiative publique (« RIP »), portés par des collectivités principalement dans le cadre du PFTHD. Ces RIP peuvent avoir des montages juridiques divers, dans lesquels plusieurs acteurs interviennent : par exemple, dans certains montages en affermage, la construction du réseau est du ressort de la collectivité ; dans les régies, l'exploitation et la construction du réseau sont réalisées en propre par les collectivités ; dans d'autres cas, les collectivités créent une société publique locale (SPL) délégataire du réseau, qui elle-même peut sous-traiter l'exploitation du réseau à un partenaire privé ; dans d'autres cas encore, le RIP confie la conception, la réalisation des travaux et l'exploitation du réseau à un concessionnaire.

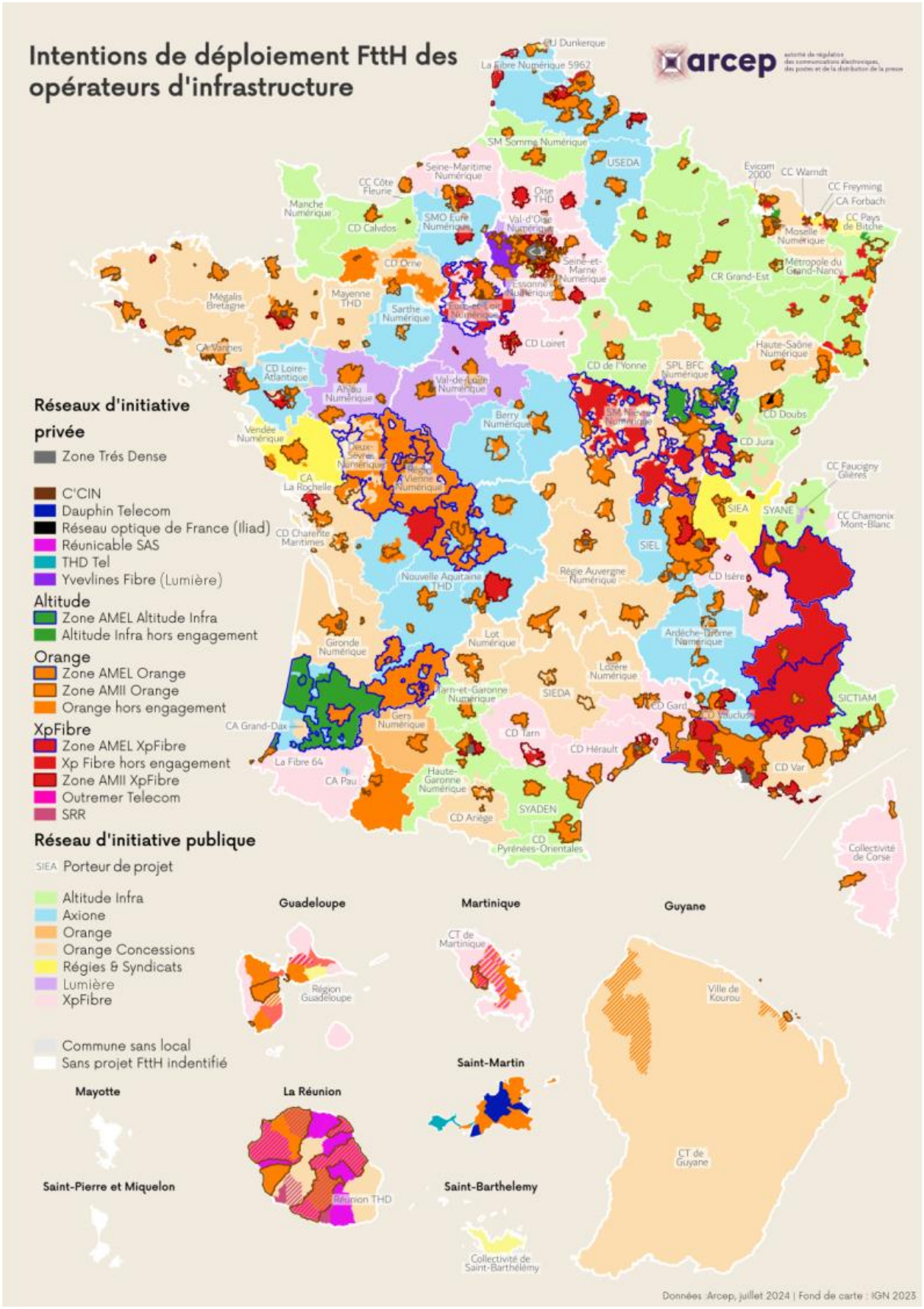
Ainsi, cette organisation du déploiement des réseaux en fibre optique a entraîné une démultiplication du nombre d'opérateurs déployant et exploitant ces réseaux sur le territoire national. Ainsi des

[5] Appel à manifestation d'intention d'investissement

[6] Appels à manifestation d'engagements locaux

opérateurs dits « intégrés » (présents sur les marchés de gros et de détail), tels Orange, SFR ou Free, coexistent avec des opérateurs d'infrastructure spécialisés, tels Axione, Lumière et Altitude notamment. Ces derniers n'interviennent pas sur le marché de détail mais proposent leurs offres d'accès sur le marché de gros à des opérateurs dits « commerciaux ». C'est notamment à ce type d'opérateurs que les collectivités confient le déploiement et l'exploitation des RIP.

La carte ci-après identifie les différents opérateurs d'infrastructure et notamment ceux exploitant les réseaux d'initiative publique.


Intentions de déploiement FttH des opérateurs d'infrastructure
arcep
Réseaux d'initiative privée
Zone Très Dense
C'CIN
Dauphin Telecom
Réseau optique de France (Iliad)
Réunicable SAS
THD Tel
Yvevlines Fibre (Lumière)
Altitude
Zone AMEL Altitude Infra
Altitude Infra hors engagement
Orange
Zone AMEL Orange
Zone AMII Orange
Orange hors engagement
XpFibre
Zone AMEL XpFibre
Xp Fibre hors engagement
Zone AMII XpFibre
Outremer Telecom
SRR
Réseau d'initiative publique
SIEA Porteur de projet
Altitude Infra
Axione
Orange
Orange Concessions
Régies & Syndicats
Lumière
XpFibre
Commune sans local
Sans projet FttH indentifié
Guadeloupe
Martinique
Guyane
Mayotte
La Réunion
Saint-Martin
Saint-Pierre et Miquelon
Saint-Barthelemy
Données :Arcep, juillet 2024 | Fond de carte : IGN 2023

Par ailleurs, plusieurs opérateurs (de grande taille, comme de taille plus modeste) déploient des réseaux de fibre optique dédiés (réseaux dits « BLOD ») spécifiquement destinés aux clients « entreprises ».

Ainsi, contrairement à l'écosystème cuivre, les infrastructures de fibre optique sont exploitées par de multiples opérateurs, ce qui accroît d'autant le nombre d'acteurs et d'interlocuteurs concernés par la résilience des réseaux et des services de communications électroniques.

b) Pour les réseaux mobiles, les opérateurs mutualisent certaines de leurs infrastructures et en externalisent certaines autres à de nouveaux acteurs

Afin d'améliorer la couverture de certaines zones du territoire et notamment résorber les zones blanches, des mutualisations d'infrastructures se sont développées entre opérateurs mobiles. Ce faisant, il apparaît que, dans certains territoires, les infrastructures permettant à différents opérateurs d'offrir un service à leurs abonnés ne sont pas redondantes et ne peuvent être utilisées comme alternatives en cas de dysfonctionnement de l'une d'entre elles, notamment pour l'acheminement des communications des forces de sécurité et de secours ainsi que des communications d'urgence des utilisateurs finals vers le 112.

