Haut Comité Français pour la Résilience Nationale

Étude préliminaire sur la résilience des réseaux d'infrastructures

Associée à une analyse bibliographique
et à des questionnaires et interviews d'opérateurs d'infrastructures de réseaux, entreprises ou collectivités

01/08/2023

Responsable : Benjamin ROMAN
Rédacteurs : Clément KAROUBI, Christian SOMMADE

Étude réalisée pour le compte de l'AFPCNT

Sommaire

Introduction

1 - Les perspectives liées au changement climatique

2 - Les interdépendances des réseaux

3 – La Vulnérabilité des réseaux face aux risques naturels, au regard du changement climatique

4 - Les actions à mettre en place

5 – Annexes

5-1 – Bibliographie

5-2 – Synthèse et détails des questionnaires des entreprises opérateurs de réseaux interrogés

5-3 – Synthèse et détails des questionnaires des collectivités, opérateurs de réseaux interrogés

Introduction

La 6e édition du rapport du GIEC a été publiée le 20 mars 2023. Les experts prévoient, pour la France, un réchauffement de plus de 4°C avec 5 à 10 fois plus de vagues de chaleur qui pourraient s'étaler sur un mois sur la période de mai à septembre et une intensification des précipitations. Les perspectives liées au changement climatique interrogent de fait sur la capacité des réseaux à fonctionner correctement dans ces conditions. À ce titre, le Ministre de la Transition Écologique, Monsieur Christophe Béchu, annonçait le 22 février 2022 sur Franceinfo, qu'il allait réunir "l'ensemble des opérateurs du ministère pour commencer à construire une trajectoire à quatre degrés"[1]. L'objectif de cette concertation est d'anticiper les conséquences du réchauffement climatique.

En effet, les infrastructures vont être confrontées à de nouveaux défis (températures élevées, augmentation des précipitations et des occurrences de tempêtes ou de vents violents) dont les conséquences, notamment sur l'énergie, les télécommunications, l'eau et les transports sont réelles, par ailleurs des menaces hybrides peuvent survenir dans le cadre géopolitique actuel. Une puissance étrangère ou des groupes terroristes pourraient profiter d'une catastrophe naturelle pour accroître les conséquences de cette dernière par des attaques cyber ou des sabotages. De fait, la sécurité et la résilience des réseaux essentiels d'infrastructures constitueront un défi majeur dans les années à venir au plan européen.

Si l'Union Européenne n'a pas réussi à influencer la majeure partie des pays européens avec la directive de 2008/114/CE concernant le recensement et la désignation des infrastructures critiques européennes au regard des objectifs de sécurité (renforcement de la protection), trop peu de pays étaient à l'époque conscients des risques encourus, le cadre géopolitique avec la guerre en Ukraine et l'impact de la crise sanitaire du COVID-19 ont conduit les états européens et la commission à reprendre leurs travaux sur ce sujet. C'est dans ce cadre que l'adoption en novembre 2022 par le Parlement et le Conseil Européen de la directive portant sur la Résilience des Entités Critiques (REC) constitue une nouvelle « étape essentielle » sur laquelle nous reviendrons.

Mais Il convient dans un premier temps de préciser la notion même de résilience. Elle peut prendre plusieurs formes : organisationnelle, structurelle et sociétale. Une définition

[1] "Climat : il faut préparer notre pays à 4°C de réchauffement climatique, prévient le ministre de la Transition Écologique", Franceinfo – 22.02.2023

communément admise de la résilience sociétale est celle-ci *"l'ensemble des moyens et actions qu'une société[2] met en œuvre aux plan collectif et individuel pour lui permettre de prévenir et de résister aux catastrophes, agressions et désastres majeurs de toutes natures avec le moins de conséquences dommageables sur la vie sociétale. Mais aussi, lui permettre de s'adapter ou de se reconstruire. Elle implique conscience des risques et menaces, préparation, rectitude des comportements, résistance psychologique et sens de l'intérêt général."* C'est une définition de la résilience qui est plus large que celle de la résilience d'un réseau technique, mais elle englobe non seulement la source du désastre, le niveau de préparation de tous les acteurs, mais aussi la réduction des conséquences. C'est dans ce cadre de cette « résilience sociétale » que la problématique des réseaux d'infrastructures se pose.

De nombreux exemples illustrent cette approche globale, en France et surtout aux États-Unis, notamment depuis le 11 septembre 2001. Les Américains ont mis en place deux institutions chargées spécifiquement de suivre ces risques : le "Community and Infrastructures Resilience" du « Departement of Homeland Security » (CIR-DHS), et dans le cadre de la gestion des incidents et de leurs conséquences au sein de la "Federal Emergency Management Agency" (FEMA).

L'Europe avec la directive REC *définit les entités critiques comme fournisseurs de services essentiels, joue un rôle indispensable dans le maintien de fonctions sociétales ou d'activités économiques vitales dans le marché intérieur"*[3]. À ce titre, les opérateurs des réseaux d'électricité, de télécommunications, d'eau et de transports, entre autres, peuvent être (voir sont) considérés comme des entités critiques, suivant des critères bien définis. En effet, la directive REC regroupe de nombreux secteurs économiques comme : l'énergie, les transports, les services bancaires, les infrastructures de marchés financiers, la santé, l'eau potable, les eaux usées, les infrastructures numériques.

Une fois transposée dans le droit français, la REC va venir remplacer le dispositif actuel de Sécurité des activités d'importance vitale (SAIV), créé par le décret de 2006 puis intégré dans le code de la défense. Ce dispositif juridique et réglementaire est piloté par le Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN). Ce dispositif interministériel vise à protéger les opérateurs considérés comme d'importance vitale, du fait de leur participation à la production et/ou à la distribution de biens ou de services indispensables à la continuité de l'État, au maintien du potentiel de défense ou de sécurité nationale et à l'économie française.

[2] Société : nation ou institutions regroupant des nations (UE…)

[3] "Directive sur la résilience des entités critiques", Parlement Européen et le Conseil – 30.11.2022

Cette protection est principalement axée autour des agressions, physiques ou cyber, sans prise en compte particulières et spécifique des risques naturels ou climatiques, ayant été créée dans l'après 11 septembre, le dispositif étant originellement tourné pour faire face à la menace terroriste, même s'il a intégré par la suite une vision plus large, vers la continuité d'activité, mais sans objectifs précis, autre que celle d'avoir un plan.

La directive REC a donc pour double objectif d'élargir les opérateurs concernés, mais aussi le spectre des risques et menaces, pour couvrir non seulement les menaces terroristes, mais également les urgences de sécurité publique, les attaques hybrides, ainsi que les risques de catastrophes naturelles, technologiques ou autres **avec un objectif essentiel la continuité d'activité des dits services essentiels avec le moins de perturbation possible.**

À ce titre, les entités concernées devront[4] donc :

- *Identifier tout risque pertinent susceptible de perturber de façon importante la fourniture de services essentiels ;*
- *Prendre des mesures appropriées pour assurer leur résilience ;*
- *Notifier les incidents perturbateurs aux autorités compétentes.*

Cette approche, plus globale et plus exigeante pour les opérateurs, vise à les préparer au mieux à la réalité des événements de toutes natures actuels et futurs.

Cette réalité se matérialise notamment lors d'événements climatiques majeurs, à l'instar de la tempête Alex, traitée dans cette analyse, ou encore des inondations, des tempêtes hivernales ou des canicules qui peuvent entraîner la perte de services essentiels pour des milliers ou dizaines de milliers de foyers et d'entreprises.

Les effets du changement climatique doivent être conjugués à une sensibilité accrue, souvent technologique, aux interdépendances entre réseaux. En effet, les plans de résilience de chaque opérateur sont souvent fondés sur l'hypothèse que les autres réseaux fonctionnent relativement normalement. À ce titre, ces plans de « gestion de crise » plus que de « résilience » sont réalisés en se concentrant uniquement sur les vulnérabilités propres de l'opérateur qui les réalise : chaque opérateur raisonnant comme s'il n'avait que sa propre vulnérabilité à résoudre, celle qui est directement sous sa responsabilité, et qu'il interviendra dans un environnement « stable » où l'énergie, les communications, les transports, les

[4] "Comment l'UE réagit aux crises et renforce la résilience", Conseil de l'Union Européenne

approvisionnements essentiels (carburants, ou autres ..) ou encore la disponibilité des personnels est acquise.. Or l'expérience des crises passées démontre la nécessité d'une autonomie « stratégique » pour l'opérateur qui veut être en mesure d'assurer son service essentiel. **Ce qui est loin d'être le cas aujourd'hui pour la plupart d'entre eux comme le démontrent nos entretiens (cf annexe).**

De nombreuses études techniques ont été menées sur les interdépendances, notamment aux Etats-Unis, et dans une moindre mesure en Europe. Mais l'analyse intersectorielle des interdépendances demeure complexe et dépend de nombreux facteurs tels que les structures techniques ou les formes de marchés des secteurs et de leurs évolutions (monopole, oligopole, duopole, concurrence de marché, etc.). Ceci a un impact très différent d'un secteur à l'autre.

Dans ce cadre, les points essentiels sont :

1 - De savoir si les sujétions de « résilience » **sont obligatoires ou facultatives**, si elles sont financièrement supportées par les entreprises et donc incluses à leurs coûts de production, ou financer sur fonds publics (impôts)
2 – De savoir **si les informations de vulnérabilités ou les échanges entre opérateurs sont prévus, codifiés par les textes, tant en termes de sécurité industrielle, technique que juridique** et que la confidentialité des données est bien assurée entre opérateurs et avec les services compétents de l'État ou des collectivités concernées.
3 – **De savoir enfin si l'objectif de résilience est chiffré**, soit en termes techniques : durée d'interruption admissible, perte acceptable de production en %, et ce dans un cadre géopolitique et de transition climatique ou technologique donné... avec en corollaire les dispositions prises par les différentes parties prenantes pour assurer ces objectifs : Entreprise, sous-traitants, pouvoirs publics, etc..
4 – **De savoir où (à quel niveau territorial) un minimum de résilience doit être assuré** au profit des populations entre les niveaux national, zonaux, régionaux, départementaux, intercommunaux ou communaux.

Sur ces points essentiels, le concept de résilience n'est pas encore complètement mature. Si nous voyons clairement avec la réglementation SAIV et bientôt la transposition de la directive REC, que les secteurs économiques concernés par ces réglementations vont vers des sujétions « obligatoires » face à une approche « tous risques (all hazards), de nombreux points restent en suspens tant sur les échanges d'information entre opérateurs que sur les objectifs de

résilience à atteindre qui ne sont pas aujourd'hui définis, ou sur la notion de résilience territoriale Vs résilience nationale. De nombreuses études complémentaires et des décisions doivent être entreprises et prises pour avoir une vision plus « claire » du concept de résilience nationale.

Car une politique de résilience nationale n'est pas qu'une politique nationale de résilience qui vise plutôt la préparation de l'État aux situations d'exception, c'est une politique qui permet à la nation de surmonter à moindre coût politique, économique et social une crise majeure par la préparation de tous les acteurs, à tous niveaux, y compris la population.

Ce rapport qui contribue à cette vision de résilience nationale a modestement pour objectif :

1- De dresser un inventaire des études menées sur la vulnérabilité des réseaux principalement face aux catastrophes naturelles (ou provoquées) à travers une bibliographie.
2- De mettre en perspective
    a. Les perspectives liées au changement climatique,
    b. Des liens d'interdépendance entre les réseaux dans ce cadre évolutif des risques,
    a. De compiler des informations sur l'organisation de certains opérateurs dans la gestion de leurs résiliences organisationnelle et structurelle.

I. Les perspectives liées au changement climatique

Les évaluations réalisées par le Groupe d'Experts Intergouvernemental sur l'Évolution du Climat (GIEC) et les données transmises par Météo France permettent d'avoir accès à une information scientifique fiable, claire et lisible sur les risques naturels induits par le changement climatique, en particulier pour les aléas inondations et canicules.

L'année 2022 a été la plus chaude mesurée en France avec une température annuelle moyenne dépassant les 14°C. Ce record n'est pas une surprise, il s'inscrit dans la tendance des 10 dernières années durant lesquelles nous avons recensé 8 des 10 températures les plus chaudes enregistrées depuis le début du XXe siècle.

Source : Bilan climatique de l'année 2022 – Météo France[5]

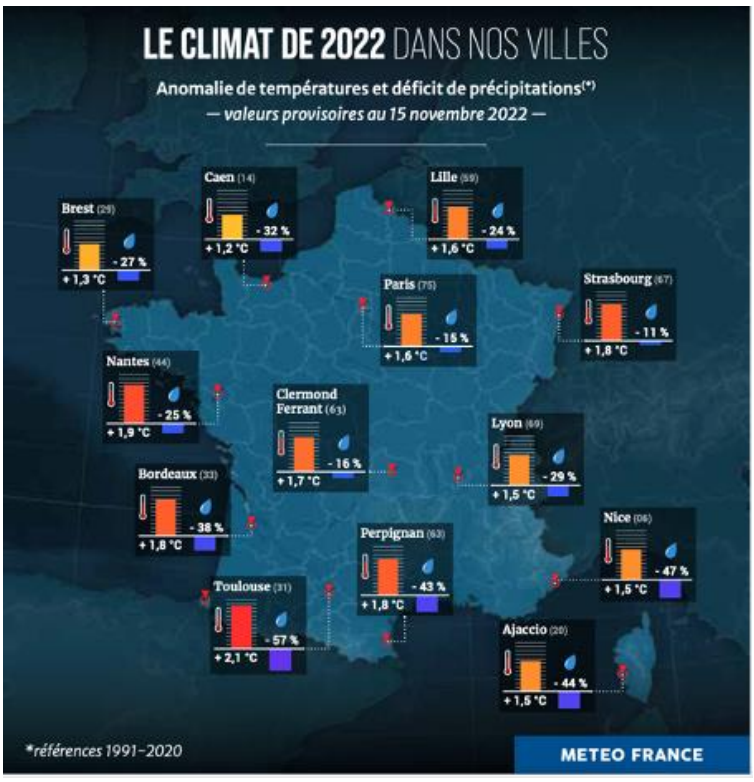
Ce record se traduit par des températures au-delà des normales de saison sur l'ensemble des mois de l'année excepté janvier et avril. De plus, trois vagues de chaleur ont accompagné cette

[5] https://meteofrance.com/sites/meteofrance.com/files/files/editorial/comm_presse_bilan_2022_site_internet.pdf

hausse généralisée. Ainsi, Météo France a recensé 33 jours de vagues de chaleurs, un record depuis 1983. Les prévisions estiment qu'en 2040 ces vagues de chaleur pourraient être 2 à 3 fois plus fréquentes et 1,5 fois plus intenses. Au-delà de l'augmentation de la température, on constate également pendant ces périodes une multiplication des orages intenses, parfois grêligènes, accompagnés parfois de mini-tornades, comme ce fut le cas en Bretagne.