Par ailleurs, historiquement propriétaires des sites où ils implantaient leurs antennes, la plupart des opérateurs mobiles ont, au cours des dernières années, cédé ou externalisé tout ou partie de leurs pylônes à des sociétés spécialisées, les *« tower companies »* (ou *towercos*), devenant ainsi dépendant de la gestion qu'ils en feront[7].

c) La virtualisation des cœurs de réseau

Certains fournisseurs de cloud, notamment ceux désignés en tant qu' « *hyperscalers*[8] *»* (Microsoft Azure, Google Cloud et Amazon Web Services) sont désormais en mesure de fournir aux opérateurs physiques et virtuels des offres, dites de « *telco cloud »*, pour l'hébergement de fonctions de cœur de réseau, telles que celles relevant du plan de transport et de gestion des flux du plan utilisateurs.

NTT DOCOMO au Japon[9] et Telefonica en Allemagne[10] ont chacun annoncé au cours du premier semestre 2024 leur projet de recourrir aux infrastructures d'AWS pour l'exploitation de leur cœur de réseaux 5G.

3.1.2 Enjeux et problématiques associés

a) De nouveaux acteurs à prendre en compte dans le cadre des obligations relatives à la résilience des réseaux

Les différents maillons de la chaîne d'acteurs impliqués dans la fourniture des services de communications électroniques ont un rôle à jouer pour en assurer la sécurité et la résilience. Ce rôle est corrélé à l'ampleur de l'effet que peut entraîner leur éventuelle défaillance sur la disponibilité des services.

---

[7] 70% des sites d'antennes en France ne sont plus la pleine propriété des opérateurs télécoms.

[8] L'*hyperscale* est un terme d'informatique qui qualifie la capacité d'une architecture à évoluer de manière juste et efficace à un accroissement de demande. Les *hyperscalers* sont des entreprises qui offrent ce type de service, pour de l'informatique en nuage en particulier (notamment AWS, Microsoft et Google).

[9] https://press.aboutamazon.com/aws/2024/2/ntt-docomo-selects-aws-to-deploy-nationwide-5g-open-radio-access-network

[10] https://www.reuters.com/business/media-telecom/amazon-breaks-into-europe-5g-networks-with-telefonica-cloud-deal-2024-05-08/

Chaque opérateur, fixe comme mobile, est légalement tenu de prendre « *toutes les dispositions techniques et organisationnelles nécessaires pour assurer la sécurité de son réseau et de ses services à un niveau adapté au risque existant* »[11].

La satisfaction de ces obligations s'apprécient toutefois, pour des raisons de proportionnalité, au regard de la criticité des réseaux considérés, des risques identifiés et des mesures de sécurité à mettre en œuvre.

Le réseau de boucle locale cuivre exploité depuis près de 50 ans par un unique opérateur national dispose de stratégies de résilience éprouvées, tant du point de vue de la sécurisation du réseau que de l'identification des risques et de la gestion de crise. A noter par ailleurs que ce réseau d'accès cuivre se différencie de ses successeurs par la téléalimentation électrique qu'il fournit via la ligne téléphonique qui permettait historiquement aux utilisateurs finals de continuer à communiquer en cas de défaillance électrique, sous réserve de disposer d'un téléphone capable de l'utiliser.

Les opérateurs d'infrastructure fibre n'ont, au contraire, été confrontés aux problématiques de résilience que de manière récente.

Les opérateurs mobiles de dimension nationale qui exploitent des réseaux de générations successives depuis plusieurs décennies, ont pu, à l'instar du réseau cuivre, se familiariser avec les problématiques de résilience et ajuster leurs processus d'exploitation à ces contraintes. Toutefois, ils pourraient être en partie dépendants de la résilience des réseaux de fibre optique, en ce qu'ils utilisent ces réseaux pour acheminer le trafic d'une partie de leurs antennes mobiles jusqu'aux cœurs de réseau. Ainsi, un incident sur le réseau fixe peut avoir un impact sur les communications mobiles, quand bien même celles-ci sont redondées physiquement (par un lien secondaire en faisceau hertzien) et géographiquement (par un équipement à proximité qui prend le relais).

Par ailleurs, compte tenu de l'émergence de nouveaux acteurs impliqués dans l'exploitation d'infrastructures de communications électroniques (*Towercos,* fournisseurs d'offres *telcocloud*), une revue des obligations de l'ensemble des acteurs impliqués permettrait de s'assurer que tous disposent d'obligations appropriées et proportionnées au regard de l'objectif de sécurisation et de résilience et, le cas échéant, d'adapter ou préciser les règles.

Il pourrait également être envisagé de demander aux acteurs les plus critiques de publier des données permettant, en cas de crise, d'informer le public des délais de remise en service anticipés.

De plus, l'émergence de ces nouveaux acteurs pourrait susciter des réflexions quant à une éventuelle extension de la liste des acteurs considérés comme opérateurs d'importance vitale (OIV) pour les communications électroniques.

Ainsi, il serait opportun que les autorités gouvernementales compétentes mènent une revue des obligations de résilience applicables à l'ensemble des acteurs liés aux infrastructures de communications électroniques pour s'assurer que le cadre de protection des infrastructures prend bien en compte les évolutions de la chaîne de valeur et, le cas échéant, instruire l'opportunité d'imposer aux acteurs les plus critiques un niveau d'exigence minimal en terme de résilience ou de qualité de service.

[11] Article D. 98-5 du CPCE

b) Des autorités locales à sensibiliser pour intégrer ces nouveaux acteurs dans leurs stratégies de résilience et de gestion de crise

Le plan « ORSEC / RETAP RESEAUX[12] » qui vise à planifier l'organisation de la réponse de sécurité civile dans le but de secourir les personnes, de protéger les biens et l'environnement en proposant la réponse opérationnelle la plus efficace possible en situation d'urgence, décrit une vision des réseaux de communications électroniques qui n'est plus d'actualité :

« *Ouvert à la concurrence, le réseau des télécommunications est animé par 4 opérateurs (Orange, SFR, Bouygues Telecom, Free) qui assurent aux abonnés, selon la couverture : - Les communications téléphoniques ; - Les transmissions de données ; - L'accès à Internet.* »

Si les opérateurs de réseaux mobiles sont bien identifiés, il n'en est pas de même pour les opérateurs d'infrastructure fibre.

Il est essentiel que les autorités, nationales et territoriales, prennent conscience de la multiplicité et des spécificités des acteurs responsables des infrastructures de communications électroniques et les intègrent pleinement dans leurs réflexions et planification en matière de résilience et de sécurité des réseaux.

Dans son audit de résilience réalisé en 2023[13], Gironde Numérique avait notamment fait état, s'agissant de la gestion de crise liée aux incendies, de la mention suivante : « *Gironde Numérique non contacté par les services de l'État : la multiplication des acteurs freine une action efficace (Etat / services de secours / ENEDIS / Opérateurs d'infras de fibre / opérateurs mobiles)* ».

Dans ces conditions, afin que les acteurs soient en mesure de travailler ensemble, il semble opportun que les préfectures disposent d'une liste des contacts locaux chargés de la gestion de crise chez chaque opérateur d'infrastructure présent sur son territoire, et puisse ainsi les inscrire sur la liste des acteurs indispensables en temps de crise.

c) Une sensibilisation et un accompagnement des territoires dans l'élaboration d'une stratégie de résilience de leur réseau fibre

Afin de sensibiliser et d'aider les territoires dans leurs démarches de résilience, la fédération InfraNum et la Banque des territoires ont publié en juillet 2023 une étude[14] au niveau national, évaluant les départements en isolant certains critères de risques (zones de vent, incendie de forêt, linéaire aérien, superficie forestière, risque d'inondation, zone de neige) et se penchant sur des scénarios d'enfouissement du réseau. Le scénario priorisé de cette étude vise à enfouir 115 000 km de fibre optique en se concentrant principalement sur les 30 départements identifiés comme à risque climatiques et environnementaux importants pour un montant estimé à 9,9 Mds d'euros.