Cette hausse des températures s'accompagne d'une baisse généralisée de la pluviométrie, d'après Météo France. Un déficit de 15 % à 25 % a été constaté par rapport à la normale 1991-2000 avec notamment un déficit de 60 % et 85 % pour les mois de mai et juillet 2022. Ce sont les mois les plus secs enregistrés depuis 1959. Ce manque d'eau a entraîné un épisode de sécheresse intense impactant 75% du territoire français et marquant la troisième période la plus longue enregistrée depuis 1976.

Si des périodes de sécheresse sont à redouter, on constate également une augmentation des précipitations en hiver, environ 10%. Mais elles ne sont pas réparties également sur le territoire et dans le temps. À ce titre, elles peuvent être source d'inondation par débordement dans de nombreuses communes.



Source : Bilan climatique de l'année 2022 – Météo France[6]

L'AFP, grâce aux données de Météo-France, permet d'établir des projections sur les évolutions climatiques, notamment en ce qui concerne la température.[7]

À partir des données, ils ont réalisé 3 scénarios à horizon 2050 : l'optimiste dans lequel les températures augmentent jusqu'à 1,6°C, l'intermédiaire dans lequel les températures augmentent de 2,2°C et un scénario pessimiste dans lequel les températures augmentent plus de 3°C. Étant donné le rapport du GIEC et les déclarations de Christophe Béchu, annonçant une hausse de 4°C en France, c'est le scénario pessimiste qui a été retenu dans ces exemples.

Le tableau ci-dessous résume les prévisions pour les villes de Paris, Marseille, Lyon et Bordeaux. Voici les éléments de définitions pour comprendre les données du tableau :

- Jours anormalement chauds : température du jour supérieure à 5°C par rapport aux normales de saison ;
- Jours chauds : journée où la température dépasse les 25°C ;
- Nuits caniculaires : nuit où la température est supérieure à 20°C.

	Température moyenne annuelle		Jours anormalement chauds		Jours chauds		Nuits caniculaires	
Paris	1976 - 2005 12°C	2050 +1,9°C	1976 - 2005 38	2050 +45 (83 jours totaux)	1976 - 2005 44	2050 +27 (71 jours totaux)	1976 - 2005 7	2050 +20 (27 nuits totales)
Marseille	1976 - 2005 15°C	2050 +2,3°C	1976 - 2005 19	2050 +55 (74 jours totaux)	1976 - 2005 89	2050 +33 (122 jours totaux)	1976 - 2005 31	2050 +40 (71 nuits totales)
Lyon	1976 - 2005 12°C	2050 +2,3°C	1976 - 2005 50	2050 +57 (107 jours totaux)	1976 - 2005 60	2050 +31 (91 jours totaux)	1976 - 2005 14	2050 +28 (42 nuits totales)
Bordeaux	1976 - 2005 13°C	2050 +2,3°C	1976 - 2005 39	2050 +50 (89 jours totaux)	1976 - 2005 66	2050 +36 (102 jours totaux)	1976 - 2005 7	2050 +21 (28 nuits totales)

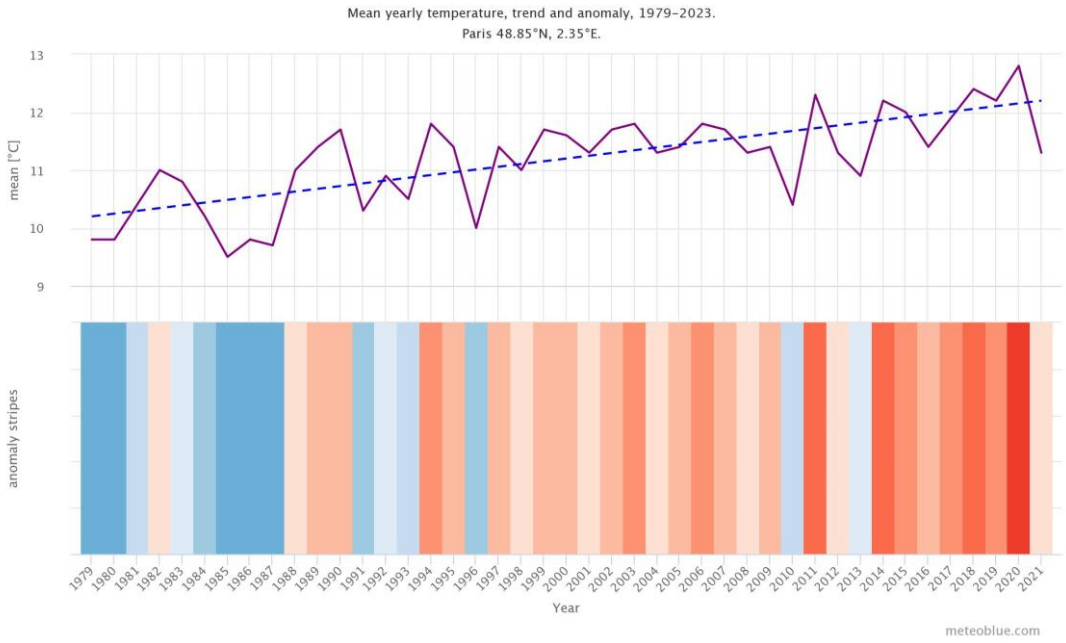
Les graphiques suivants, fournis par Meteoblue, relèvent les températures moyennes annuelles depuis 1979. Ils témoignent de la réalité de la hausse des températures. La ligne

[6] *Ibid*

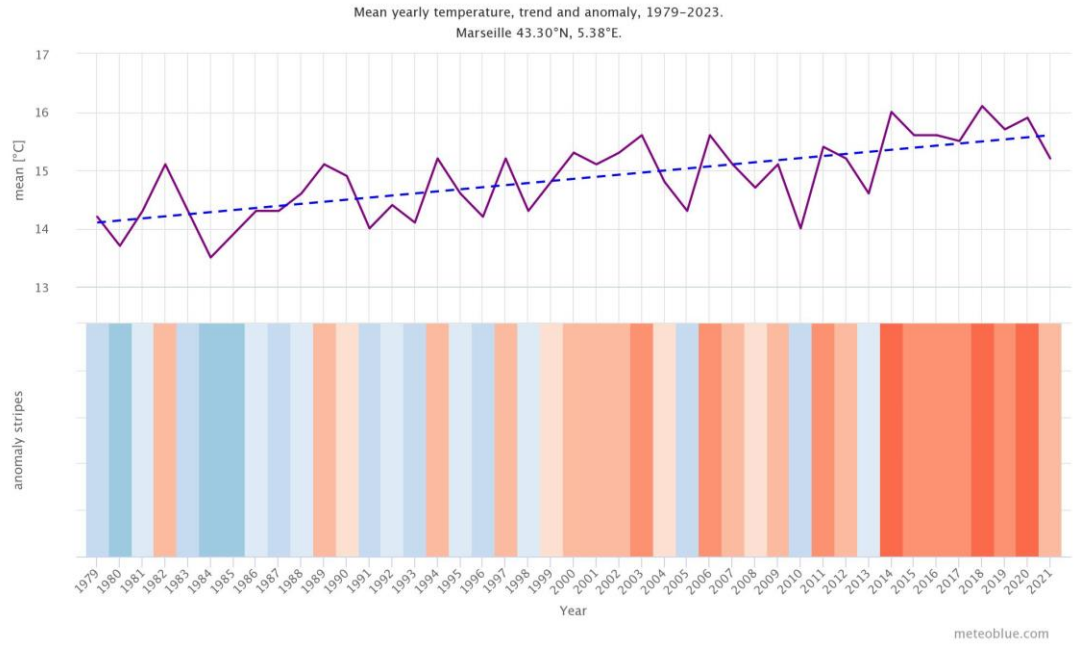
[7] "Quel climat en France dans votre commune en 2050 ?", AFP

bleue en pointillée représente la tendance du changement climatique, la ligne violette représente la température moyenne effective de l'année. Enfin, les barres verticales représentent les "bandes de réchauffement", chaque couleur représente la température moyenne d'une année, bleu pour les années les plus froides et rouge pour les années les plus chaudes.

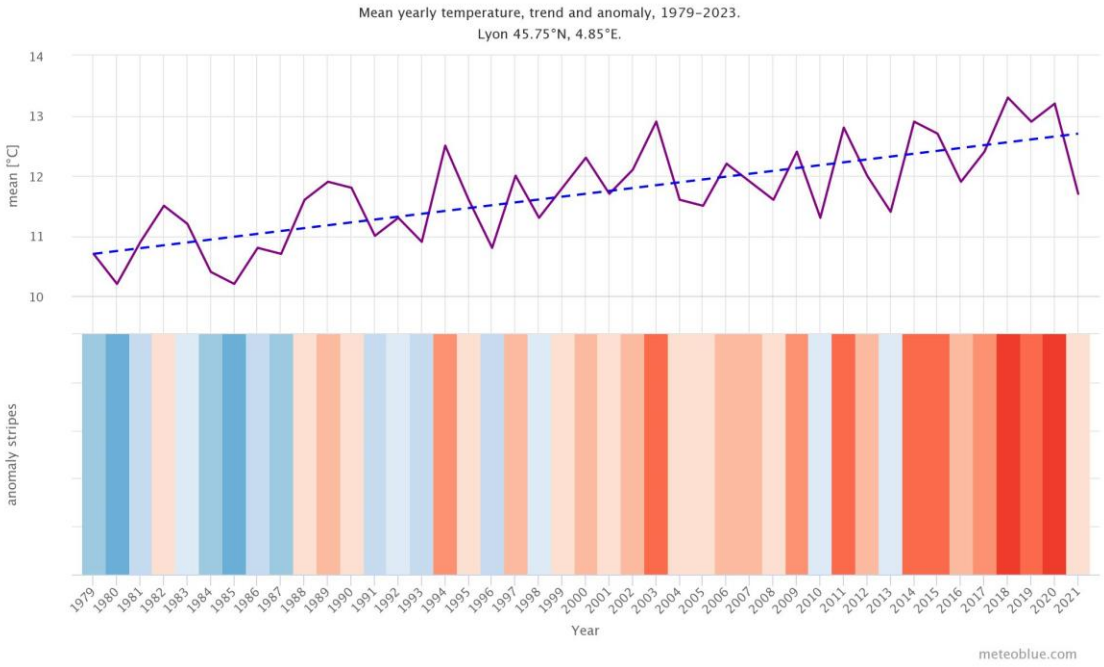
Paris



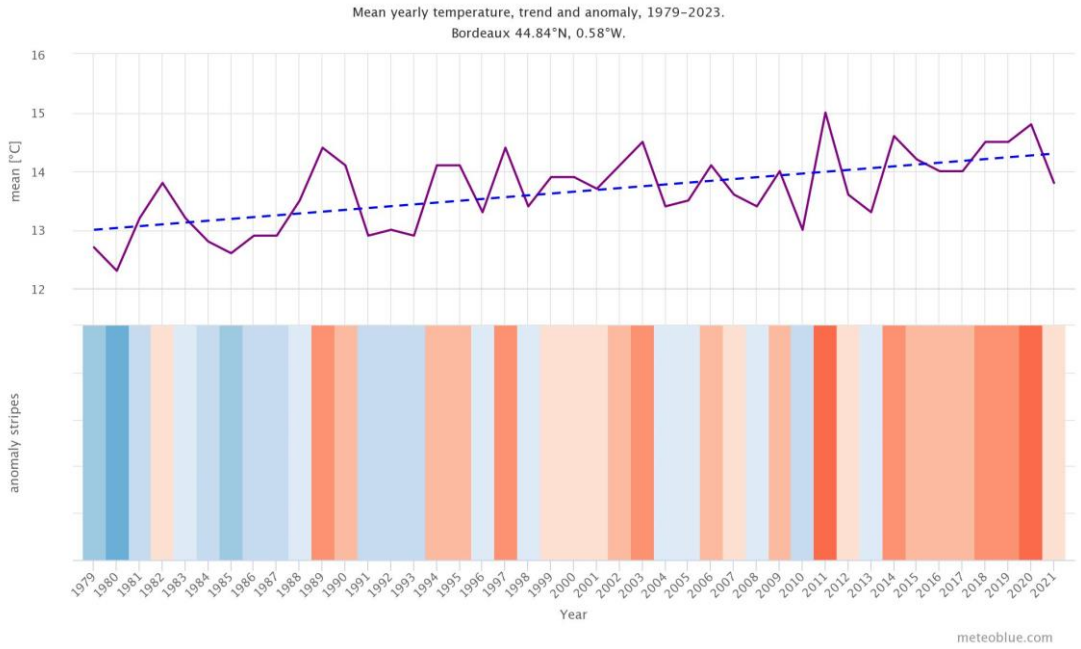
Marseille



Lyon



Bordeaux



Au-delà des évolutions affectant la vie quotidienne, le changement climatique est également à l'origine d'une multiplication et d'une intensification des événements climatiques. En France, ces dernières années font figure d'exemple : la tempête Alex en 2020 qui a dévasté notamment le département des Alpes-Maritimes, les incendies de la Teste-de-Buch et Landiras (33) en juillet 2022, accompagnés de plus de 100 départs de feux sur le même secteur et précédés d'une importante tempête de grêle en juin, les orages à Paris et en Corse au mois d'août 2022… À titre d'exemple, entre janvier et juin 2022, les pompiers des Bouches-du-Rhône sont intervenus sur 641 départs de feux, dont 230 uniquement au mois de juin.