L'ANCT, toujours avec la Banque des territoires, a présenté en novembre 2023 un guide méthodologique[15] pour « élaborer son schéma local de résilience (SLR) », établi en lien avec l'ensemble des acteurs de l'écosystème (collectivités, préfectures, opérateurs, ministères, ENEDIS, Arcep, etc.). Ce

[12] Guide ORSEC « Rétablissement Et Approvisionnement d'urgence Des Réseaux Électricité, Communications Électroniques, Eau, Gaz, Hydrocarbures » publié en 2015 par les ministères de l'environnement, des affaires sociales, de l'intérieur et de l'économie

[13] https://www.avicca.org/document/21316/dl

[14] https://infranum.fr/publications/resultats-de-letude-resilience-pour-infranum-en-partenariat-avec-la-banque-des-territoires/

[15] https://agence-cohesion-territoires.gouv.fr/resilience-des-reseaux-la-banque-des-territoires-et-lagence-nationale-de-la-cohesion-des

guide encourage ainsi l'ensemble des porteurs de RIP à effectuer de tels schémas, pour lesquels la Banque des Territoires propose par ailleurs un accompagnement financier.

Le syndicat mixte Gironde Numérique, a été le premier RIP à établir un tel audit de résilience[16], finalisé en 2023, qui lui a permis de cartographier les risques et prioriser les actions grâce à un outil de *scoring* : l'investissement de quelques millions d'euros dans la sécurisation des points les plus critiques du réseau permettait d'augmenter de manière significative le niveau de résilience rapidement.

Cette démarche, entreprise depuis par un nombre croissant de porteurs de RIP (par exemple Haute-Garonne Numérique[17], Saint-Barthélémy[18] ou encore la Collectivité de Corse [19]), a permis à la collectivité d'identifier différentes actions possibles, assorties des coûts et les effets attendus sur la résilience du réseau, et *in fine* d'élaborer un plan de renforcement sur plusieurs années. Elle a notamment permis de mettre en lumière, dans ce cas, que si l'enfouissement est une piste à considérer pour certaines parties du réseau spécifiquement identifiées, il ne s'agit pas d'une solution générale devant être considérée comme prioritaire par rapport toutes autres actions.

Il est donc essentiel que les collectivités porteuses de projets d'aménagements numériques réalisent leur SLR. Dans cet objectif, il serait utile qu'elles aient accès aux informations relatives aux pannes et incidents pour être en mesure d'identifier les actions nécessaires au maintien de la résilience de ces réseaux.

d) Assurer une meilleure coordination entre les acteurs

Dans son audit de résilience (*cf*. 3.1.2c), le syndicat mixte Gironde Numérique indique s'agissant de la gestion des incendies qu'il n'a pas été contacté par les services de l'Etat, et que « *la multiplication des acteurs freine une action efficace* » en vue du traitement des incidents : l'ensemble de la chaîne n'a *a priori* pas la même connaissance de l'état du réseau à chaque instant.

En effet, selon le type d'incident, l'opérateur d'infrastructure peut ne pas en être informé d'un incident en l'absence de signalement transmis par les opérateurs commerciaux ou par leurs clients ; la source du problème n'est pas toujours identifiable (poteau tombé, chute d'arbre, etc.) ainsi, le niveau d'information relatif à une panne n'est pas identique pour tous les acteurs de la chaîne, etc.

À cet égard, certains acteurs ont mis en place un portail de signalement des incidents réseau ainsi qu'un serveur vocal interactif pour informer régulièrement les opérateurs commerciaux.

La mise en place de processus au sein du secteur est souhaitable afin de fluidifier les échanges, de gagner en efficacité et, le cas échéant, de coordonner les interventions en vue d'une remise en service plus rapide.

3.2 Accroissement de la concurrence pour l'accès aux ressources stratégiques

Outre la fragmentation du secteur, l'accès aux ressources en électricité, en eau et en métaux stratégiques (terres rares et silicium pour la fabrication des semi-conducteurs ; lithium pour les batteries pouvant secourir les équipements en cas de défaut d'alimentation électrique) nécessaires au fonctionnement des infrastructures de communications électroniques et des centres de données

[16] https://www.avicca.org/document/21316/dl

[17] https://espace-presse.haute-garonne.fr/adoption-de-la-nouvelle-feuille-de-route-numerique-pour-que-le-digital-soit-a-notre-service-et-non-linverse/

[18] https://actes.eservices-comstbarth.fr/PJ/Deliberation%20CT/Deliberation%20CT_2024/2024_065_ct_annexe.pdf

[19] https://www.isula.corsica/assemblea/docs/rapports/2024E1131-annexes.pdf

hébergeant les cœurs de réseau pourrait devenir un enjeu de plus en plus important pour assurer la résilience des réseaux.

En effet, plusieurs facteurs sont susceptibles de mettre en tension leur disponibilité à l'avenir :

- l'instabilité géopolitique, comme ont pu l'illustrer les conséquences de la guerre en Ukraine en 2022/2023 sur l'approvisionnement énergétique et notamment la crainte de délestages électriques ;
- l'explosion de la demande d'appareils électroniques face au faible nombre d'entreprises qui produisent des semi-conducteurs ;
- le développement de nouveaux services tels que ceux reposant sur l'intelligence artificielle, réputés très gros consommateurs d'énergie[20] ;
- le réchauffement climatique qui menace non seulement la ressource hydrique dans certains territoires mais peut également influer sur la disponibilité des moyens de production électriques[21].

Ces ressources risquent ainsi de devenir plus coûteuses, plus rares voire indisponibles lors d'évènements extrêmes (canicule ou vague de froid) alors même que les opérateurs, et plus généralement l'ensemble de l'écosystème numérique, sont susceptibles de connaître une augmentation de leurs besoins, notamment pour le refroidissement des centres de données en période caniculaire.

A titre d'exemple, au Chili, une décision de justice se serait opposée à l'implantation d'un centre de données par Google au motif que le projet consommerait trop d'eau compte tenu de la sècheresse qui sévit dans le pays[22]. De telles actualités ne sont plus des faits très rares et montrent bien l'importance de réflechir à la gestion durable de la ressource en eau. A cet égard, l'Arcep a élargi le périmètre de sa collecte de données environnementales aux opérateurs de centres de données et à la ressource en eau. Ainsi, la quatrième édition de son enquête annuelle « Pour un numérique soutenable »[23] indique que le volume d'eau prélevée par les opérateurs de centres de données concernés par la collecte est en hausse constante d'années en années (+ 20 % entre 2021 et 2022, + 19 % entre 2022 et 2023). Si ce volume reste modeste au regard des volumes prélevés par d'autres usages en France, sa dynamique de croissance montre l'intérêt de suivre ce type d'indicateur dans le temps afin d'éclairer les réflexions prospectives afférentes.

En conséquence, l'ensemble de l'écosystème numérique (opérateurs télécoms et opérateurs de centres de données) doit prendre en compte ce risque en diminuant l'usage de ces ressources, en sécurisant leurs approvisionnements et en favorisant des solutions adaptées à ce nouveau contexte.

---

[20] Selon un rapport publié en 2024 par l'Agence international de l'énergie faisant état de prévision à l'horizon 2026, par rapport à un horizon de référence en 2022 « *An important new source of higher electricity consumption is coming from energy-intensive data centres, artificial intelligence (AI) and cryptocurrencies, which could double by 2026* » - https://iea.blob.core.windows.net/assets/ddd078a8-422b-44a9-a668-52355f24133b/Electricity2024-Analysisandforecastto2026.pdf

[21] En période de canicule, l'Autorité de sureté nucléaire, indique que s'agissant de la température de l'eau en avant d'une centrale nucléaire, « *en cas de dépassement des valeurs limites, l'exploitant doit réduire la puissance du réacteur ou l'arrêter* » - https://www.asn.fr/l-asn-informe/actualites/le-fonctionnement-des-reacteurs-nucleaires-en-periode-de-canicule

[22] https://www.jeuxvideo.com/news/1865849/google-souhaitait-ouvrir-un-data-center-au-chili-avec-200-millions-de-dollars-il-a-ete-bloque-a-cause-d-une-utilisation-excessive-d-eau.htm

[23] Enquête annuelle "Pour un numérique soutenable" - édition 2025 (données 2023) | Arcep. Les opérateurs de centres de données concernés par cette collecte nationale sont ceux tels que définis par le codes des postes et des communications électroniques, dont le chiffre d'affaires HT est supérieur à 10 M€.