Exemple d'interruption des réseaux à la suite de la Tempête Alex

Si la tempête Alex a traversé la France, le département des Alpes-Maritimes a été particulièrement touché. Elle y a provoqué des pluies atteignant 500 litres par mètre carré qui ont entraîné des crues diluviennes.

Entre le 2 et le 3 octobre 2020, la tempête Alex a touché trois vallées de montagne dans l'arrière-pays niçois : la Roya, la Vésubie et le basse Tinée. Ce phénomène méditerranéen, stationnaire et violent a été à l'origine de précipitations exceptionnelles entraînant des crues torrentielles rapides, des éboulements et des glissements de terrain. 10 personnes perdront la vie.

Les dommages sont estimés à environ un milliard d'euros, avec des dégâts considérables aux infrastructures publiques, aux réseaux et à près de 500 bâtiments (plus de 2 300 bâtiments ont dû être expertisés pour leur stabilité). Les destructions ont entraîné l'isolement de plusieurs communes pendant plusieurs mois. À titre d'exemple, neuf mois après l'événement, l'accès routier au secteur de la Tende était encore possible uniquement par convoi et le hameau de Casterino est toujours isolé.

Le cumul de ces précipitations a entraîné également des coupures d'électricité. Selon Enedis, environ 13 500 clients sont privés d'électricité en fin de soirée dans 13 communes, dont Saint-Martin-Vésubie, commune la plus touchée par la tempête. Les réseaux téléphoniques ont été coupés dans les trois vallées à cause de l'interruption des réseaux filaires et la coupure du réseau électrique. Mis à part les sites soutenus par groupe électrogène, l'ensemble des infrastructures se sont retrouvées sans électricité. Au total, près de 100 sites de radio (GSM) ont été affectés, les opérateurs mobiles et tous les sites radio de l'État ont subi des dégradations, les rendant inopérants pendant au moins 48h. Pour retrouver une situation normale sur l'ensemble du territoire, il faudra attendre plusieurs semaines.

Les lignes fixes, étant enterrées le long des routes ou fixées à des poteaux, ont été emmenées par les crues tandis que les réseaux mobiles ont été mis hors circuit, car les antennes, connectées par fibre optique et alimentée en électricité ont perdu ces deux éléments.

Par son intensité et ses conséquences, la tempête Alex témoigne bien de l'interdépendance et de la fragilité des réseaux face aux événements climatiques.

De manière générale, on peut considérer que dans le cadre du changement climatique et des risques naturels (et technologiques), **une analyse de risque doit être menée de manière « dynamique » à échéance régulière pour bien voir l'évolution des risques et les dispositifs clés à mettre en place** (redondance, durcissement, remplacement rapide...) en termes de résilience nationale et territoriale des réseaux d'infrastructures.

II. Les interdépendances des réseaux

De nos jours, le fonctionnement de la plupart des infrastructures de réseaux vitaux est étroitement lié les uns aux autres, ce sont ces interdépendances qui sont critiques au bon fonctionnement des services dits essentiels.

Les réseaux de transport, d'eau, d'électricité, de télécommunications et autres sont interconnectés et dépendent des autres réseaux (au moins en partie) pour leur fonctionnement. Ces interconnexions peuvent avoir des effets positifs sur le plan opérationnel, mais elles peuvent également aggraver la vulnérabilité des systèmes face aux pannes, incidents ou catastrophes.

Dans cette optique, il est crucial de comprendre comment les réseaux sont interconnectés et comment ils interagissent les uns les autres afin de mieux prévoir les risques liés à ces interdépendances et les effets d'un dysfonctionnement de l'un des réseaux sur l'ensemble du système.

Il convient donc de revenir dans un premier temps sur une description quantitative des principaux réseaux d'infrastructures vitaux en France :

- **Électricité**
  - **Nombre de sites de production**
    - 19 centrales nucléaires
    - 427 centrales hydrauliques
    - 600 barrages
    - 8000 Éoliennes (22 GW)
  - **Lignes électriques**
    - 1 400 000 km dont 105 000 km de très haute tension et haute tension reposant sur 100 000 pylônes
  - **Transformateurs** : 760 000 (en augmentation)
- **Transport**

- **Ferroviaire**
  - Réseau ferré 27 483 km dont 2 800 km de ligne à haute vitesse[8]
- **Routier**[9]
  - Réseau global : 1 103 451 km
  - Autoroutes : 12 379 km
  - Routes nationales : 8 470 km

- **Télécommunications**

  - Lignes téléphoniques
    - 1 100 000 km dont 390 000 km de lignes aériennes
    - 15 000 000 de poteaux
  - Connexion internet
    - 21 250 nœuds de raccordement abonné/optique[10]
    - 720 000 km de fibre optique
    - 2 200 datacenters
  - Téléphonie mobile
    - 15 000 antennes relais

- **Eau**

  - Stations d'épurations
    - 21 000 stations
  - Transport
    - 1 000 000 km de canalisations d'eau potable
    - 380 000 km de réseau d'assainissement

Ces réseaux sont vulnérables au changement climatique, tant par l'augmentation moyenne de la température, que par la multiplication et l'intensification des événements climatiques extrêmes. Du fait de l'interconnexion, les réseaux ou les systèmes de commande-contrôle (SCADA) , peuvent sous des délais plus ou moins longs, être impactés et « tombés » en cascade, rendant la délivrance des services essentiels impossible

[8] Source SNCF Réseau

[9] Source Bison Futé

[10] Le NRA/NRO est le point où convergent les lignes des abonnés d'un même quartier pour se raccorder au réseau national

Ces interconnexions peuvent se matérialiser de plusieurs manières. L'étude proposée par France Stratégie[11] identifie quatre types de vulnérabilités, de dépendances :

- Dépendance physique, qui se caractérise par un lien matériel entre les infrastructures
- Dépendance géographique, c'est-à-dire un lien de proximité entre les infrastructures (par exemple les câbles électriques suivent les routes) ;
- Dépendance cyber, quand il y a une transmission d'informations entre les réseaux. À titre d'exemple, si on utilise les télécommunications pour transmettre des informations politique, organisationnelle ou sociétale.

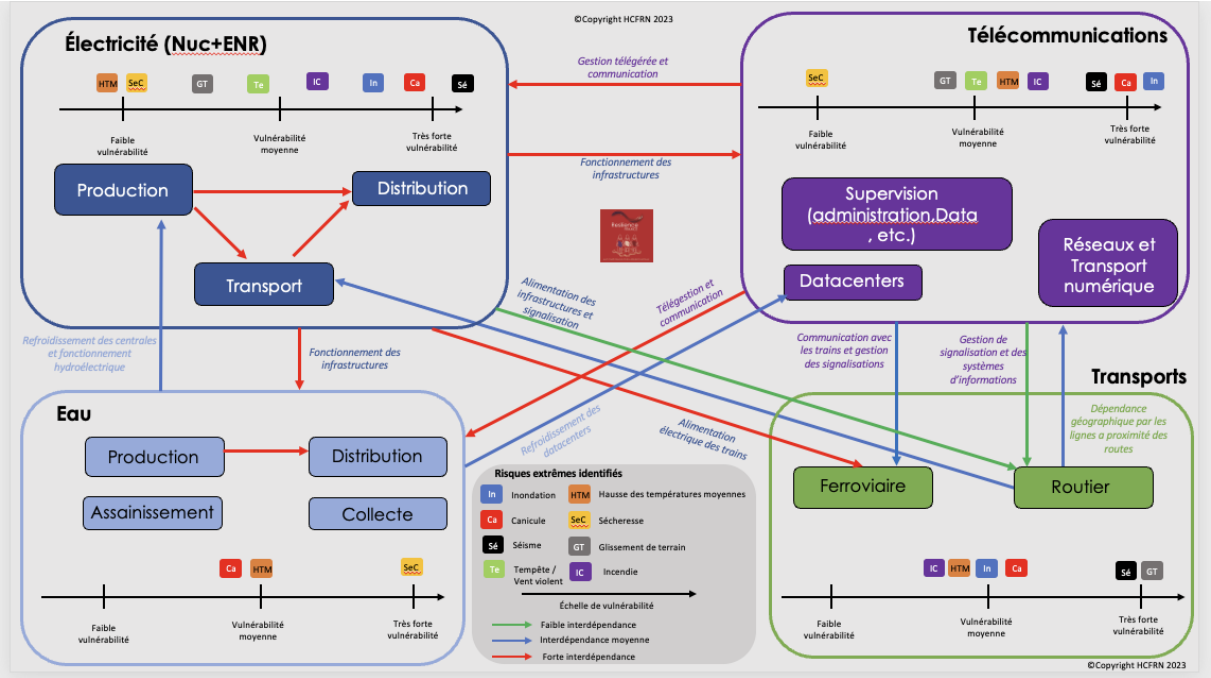
À laquelle on pourrait rajouter la dépendance économique extérieure, susceptible de fragiliser les investissements de sécurité, par exemple.

Il est important de noter qu'un réseau peut faire l'objet de plusieurs dépendances et de plusieurs types d'interdépendances.

Ce graphique, page suivante, créée par le HCFRN, résume les interdépendances entre les réseaux et les risques auxquels ils sont exposés, notamment face aux risques naturels ou climatiques. Une vision plus large schéma est disponible en annexe.

Au-delà des interdépendances techniques évidentes, comme l'alimentation en électricité par exemple, il faut souligner que certaines interdépendances ou mises en commun de ressources entre opérateurs présentent certains avantages tant économiques qu'environnementaux. Les opérateurs peuvent partager des sites d'installations et profiter d'accès déjà établis. Elles permettent aux opérateurs d'avoir une nouvelle approche de leurs réseaux, notamment grâce aux technologies de supervision et de contrôle à distance qui nécessitent des liens de télécommunications. En visualisant en direct l'état d'un site tant sur le plan de la supervision technique que souvent en vidéo, les opérateurs peuvent avoir une meilleure anticipation et une plus grande réactivité en cas d'incident.

[11] Risques climatiques, réseaux et interdépendances : le temps d'agir, France Stratégie, https://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/fs-2022-na108-risques_climatiques-mai.pdf



Si l'interconnexion des réseaux présente des avantages, elle peut également amplifier une crise, un aléa peut détériorer un secteur et entraîner une chaîne de dysfonctionnement induit en cascade. L'alimentation en eau potable est un exemple de cette interdépendance. En effet, les stations de traitement ont besoin d'un approvisionnement en électricité pour fonctionner, et des télécommunications pour que les systèmes de pompage et de traitement de l'eau fonctionnent et soient supervisés efficacement. Une perte d'un de ces réseaux peut donc entraîner une défaillance globale sur l'approvisionnement en eau potable.

Il est donc important d'analyser les interactions entre les réseaux pour comprendre les désordres qui pourraient survenir. Par exemple, une crue de la Seine à Paris pourrait toucher l'ensemble des réseaux et paralyser la vie économique. Chaque opérateur doit donc identifier les réseaux auxquels ils sont connectés et comprendre leurs vulnérabilités. C'est à partir de cette étude qu'ils seront en mesure d'analyser l'ensemble des risques auxquels ils sont exposés.

À partir du graphique étudié précédemment, on peut identifier des réseaux comme *"critiques"* du fait de leurs liens d'interdépendances avec les autres. Sur ces réseaux, un dysfonctionnement entraîne des réactions sur une grande partie des autres réseaux.

À ce titre, on retrouve quatre liens critiques d'interdépendances, qui ont également été relevés par le GIEC :

- Utilisation des technologies de l'information et de la communication pour le fonctionnement de nombreuses infrastructures ;
- Utilisation de l'eau pour la production électrique et le refroidissement d'unités de production ;
- Utilisation d'énergie pour le fonctionnement des systèmes d'infrastructures ;
- Utilisation des transports pour accéder aux ressources et aux réponses d'urgences.

Réseau électrique

Le réseau électrique est essentiel à une grande majorité des autres réseaux pour assurer leur fonctionnement. Cependant, il est lui aussi dépendant dans certains domaines. En effet, en ce qui concerne la production, les réseaux d'eau sont importants pour assurer le refroidissement des centrales nucléaires et pour mettre en œuvre les ouvrages hydroélectriques. Selon le degré de défaillance de l'approvisionnement en eau, pouvant aller d'une limitation du débit disponible à un arrêt complet, cela peut entraîner une limitation ou un arrêt de la production électrique.

De plus, les systèmes de télécommunications jouent également un rôle majeur pour coordonner la production et assurer la distribution électrique.

Enfin, au-delà de ces dépendances, le réseau de distribution électrique (Enedis) a une dépendance géographique avec le réseau routier, ce qui est moins le cas du réseau de transport (RTE - haute et moyenne tension). En effet, les infrastructures électriques de distribution suivent généralement le tracé des routes. De fait, un aléa sur ce réseau aura probablement des conséquences sur la distribution électrique.

Le réseau électrique a plus d'impacts sur les autres réseaux que de dépendances à ces derniers. Cependant, une défaillance en eau ou en télécommunication pourra le mettre à défaut dans ses capacités de production et de transport et une défaillance de l'approvisionnement en eau pourra limiter sa capacité de production.

Réseau de télécommunication

À l'instar du réseau électrique, le réseau de télécommunication est essentiel à une majorité d'autres réseaux et aussi extrêmement important en temps de crise pour les populations. En matière de contrôle-commande, de supervision (SCADA), d'échanges de data, et de surveillance, les télécommunications se sont développées dans l'ensemble des secteurs de la vie économique et sociale.

Les réseaux de télécommunication sont également dépendants du réseau électrique pour faire fonctionner leurs propres infrastructures, bien que la plupart, notamment les antennes relais et les datacenters, soient secourus, soit par des batteries ou par des groupes électrogènes, mais pour des durées courtes.