S'agissant de la réduction de l'usage, il convient de souligner l'initiative des opérateurs de la fédération française des télécoms qui se sont engagés via la *Charte des opérateurs en faveur d'un numérique durable*[24] à contribuer à la neutralité carbone sur les scopes 1 et 2[25] d'ici 2040 notamment via la limitation de leur impact sur les ressources naturelles.

A cette fin, les opérateurs investissent d'ores et déjà dans des équipements moins énergivores, plus économes et plus efficients (notamment pour les serveurs), et tant côté opérateurs que fournisseurs, ces évolutions se mettent progressivement en place, qu'il s'agisse :

- d'ingénierie physique des centres de données (taille des baies) ;
- de travaux de maintenance réguliers, notamment sur les climatisations et sur les nouveaux systèmes de climatisation en remplacement de groupes de froid ;
- d'utilisation de la méthode de ventilation free-cooling pour refroidir les centres de données;
- d'équipements radio pour limiter la consommation énergétique ;
- d'une régionalisation de l'implantation du cœur de réseau 5G.

Au-delà des investissements dans des solutions plus économes pour les infrastructures existantes, la prise en compte des effets du réchauffement climatique par les opérateurs et les hébergeurs est indispensable pour déterminer la localisation géographique de leurs futurs investissements. Par exemple, l'installation de centres de données qui nécessitent un fort apport en eau ou en énergie pour les refroidir, devraient éviter autant que possible les zones les plus susceptibles de subir des épisodes de canicules et de sécheresse.

Dans son livre blanc d'octobre 2022[26], OVHcloud indique que de plus en plus de technologies et de nouvelles approches de conception sont mises en œuvre dans les centres de données pour minimiser l'empreinte carbone tout en réduisant les coûts et que l'optimisation de la consommation d'eau est au centre des attentions.

OVHcloud indique avoir amélioré son profil eau, énergie, carbone (WEC) grâce à l'utilisation d'une technologie exclusive de refroidissement par eau qui introduit le refroidissement liquide pour le processeur. Combiné à un refroidissement par air libre, ce système à eau a permis à l'entreprise d'atteindre des scores PUE (*« Power Usage Effectiveness »*) et WUE (*« Water Usage Effectiveness »*) très compétitifs. Son système de refroidissement est en boucle fermée, l'utilisation de l'eau est donc très modérée.

À l'aide d'échangeurs de chaleur qui refroidissent les processeurs et d'autres composants dégageant de la chaleur, le système introduit du liquide à l'intérieur des serveurs pour assurer un refroidissement de précision. Environ 70 % de la chaleur générée par les serveurs est captée, puis transférée dans un système en boucle fermée qui achemine le liquide chauffé vers l'extérieur du bâtiment pour le refroidir. En éliminant le besoin d'infrastructures de refroidissement par air des serveurs, telles que les ventilateurs de serveurs, les canaux d'air et les filtres, cette approche permet de réaliser d'importantes économies d'énergie.

[24] https://www.fftelecoms.org/app/uploads/2021/12/Charte-des-operateurs-en-faveur-dun-numerique-durable.pdf

[25] Scope 1 : émissions directes de gaz à effet de serre issues de combustibles fossiles (pétrole, gaz, charbon…). Scope 2 : émissions indirectes résultant de la production d'énergie achetée et consommée par l'organisation (électricité et réseaux de chaleur / froid).

[26] « Datacenters et Cloud : 4 stratégies pour un écosystème numérique responsable et durable » : , https://corporate.ovhcloud.com/sites/default/files/2022-10/ovhcloud_livre_blanc_eco_fr_compressed.pdf

En complément de stratégies visant à diminuer l'usage de ces ressources par l'amélioration de l'efficacité énergétique et hydrique de leurs équipements et centres de données, il ressort des échanges et publications que certains acteurs ont commencé à sécuriser leurs approvisionnements énergétiques sur long terme en diversifiant leurs sources d'approvisionnement. À cet égard, le groupe Iliad notamment a annoncé début 2024 avoir signé trois contrats de fourniture d'électricité d'origine photovoltaïque supplémentaires en France ainsi qu'en Italie et en Pologne, à partir de 2025, pour les 10 à 15 ans à venir, portant sur plus de 110 GWh/an[27]. On peut toutefois noter que le seul recours à l'électricité photovoltaïque, de par sa variabilité, n'est pas en mesure de répondre aux besoins des infrastructures de communications électroniques qui fonctionnent en permanence.

Par ailleurs, de grandes entreprises du numérique réfléchissent ou ont fait le choix d'investir directement dans des différents types de production énergétique. C'est le cas d'Amazon qui investit dans des installations photovoltaïques, des parcs éoliens et solaires[28] ou celui de Microsoft qui investiguerait la technologie des mini-réacteurs nucléaires modulaires (SMR) pour alimenter ses centres de données[29]. Ces acteurs puissants font le choix stratégique d'une production d'électricité la plus autonome afin que leurs projets ne soient pas entravés par une dépendance trop importante à un approvisionnement extérieur.

4 Risques technologiques

4.1 Les câbles sous-marins, des infrastructures critiques pour assurer la connectivité mondiale et notamment l'ouverture d'Internet

Le bon fonctionnement de l'internet dépend notamment de la connectivité internationale. Dans ce contexte, l'infrastructure des câbles sous-marins qui achemine la majorité du trafic international de données, constitue un maillon essentiel de l'écosystème.

Or l'empreinte internationale des infrastructures sous-marines complexifie leur protection par les outils de régulation nationaux. Pour autant, les conséquences que d'éventuels incidents pourraient avoir sur l'ensemble du territoire, à l'instar des coupures et dysfonctionnement de câbles qui ont été jusqu'à priver d'Internet plusieurs pays d'Afrique en mai 2024, mérite une attention toute particulière afin de mieux appréhender les impacts (géographiques et sur les services) de telles coupures et préciser les attendus en matière de sécurité et de résilience applicables aux acteurs qui les exploitent.

À cet égard, la Commission européenne a présenté le 21 février 2024 sa recommandation sur la sécurisation des câbles sous-marins[30]. Elle propose notamment de créer un groupe d'experts de ces infrastructures qui serait chargé de proposer une boîte à outils pour la sécurité des câbles, à l'instar de ce qui a été fait pour la sécurisation des réseaux 5G.

Elle encourage par ailleurs les États membres à cartographier leurs infrastructures nationales, à évaluer les risques et les vulnérabilités de la chaîne d'approvisionnement, ainsi qu'à effectuer des tests de résistance réguliers des infrastructures (*stress tests*) afin d'évaluer leur résilience selon différents scénarii. De tels tests de résistance pourraient notamment apprécier la reconfiguration des routes d'acheminement du trafic, les capacités résiduelles et donc l'impact sur la qualité des services

[27] https://www.iliad.fr/fr/actualites/article/le-groupe-iliad-annonce-3-nouveaux-projets-d-energies-renouvelables-dans-ses-3-geographies-et-valide-sa-trajectoire-carbone-aupres-de-la-sb-ti

[28] https://www.aboutamazon.fr/actualites/durabilite/amazon-etablit-un-nouveau-record-de-volume-denergie-renouvelable-achete-par-une-seule-entreprise

[29] https://www.linkedin.com/in/archie-manoharan/

[30] https://commission.europa.eu/news/getting-eus-digital-infrastructures-ready-tomorrows-world-2024-02-21_fr

d'internet pour ces différents scénarios. De cette manière, pourrait être identifiées les actions demandées aux acteurs de l'internet afin de préserver autant que possible la connectivité globale dans de telles circonstances. Pour rappel, au printemps 2020, face au développement des usages vidéo lié à la crise sanitaire, les plateformes de diffusion vidéo avaient réduit la résolution des flux pour limiter l'engorgement des réseaux.