À titre d'exemple, les antennes 4G et 5G disposent bien d'une batterie de secours, mais qui ne dispose le plus souvent que de 20 à 40 minutes d'autonomie[12]. Un manque d'électricité, qu'il soit lié à une panne de production ou de distribution, entraînera de fait une défaillance rapide sur le réseau de télécommunication mobile, voire fixe.

Le concept est toujours une prise en charge automatique sur une durée courte (pas défini par chacun des opérateurs de la même manière) par ces dispositifs et une mise en œuvre de groupes de secours sur des réserves régionales ou nationales de l'opérateur ou d'opérateurs ou d'entreprises de services extérieurs si la panne est de plus longue durée. Mais dans ce dernier cadre, les problèmes d'approvisionnement, de transport ou d'accès de moyens peuvent se poser (exemples : les tempêtes Klaus ou Alex ou l'ouragan Irma à Saint-Martin)

Mais les capacités de réserves nationales ou régionales sont souvent par définition limitées et ne peuvent garantir un approvisionnement « sécurisé » à chacun en cas d'évènement majeur..

À l'instar du réseau électrique, une grande partie du réseau de télécommunication a une dépendance géographique avec les routes : les câbles et les pylônes suivant leur tracé. À ce titre, un aléa sur ce réseau pourra avoir des conséquences sur les réseaux de télécommunication fixe et mobile.

[12] Source : Conversations avec Orange, gestionnaire d'antennes réseau, sur les plans « délestage »

Production et distribution d’eau potable

Comme indiqué précédemment, le réseau d’eau potable a des liens avec le réseau électrique. Les usines de production d’eau et les systèmes de stockages (réservoirs) et de distribution sont également dépendants de l’électricité pour assurer le bon fonctionnement des infrastructures. Une coupure électrique peut entraîner rapidement une défaillance dans la production et la distribution d’eau potable, même si de nombreux réseaux locaux utilisent le principe de la gravité pour la distribution, les besoins de pompage et de supervision demeurent sur ces réseaux très diffus géographiquement.

Par ailleurs, les réseaux d’eau potable sont majoritairement gérés en télégestion. Cette automatisation permet de contrôler l’ensemble des installations techniques : de leur pilotage à l’analyse du traitement en passant par la surveillance de l’état des installations. Le réseau d’eau est donc dépendant des réseaux de télécommunication pour la production d’eau potable (notamment en dehors des heures ouvrables), mais également la distribution (contrôle du niveau des réservoirs).

Le réseau d’eau potable a donc deux dépendances principales, l’électricité et les télécommunications. Une défaillance d’un de ces deux réseaux risquera d'entraîner une dégradation ou un arrêt de la production ou du transport et donc de la distribution d’eau potable à la population.

Réseaux de transport ferroviaire et routier

On identifie au sein du réseau deux modes de transport : le transport ferroviaire et le transport routier. Chacun ayant des besoins et des relations différentes avec les autres réseaux d’infrastructures.

Le réseau routier n’est pas très dépendant des autres réseaux d’infrastructures. Il peut presque fonctionner en autonomie. C’est la qualité de service sur le réseau qui va être affectée en cas de défaillance électrique ou de télécommunication. En effet, le réseau routier va avoir des dépendances sur la signalisation, l’éclairage, les pompes de carburants, et les péages. Ce sont des éléments qui peuvent perturber ou limiter les automobilistes et les routiers, mais qui n'empêchent pas la circulation physique sur le réseau. L’encombrement ou l’accident sont les principaux risques sur le réseau routier, avec un risque pour l’intervention des services de

secours et des équipes des DIR, hors dégradation physique de ce dernier suite à un aléa majeur : inondation, neige, glace, pluie intense, canicule (avec risque de fonte des enrobés) . Là, la remise en état dépendra aussi de l'accès aux infrastructures pour les opérateurs en charge de la restauration de l'infrastructure routière concernée.

Le réseau ferroviaire a plus de vulnérabilités face aux réseaux électriques et de télécommunication, le premier fournissant l'énergie indispensable à la circulation des trains (à l'exception des motrices diesel) et le deuxième permettant de coordonner cette circulation et de gérer la signalisation. Une défaillance sur le réseau électrique entraînera le quasi-arrêt de la circulation, l'impact d'une perte des télécommunications dégradera au moins la qualité du service ou imposera l'arrêt complet du trafic pour des questions de sécurité, même si des modes dégradés ultimes existent dans le transport ferroviaire, cela limite considérablement la viabilité du réseau ferroviaire.

Exemple des conséquences d'une défaillance sur le réseau électrique

À titre d'exemple, un aléa causant des dommages « longs » sur la production et/ou la distribution d'électricité sur une zone géographique importante risque d'entraîner une panne des télécommunications, notamment mobile et radio, car les antennes sont reliées au réseau électrique. En cascade, cette panne électrique et des télécommunications impacteront le réseau ferroviaire, en le réduisant ou en le paralysant, et le réseau routier, en le congestionnant au moins et réduisant ainsi les capacités de réponse des pouvoirs publics. D'une crise sectorielle peut découler une crise intersectorielle, puis dans la durée une crise potentielle « sécuritaire » voire, en fonction des temps de rétablissement, une crise politique et sociétale.

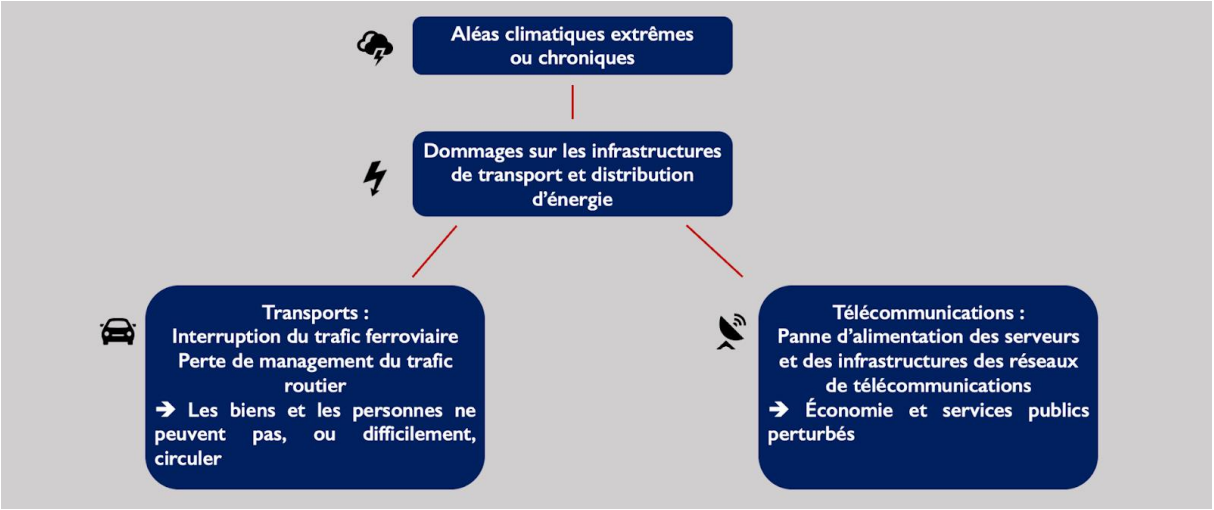


Schéma inspiré de la figure 6.2 du Rapport du GIEC[13]

Sur l'action des opérateurs et de l'État en temps de crise, une défaillance des réseaux de télécommunications pourra perturber non seulement la remise en bon état de marche des autres réseaux touchés, mais aussi les équipes de réparation ayant besoin de communications fiables, pour coordonner leurs efforts et planifier les travaux de réparation[14]. De plus, une perte des télécommunications risque également de toucher les réseaux de communication des services de sécurité et de secours qui ne seront plus indépendants des réseaux grand public d'ici quelques années (Réseau RRF), même si ces entités bénéficieront de canaux prioritaires, il faut que le système soit opérationnel.