4.2 Virtualisation et programmation logicielle des réseaux à l'origine d'une mutation profonde des architectures des opérateurs

Les architectures réseaux des opérateurs de communications électroniques sont en pleine mutation avec le développement de la virtualisation et de la programmation logicielle. Si ces technologies sont porteuses de nombreuses promesses en termes d'efficacité et d'apport de nouveaux services, elles constituent une rupture technologique pour les équipes d'ingénierie des opérateurs.

4.2.1 L'ouverture à des tiers grâce à des API engendrent de nouvelles vulnérabilités pour les réseaux 5G par rapport aux réseaux de génération antérieure

Avec la mise en place d'API, la 5G permet à des tiers d'accéder à des informations et des fonctions de paramétrage du réseau jusqu'alors exclusivement réservées aux équipes d'ingénierie des opérateurs. Par exemple, les clients et fournisseurs de services peuvent être en mesure d'adapter la capacité du réseau à leurs besoins, des organismes bancaires peuvent vérifier la date du dernier changement de carte SIM d'un abonné afin de se prémunir contre le risque de fraude exploitant la technique dite de *SIM swapping*.

Plus précisément, cette ouverture permet à des tiers (sociétés de services, fournisseurs d'applications, clients industriels/verticaux, MVNO, etc.) d'instancier et d'orchestrer[31] eux-mêmes des services virtualisés. Elle implique donc que de nouveaux acteurs auront accès à certaines données et fonctions liées à l'exploitation du réseau, notamment celles de configuration et de souscription — ce qui relève du suivi de performance, de la supervision et de la maintenance du réseau devraient *a priori* rester sous contrôle exclusif de l'opérateur de réseaux).

Une telle ouverture augmente les possibilités d'attaque et de compromission du réseau par des tiers et il convient d'inclure ces nouveaux risques dans la stratégie de protection des opérateurs contre les menaces cyber.

4.2.2 Des technologies nouvelles auxquelles les opérateurs doivent se former pour conserver la maitrise de leur réseau

Le processus de virtualisation des réseaux mobiles, qui implique le déport de fonctionnalités critiques d'orchestrationvers le *cloud*, implique des changements importants pour les opérateurs télécoms. Si les opérateurs disent avoir pris conscience de ce changement et que la virtualisation est présente dans leurs systèmes depuis plusieurs années, ils conviennent que l'arrivée de fonctionnalités réseau faites spécifiquement pour un hébergement cloud (*« cloud native »*) reposant sur de la conteneurisation, des micro services et de l'intelligence artificielle constitue un défi pour les équipes d'ingénierie qui doivent monter en compétence sur ces technologies pour conserver une parfaite maitrise de leur réseau. Pour

[31] L'orchestration correspond à la configuration, la gestion et la coordination automatisées des systèmes informatiques, applications et services tels que l'approvisionnement de serveurs, la gestion des incidents, l'orchestration du cloud, la gestion des bases de données, l'orchestration des applications ainsi que de nombreux autres processus et tâches.

cela, ils indiquent avoir notamment recours à des plans de formation et des programmes de recrutement d'experts de ces technologies.

Une telle montée en compétence leur permet d'héberger ces fonctions réseau sur leurs propres infrastructures situées dans leurs centres de données et ainsi éviter de faire appel à des tiers pour opérer leur infrastructure de virtualisation.

Par ailleurs, Orange participe au projet SILVA, regroupant des opérateurs européens ainsi que les équipementiers Nokia et Ericsson, dont l'objectif est de réduire la complexité de l'écosystème cloud utilisé par les différents acteurs du secteur en rendant les outils télécoms et IT plus interopérables.

5 Risques naturels

Les infrastructures de communications électroniques sont particulièrement vulnérables aux catastrophes naturelles, non seulement les réseaux d'accès fixes et mobiles mais également les cœurs de réseaux hébergés au sein de centres de données. Il semble important de caractériser ces risques, d'identifier les points les plus vulnérables, d'anticiper des plans d'action de renforcement ainsi que les processus de gestion de crise pour favoriser le retour à la normal après la survenue de telles évènements. Facteur aggravant, les effets du changement climatiques devraient se traduire, d'une part, par une amplification des phénomènes connus en fréquence et en intensité et, d'autre part, faire peser de nouveaux risques climatiques sur des territoires jusqu'alors épargnés.

5.1 Des menaces significatives pour les réseaux de communications électroniques

Sur 155 incidents sur les réseaux de communications en Europe répertoriés en 2022 par l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)[32], 6 % des pannes étaient dues aux phénomènes climatiques, représentant une perte de 168 milions d'heures d'utilisation, un chiffre en forte hausse (contre 41 millions d'heures en 2021). En effet, les évènements naturels peuvent avoir des conséquences importantes pour les infrastructures de communications électroniques :

- les vents violents précipitent la chute des arbres sur les poteaux et les lignes aériennes ;
- les fortes précipitations entrainent inondations et crues pouvant emporter des infrastructures enfouies ;
- les épisodes de sécheresse et les fortes canicules facilitent les incendies et sont susceptibles perturber les centres de données en poussant à leurs limites les systèmes de climatisation[33].

[32] https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA_Telecom%20Incident%20Reporting_en_1.pdf

[33] En raison de températures anormalement élevées à l'été 2022 à Londres (40° C) un des centres de données de Google a connu des dysfonctionnements en raison de pannes des systèmes de refroidissement - https://www.lefigaro.fr/secteur/high-tech/a-londres-les-data-centers-de-google-et-oracle-n-ont-pas-supporte-la-chaleur-20220720

Cas de la tempête Alex – échanges avec le SIDPC[34] du département des Alpes-Maritimes

La tempête Alex qui s'est abattue sur le département des Alpes-Maritimes les 2 et 3 octobre 2020 a été qualifiée de bombe météorologique par les experts : un événement exceptionnel qui a cumulé plusieurs phénomènes (pluies, vagues, submersion, orage et vents violents) affectant cinq vallées des Alpes-Maritimes, dont trois particulièrement sinistrées : la Vésubie, la Roya et la Tinée.

Malgré l'anticipation et la préparation des autorités afin de déployer des moyens visant à limiter ses effets (suivi des alertes de Météo France, activation exceptionnelle de la cellule de crise en amont de la tempête, diffusion de mesures de sécurité aux populations, déclenchement du plan Orsec[35]) ainsi que la mobilisation des acteurs privés, notamment les opérateurs de communications électroniques, le caractère exceptionnel de cet événement n'a pu empêcher les nombreux dégâts matériels. Une partie des infrastructures a été emmenée par les crues, privant ainsi de nombreuses communes d'eau potable, d'électricité, de liaisons routières et ferroviaires et de moyens de communication.

S'agissant des infrastructures de communications électroniques, il ressort du retour d'expérience effectué par les autorités que les réseaux ont été impactés par la rupture de réseaux filaires (cuivre et fibre) situés en bordure de routes qui avaient été emportées par les crues. Les 85 km de routes emportées et les 12 ponts détruits ont rendu les interventions sur sites compliquées, voire parfois impossibles.

A contrario, une très grande majorité des sites radio impactés durant la crise a pu à nouveau fonctionner dès le retour de l'électricité.

Dans ce contexte, les solutions satellitaires (téléphones ou kits d'accès à Internet notamment mis à disposition par Orange et Enedis) ont été essentielles pour permettre à des services de secours ou des collectivités parmi les plus sinistrées de pouvoir communiquer dans l'attente d'un retour à une situation « normale ».

Or, comme l'indique le GIEC[36], dans son 6e rapport d'évaluation publié en mars 2023[37], les effets du changement climatique vont s'accentuer à mesure que le réchauffement mondial s'amplifie et notamment les températures extrêmes, l'intensité des précipitations, la sévérité des sécheresses et l'augmentation en fréquence et intensité des événements climatiques rares.

Ainsi, l'augmentation probable à venir des pannes liées aux phénomènes naturels confirme la nécessité pour les parties prenantes, et notamment les opérateurs de communications électroniques, d'intégrer au mieux cet enjeu de résilience dans la phase de vie (entretien, extension…) de leurs réseaux, et de prendre des mesures d'adaptation à ces phénomènes en complément des mesures d'atténuation du changement climatique auxquels ils se sont par ailleurs engagés[38].

⁂

[34] Service interministériel de défense et de protection civile

[35] Organisation de la réponse de la sécurité civile

[36] Groupe d'experts intergouvernemental sur l'évolution du climat

[37] https://www.ecologie.gouv.fr/publication-du-6e-rapport-synthese-du-giec

[38] Au niveau national, les quatre opérateurs mobiles se sont engagés dans le cadre d'une « Charte pour un numérique durable » signée en décembre 2021, avec pour objectif commun de contribuer à la neutralité carbone sur les scopes 1 et 2 d'ici 2040 notamment via la réduction de leurs émissions de CO_2, la limitation de leur impact sur les ressources naturelles ou encore mettre le numérique au service de l'environnement.

Généralement moins connues, les éruptions solaires et les tempêtes électromagnétiques qu'elles engendrent ont non seulement la capacité de perturber les communications, d'endommager les satellites mais également les équipements de surface.

Les éruptions solaires constituées d'expulsions massives de plasma induisent des tempêtes solaires en atteignant la Terre susceptibles de perturber le champ magnétique terrestre et de dégrader les systèmes de navigation, les réseaux électriques, ainsi que les réseaux de communications radioélectriques et satellites. Ces éruptions sont liées au cycle solaire dont la période est d'environ 11 ans.

Par exemple, l'éruption solaire du 13 mars 1989 a causé un *black-out* de plusieurs heures dans certaines parties du Canada[39] : perturbé par une tempête solaire, le champ magnétique terrestre a brusquement varié, ce qui a provoqué le déclenchement de mécanismes de protection des réseaux de transport et de distribution d'électricité au Québec, occasionnant un *black-out*.

Les conséquences d'éruptions solaires d'une telle intensité, bien que rares, pourraient se révéler encore plus dévastatrices : outre la perturbation des réseaux d'électricité, d'autres infrastructures notamment de communications électroniques et des centres de données, pourraient être gravement endommagés sous l'influence de forts courants électromagnétiques.

5.2 Planification des investissements dans le cadre d'une stratégie d'adaptation

L'intensification des catastrophes naturelles liées au réchauffement climatique, désormais incontesté en France, est un nouveau paramètre à prendre en compte pour assurer la robustesse des réseaux. Les opérateurs de communications électroniques ont besoin de s'adapter et de prendre les dispositions nécessaires pour en limiter les impacts et veiller à la disponibilité de leurs réseaux et services.

Il ressort des entretiens menés dans le cadre de cette étude que la prise de conscience des opérateurs est réelle. Depuis plusieurs années, ils ont été confrontés à différents types de catastrophes climatiques (tempêtes, canicules et incendies, crues et inondations en métropole, cyclones et risques de séisme et de submersions en outre-mer) et ont pu en voir les conséquences sur leurs infrastructures de réseaux.

Afin d'y faire face, les opérateurs mènent des analyses de risques climatiques pour réaliser des projections à différentes échéances (2030, 2040, 2050) et identifier les investissements nécessaires à long terme. Ces outils de cartographie des risques climatiques associés à un diagnostic des vulnérabilités du réseau leur sont indispensables afin de renforcer leur réseau. Il s'agit pour eux de se doter d'une stratégie d'investissements prioritaires avec des échéances et des zones identifiées et de se coordonner avec d'autres acteurs impliqués (puissance publique, gestionnaire du réseau électrique, etc.) en fonction des aléas considérés.

Ces stratégies impliquent notamment de :

- sécuriser les réseaux fibres (backbone, nœuds de raccordement optique (NRO), PoP, locaux et chambres d'accès etc.) ;
- renforcer les bracons d'antennes de faisceaux hertziens pour résister aux vents violents et éviter les dépointages ;
- surveiller les zones à élaguer ;

[39] https://fr.wikipedia.org/wiki/%C3%89ruption_solaire_de_1989

- contrôler les équipements de climatisation de manière accrue avant la survenance d'un épisode de chaleur ;
- renforcer les centres de données en vue de crues exceptionnelles ;
- déployer des sondes de température afin de refroidir préventivement les sites concernés par un éventuel événement.

Les opérateurs sont d'ailleurs tenus de partager certains éléments de cette stratégie avec les autorités, puisque les préfets de département pour lesquels une exposition à des risques naturels pourrait conduire à un arrêt de tout ou partie du service peuvent, en application de la loi portant lutte contre le dérèglement climatique[40], demander aux opérateurs présents sur leur territoire de leur communiquer notamment le diagnostic de vulnérabilité de leurs ouvrages ainsi qu'un « *programme des investissements prioritaires pour améliorer la résilience des services prioritaires pour la population en cas de survenance de l'aléa* ».

Résistance des réseaux fixe et mobile aux tempêtes

Lors de la tempête Ciaran du 1er novembre 2023, un des opérateurs mobiles a constaté que 90 % des sites indisponibles l'étaient en raison de la pénurie d'électricité et que les 10 % restants concernaient des désorientations d'antennes ainsi que des difficultés d'accès aux sites (routes impraticables ou non sécurisées pour les techniciens), qui ont pu rallonger les délais de rétablissement.

Il explique ce constat par la résistance des infrastructures passives et actives aux aléas climatiques : d'une part, les éléments passifs (pylônes, mâts, fausses cheminées, boîtiers, etc.) respectent, lors de la construction, les différents plans d'urbanisme et de prévention des risques ainsi que des notes de calculs (emprise au sol, micro-pieux, massif) et, d'autre part, du fait que le fonctionnement du matériel radio déployé en extérieur (antennes actives, amplificateurs de puissance) en conditions extrêmes est garanti par les équipementiers (les matériels déployés à l'intérieur des baies ventilées sont eux, protégés par la baie). Ainsi ces équipements peuvent résister à des inondations (mêmes équipements qu'en Asie du Sud), à des canicules (mêmes équipements qu'au Moyen-Orient) et au froid extrême (mêmes équipements qu'en Scandinavie).

Enfin, certains réseaux fixes s'appuient sur des poteaux d'Enedis qui ont été cassés ou enfouis sous la végétation. Les opérateurs exploitant ces réseaux ont donc été en partie dépendant de la remise en état d'Enedis notamment au regard du risque d'électrocution des intervenants du fait de l'enchevêtrement des câbles électriques et télécom tombés. En pareille situation, un câble provisoire est parfois laissé au sol pour une remise en service rapide avant la remise en état finale.

5.3 Organisation, moyens mis en œuvre et retours d'expérience pour la gestion de crise

Les opérateurs ont mis en place plusieurs moyens pour anticiper, faciliter et accélérer la reprise du service en cas d'événement :

- des dispositifs de veille et d'anticipation (par exemple, surveillance ou convention avec des sites météorologiques, surveillance des cartes de vigilance des crues – Vigicrue) afin de pouvoir renforcer les astreintes en amont d'un événement ;

[40] Loi nº 2021-1104 du 22 août 2021 et plus particulièrement son article 249.

- des stocks de matériels (câbles de fibre, NRO, armoires de rue, groupes électrogènes, batteries, poteaux, etc.) disséminés sur le territoire ;
- des personnels d'astreinte sur place (en propre avec éventuel recours à des sous-traitants) pour intervenir rapidement (certains ont créé une « force d'intervention rapide ») et être à la disposition des autorités.

Ils disposent également de moyens et de solutions temporaires pour une remise en service rapide, tels que par exemple des NRO mobiles, des nacelles sur remorque, des climatiseurs mobiles voire des moyens de communications alternatifs tels que des kits satellite.

Le satellite, un outil au service de la gestion de crise et de la résilience des infrastructures

Lors de la tempête Alex, les solutions satellitaires ont été essentielles pour maintenir les communications de façon temporaire et ont illustré l'importance de diversifier les moyens de communications et prévoir des moyens alternatifs de secours pour maintenir les communications quand les réseaux fixes et mobiles sont hors service.

Le secteur spatial connaît depuis quelques années une révolution avec l'arrivée de nouveaux acteurs privés apportant une série d'innovations technologiques et de nouveaux business models, permettant une réduction significative des coûts de l'accès au spatial et une mise en place de nouveaux produits et services.

C'est d'ailleurs le satellite, via la constellation de satellites « IRIS2 » (Infrastructure pour la résilience, l'interconnectivité et la sécurité par satellite), que la Commission Européenne a choisi pour son réseau fiable et sécurisé permettant notamment d'échanger en toute sécurité.

Au-delà de l'acheminement des communications d'urgence en période de crise, les services satellitaires peuvent offrir des perspectives de plus grande intégration aux services terrestres, notamment pour la collecte des réseaux ou redonder certains sites, et ainsi maintenir une connectivité de secours en cas de dysfonctionnement des infrastructures terrestres.

Une fois l'événement terminé, un retour d'expérience est généralement effectué afin d'analyser ce qui n'aurait pas fonctionné et d'adapter les processus en conséquence.

Les opérateurs tirent ainsi parti des événements climatiques qui les affectent (tempêtes dans le Gers et la Haute-Garonne au printemps 2023, tornade en juillet 2023 en Haute-Garonne, incendies en Pyrénées-Orientales en août 2023, tempêtes Ciaran et Domingos à l'automne 2023) pour gagner en expérience et ainsi affiner leur « réponse ».

Il ressort des entretiens que les principaux axes d'amélioration relevés à l'occasion des retours d'expérience des évènements récents sont essentiellement d'ordre organisationnel : monter en compétence sur les processus de gestion de crise ; organiser les remises en l'état et en maîtriser les délais ; améliorer la connaissance mutuelle des différents acteurs ; renforcer les échanges avec les autorités afin d'être identifié et convié en cellule de crise ; planifier des séances de partage d'information.

Pour répondre à ces défis, différentes mesures sont prises par les opérateurs afin que leurs personnels connaissent l'organisation et les processus en temps de crise tant au sein de l'entreprise qu'avec l'ensemble des partenaires :

- organisation de sessions de formation ou de journées annuelles de sensibilisation à la gestion de crise ;
- organisation d'exercices ou de simulations de crises, dans la mesure du possible en intégrant les autorités locales compétentes ;

- contractualisation avec des prestataires locaux ou avec des acteurs nationaux de maintenance 24 heures sur 24, afin d'intervenir rapidement, en renfort des équipes internes et externes avec des moyens plus importants ;
- accords avec des loueurs de nacelles d'urgence, groupes électrogène, 4 × 4, motos-neige, etc. ;
- accord pour accès prioritaire avec des aérodromes pour accès en hélicoptère sur des zones dont les routes sont impraticables.

5.4 Prendre conscience de la complexité et de l'interdépendance des réseaux pour agir efficacement

Les opérateurs de communications électroniques ne sont pas seuls à affronter les crises et sont souvent tributaires d'autres acteurs pour effectuer les remises en état et en service de leurs infrastructures : restauration de l'alimentation électrique, circulation et mise en place des chantiers, obtention des autorisations des autorités et services de secours pour accéder aux zones et commencer les travaux de réparation, prévention des risques de suraccident, notamment d'électrocution en cas d'enchevêtrement des câbles électriques et télécoms.

La tempête Alex a illustré l'interdépendance des réseaux (électriques, de communications électroniques, routiers etc.) qui augmente leur vulnérabilité et impacte les délais de remise en service des réseaux de communications.

Comme le relève France Stratégie dans sa note d'analyse *Risques climatiques, réseaux et interdépendances : le temps d'agir*[41], *« les réseaux d'électricité, de transports routier et ferroviaire et de télécommunications sont associés, en fonctionnement normal comme en temps de crise, par de nombreux liens de dépendance, physiques ou découlant des relations entre les acteurs* ».

D'une part, les câbles électriques ou de télécommunications en proximité immédiate des routes sont soumis aux aléas touchants celles-ci ; les réseaux de communications dépendent de leur alimentation électrique de même que les réseaux électriques ont besoin des réseaux de communications pour fonctionner. Les équipes d'interventions (électriques et télécom) ont besoin des routes pour accéder aux sites afin de remettre en état les réseaux.

D'autre part, il apparait ainsi que les spécificités de l'architecture des différents réseaux impliqués ont besoin d'être précisément comprises par les autorités publiques afin de définir les priorités de rétablissement des sites. Par exemple, si la restauration d'un site d'un opérateur mobile est considérée comme prioritaire en raison du nombre d'autres sites mobiles qu'il permet de rétablir, il est nécessaire que le site électrique correspondant soit au moins doté de la même priorité de rétablissement même s'il n'est pas considéré comme stratégique du seul point de vue du réseau électrique. La prise en compte des sites prioritaires de chaque réseau et de leurs dépendances au sein des autres réseaux est essentielle à une prise de décision éclairée.

[41] https://www.strategie.gouv.fr/publications/risques-climatiques-reseaux-interdependances-temps-dagir

Annexe 1 : Références

Un cycle d'entretiens a nourri la réflexion de l'Arcep sur la résilience des réseaux. Toutefois, les positions prises dans cette note ne reflètent pas nécessairement les points de vue des personnes auditionnées ni des institutions auxquelles elles appartiennent.

Ont notamment été reçus en entretien :

- Orange
- Bouygues TelecomSFR
- Axione
- Altitude Infrastructure
- XP Fibre
- Préfecture des Alpes-Maritimes
- Préfecture de Police de Paris
- France Stratégie
- ANCT (Agence Nationale de la Cohésion des Territoires)
- Enedis
- CNES (Centre national d'études spatiales)
- DGNUM (Direction générale du Numérique et des Systèmes d'information et de communication)

Séminaires

- Avicca : TRIP d'automne 2023
- Cercle CREDO : Réussir la résilience des réseaux Ftth : stratégie et solutions, novembre 2023
- BEREC Workshop on international submarine connectivity in the EU, septembre 2023
- Banque des Territoires : Résilience des réseaux numériques : anticiper maintenant pour ne pas subir demain, avril 2024

Références bibliographiques :

- Élaborer son schéma local de résilience - Guide méthodologique – Banque des territoires
- Étude « Résilience des réseaux FttH » - InfraNum et la Banque des Territoires
- Risques climatiques, réseaux et interdépendances : le temps d'agir – France Stratégie
- La résilience des territoires aux catastrophes – Ministère de la transition écologique et solidaire
- Document de référence interministériel sur la stratégie nationale de résilience dans le domaine de la défense et de la sécurité nationale - SGDSN
- Guide ORSEC RETAP RESEAUX - Ministère de l'intérieur
- Recommandation sur la sécurité et la résilience des infrastructures de câbles sous-marins – Commission européenne
- Identifying emerging cyber security threats and challenges for 2030 - ENISA
- Charte des opérateurs en faveur d'un numérique durable - FFT

Annexe 2 : Cadre juridique et partage des compétences

L'ensemble des opérateurs de communications électroniques sont assujettis à une obligation d'assurer la permanence, la disponibilité et la sécurité de leur réseau au titre du Code européen des communications électroniques[42] et du CPCE (Code des postes et des communications électroniques).

En particulier, 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. »*.

En outre, l'article D. 98-5 prévoit que *« L'opérateur prend toutes les mesures appropriées pour assurer l'intégrité de ses réseaux et garantir la continuité des services fournis. »,* de même : *« l'opérateur prend toutes les dispositions techniques et organisationnelles nécessaires pour assurer la sécurité de son réseau et de ses services à un niveau adapté au risque existant. En particulier, des mesures sont prises pour prévenir ou limiter les conséquences des atteintes à la sécurité pour les utilisateurs et les réseaux interconnectés. ».*

De plus, en cas d'incident majeur, les opérateurs sont tenus d'informer les autorités : « *Dès qu'il en a connaissance, l'opérateur informe le ministre de l'intérieur de toute atteinte à la sécurité ou perte d'intégrité ayant un impact significatif sur le fonctionnement de ses réseaux ou de ses services. Ce dernier en informe le ministre chargé des communications électroniques ainsi que les services de secours et de sécurité susceptibles d'être concernés. Lorsque l'atteinte à la sécurité ou la perte d'intégrité résulte ou est susceptible de résulter d'une agression informatique, l'opérateur en informe également l'autorité nationale de défense des systèmes d'information. ».*

Enfin, *« il se conforme aux prescriptions techniques en matière de sécurité éventuellement édictées par arrêté du ministre chargé des communications électroniques. Ce dernier peut se faire communiquer à titre confidentiel les dispositions prises pour la sécurisation du réseau. ».*

Ces obligations s'apprécient notamment au regard de la proportionnalité entre la criticité des réseaux considérés, les risques identifiés et les mesures de sécurité à mettre en œuvre.

Au-delà de ce cadre général, il existe un dispositif particulier de sécurité des activités d'importance vitale mis en place par le Premier ministre et codifié au Code de la défense[43].

En effet, les opérateurs de réseaux de communications électroniques opérant les systèmes les plus critiques peuvent être désignés par le gouvernement « Opérateurs d'importance vitale[44] » (ci-après « OIV »). Cette désignation emporte des obligations supplémentaires en matière de sécurité logique et physique d'éléments du réseau et des systèmes d'information. Elle permet également à ces opérateurs de bénéficier d'une assistance accrue des pouvoirs publics, notamment de l'ANSSI et du SGDSN pour la mise en place de mesures de sécurité adéquates en cas de crise, ainsi que des préfectures via l'élaboration de plans de protection externe (PPE) comportant les mesures de vigilance et d'intervention prévues en cas de menace ou d'attentat visant les points d'importance vitale. Des compétences partagées entre le gouvernement, l'Arcep et les préfets de département

La résilience et la sécurité des réseaux constitue une problématique dont les compétences sont partagées au niveau national :

[42] La directive NIS2, en cours de transposition, reprend les dispositions du CECE relatives à la sécurité des réseaux qui seront supprimées du CECE.

[43] Articles L. 1332-1 et suivants du Code de la défense relatifs aux opérateurs d'importance vitale (« OIV »)

[44] La liste des opérateurs désignés en tant qu'opérateur d'importance vitale est classifiée

- Le ministre des communications électroniques, qui veille au respect des règles et peut élaborer des prescriptions techniques en matière de sécurité, notamment par le biais du CCED ;
- Le ministre de l'intérieur, notamment via le COGIC et, le cas échéant l'ANSSI, qui sont les autorités devant être informées en cas d'incident ayant un impact significatif ; L'Arcep dont le rôle consiste essentiellement à veiller au respect des règles, conjointement avec le ministre, et en cas de manquement présumé, ouvrir une procédure, voire à sanctionner l'opérateur.

Un guide de déclaration des incidents a été élaboré par le CCED[45] en liaison avec le service du HFDS[46] de Bercy afin d'en préciser les modalités pratiques. Il prévoit deux types d'incidents devant être déclarés selon les modalités suivantes :

- Cas de l'incident d'intégrité (dysfonctionnement technique)

Tout incident donnant lieu à indisponibilité totale de l'un et/ou l'autre des services (téléphonie ou internet, fixe ou mobile) lorsque la durée d'impact dépasse 4 heures pour au moins 100 000 abonnés doit être signalé au ministère de l'intérieur (COGIC[47]).

Tout incident constitué par l'indisponibilité totale d'au moins un numéro d'appel d'urgence, dans au moins un département, lorsque la durée d'impact dépasse 2 heures, doit être signalé au ministère de l'intérieur, y compris lorsque la cause ne relève pas directement de l'opérateur.

- Cas de l'incident de sécurité (attaque informatique ou suspicion d'attaque)

Tout incident de sécurité correspondant à la détection d'attaque sur les systèmes d'information des opérateurs de réseaux ouverts au public, ou à la suspicion d'une attaque, doit être signalé à l'ANSSI.

Au niveau local, les préfets de département des territoires exposés à un ou plusieurs risques naturels (inondations, vents cycloniques, incendies de bois et forêts et sismiques) peuvent demander aux opérateurs[48] :

- Un diagnostic de vulnérabilité de leurs ouvrages ;
- Les mesures prises en cas de crise pour prévenir les dégâts et pour assurer un service minimal qui permette d'assurer la continuité de la satisfaction des besoins prioritaires de la population ;
- Les procédures de remise en état du réseau après la survenance de l'aléa ;
- Un programme des investissements pour améliorer la résilience des services prioritaires pour la population en cas de survenance de l'aléa.

S'agissant spécifiquement du rôle de l'Arcep en matière de résilience, il consiste principalement à veiller au respect, par les opérateurs, de leurs obligations en la matière (cf 1.2).

De plus, l'article L. 36-6 CPCE prévoit que l'Autorité est compétente pour préciser, par décision homologuée par arrêté du ministre chargé des communications électroniques et publiée au Journal officiel, les règles concernant notamment les droits et obligations afférents à l'exploitation des différentes catégories de réseaux et de services de communications électroniques, en application de l'article L. 33-1.

[45] Commissariat aux communications électroniques de défense

[46] Haut fonctionnaire de défense et de sécurité

[47] Centre opérationnel de gestion interministérielle des crises

[48] Loi n° 2021-1104 du 22 août 2021 portant lutte contre le dérèglement climatique

Son action peut également contribuer, d'une manière informelle, au renforcement de la sécurité et de la résilience des réseaux, dans le cadre de ces travaux et échanges réguliers avec les opérateurs, notamment dans le cadre de la régulation des réseaux FttH.

D'autre part, l'Arcep contribue aux travaux pilotés par le gouvernement sur ces questions, notamment dans le cadre des travaux menés par la Commission interministérielle de coordination des réseaux et des services de communications électroniques pour la défense et la sécurité publique.

C'est dans cet objectif que s'inscrivent les travaux de l'Arcep en matière de résilience des réseaux de manière générale ayant notamment conduit à l'élaboration de la présente note.

Le tableau suivant présente le partage des compétences en matière de sécurité.

	ANSSI	ARCEP	COGIC	Ministre des CE /CCED	Préfets de département
Informer des incidents significatifs	(X)		X		
Auditer la sécurité	X				
Élaborer des prescriptions techniques	X			X	
Veiller au respect des règles		X		X	
Demander un diagnostic de vulnérabilité					X
Demander les mesures prises en cas de crise ainsi que les procédures de remise en état					X
Demander un programme des investissements prioritaires					X
Sanctionner		X			