L'interdépendance et l'interconnexion entre les réseaux sont donc une réalité incontournable. Si c'est une source non négligeable d'avantages techniques et économiques, cela présente également des risques de contagion entre ces derniers, pouvant entraîner des conséquences pour les populations touchées et de manière générale en termes de sécurité nationale.

Il est donc essentiel de mieux comprendre leurs interdépendances et leurs vulnérabilités pour améliorer la résilience de ces réseaux face aux risques et menaces à venir, dont les défis liés au changement climatique. La doctrine repose souvent plus sur des postures réactives, en s'appuyant sur des retours d'expériences, que sur une réelle anticipation des phénomènes. Le changement climatique va imposer aux opérateurs un travail d'anticipation plus sérieux.

[13] Climate Change 2022 : Impacts, Adaptation and Vulnerability – p.928

[14] Retex Klaus et Sandy

Cette prise en compte des interdépendances est complexe pour les opérateurs pour plusieurs raisons. Dans un premier temps, la multiplicité des réseaux et des opérateurs dans un cadre d'économie de marché plus ouverte et plus concurrentiel rend plus difficile l'approche globale des risques et des interdépendances, car les responsabilités sont plus diluées entre opérateurs complémentaires sur un créneau global, mis les règles d'ouvertures des marchés rend également la démarche plus difficile.

L'exemple de la structure de la SNCF ou d'EDF est parlant à cet égard. SNCF :Holding, Réseau, Gares et connexions, autant de structures quasi indépendantes sur les questions de sécurité et de résilience ... L'énergie électrique (EDF, RTE, Enedis..), autant de structures indépendantes quasi monopolistiques sur un créneau majeur de production de services essentiels souhaitées par l'Europe pour éliminer les monopoles, et qui en fait les égratignent à peine, compte tenu des niveaux d'investissements majeurs pour « rentrer » dans ces marchés. **Cette approche très doctrinaire provoque un niveau de complexité majeur sur les questions de sécurité et de résilience**. Elles limitent également l'approche globale et rendent plus difficiles les investissements nécessaires.

III. Vulnérabilité des réseaux face aux risques naturels au regard du changement climatique

Le travail mené sur les réseaux d'électricité, de transport routier et ferroviaire et de télécommunications souligne la vulnérabilité des infrastructures dans le contexte d'un climat en pleine évolution.

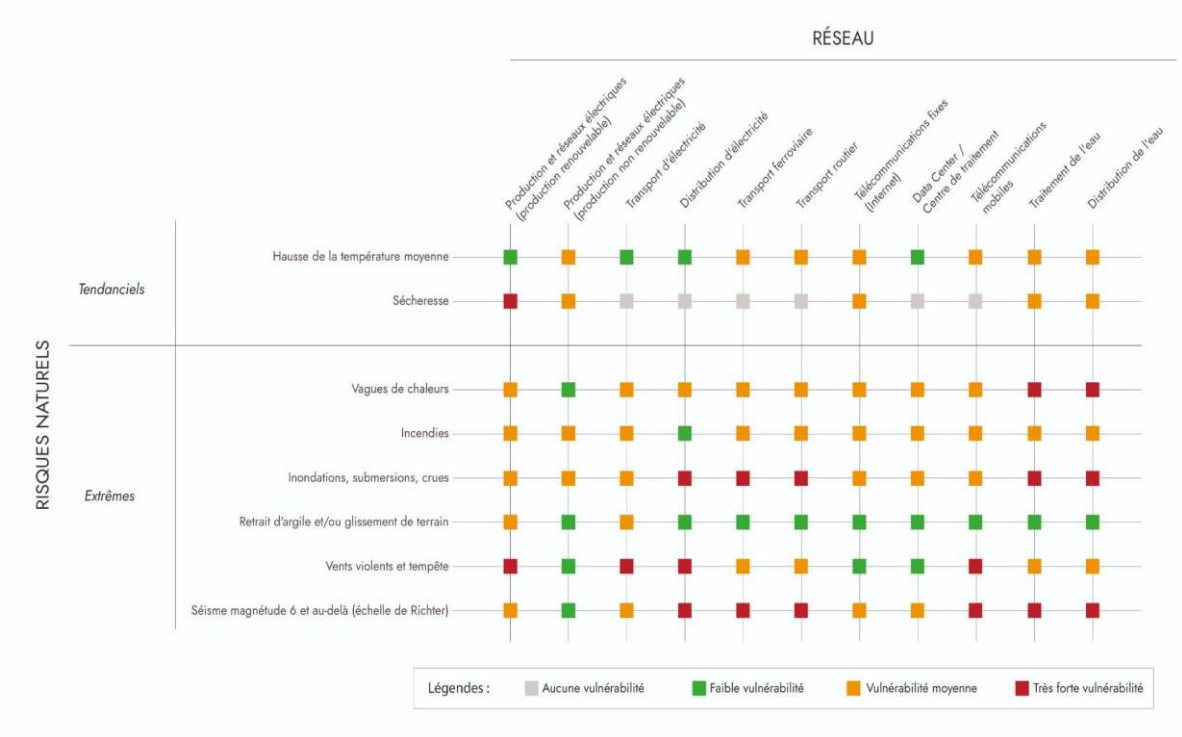
Les risques liés à la hausse des températures et aux événements climatiques extrêmes peuvent avoir des conséquences sur les équipements actifs ou passifs des réseaux. Dans ce cadre, l'interdépendance des réseaux augmente leurs vulnérabilités. D'après le GIEC, les interdépendances dans le contexte du changement climatique concernent notamment l'utilisation des technologies de l'information et les réseaux d'électricité du fait de leur vulnérabilité intrinsèque et des conséquences de leurs défaillances sur les autres réseaux.

Pour rappel, le changement climatique est notamment générateur en France des aléas suivants :

- Hausse globale des températures ;
- Augmentation et intensification des vagues de chaleur (on parle en France de vagues de chaleur à partir de 30°C diurnes et 18°C nocturnes pendant 3 jours consécutifs) ;
- Augmentation des précipitations en hiver (environ 10%, mais de manière plus violente et localisée) ;
- Baisse des précipitations en été (générateur de sécheresse) ;
- Augmentation de l'occurrence de tempêtes et de vents violents.

Chaque risque va impacter plus ou moins fortement le fonctionnement d'un réseau. Il est possible d'établir l'exposition des réseaux identifiés comme *"critiques"* aux aléas induits par le changement climatique. Pour rappel, les réseaux identifiés comme *"critiques"* dans cette étude sont l'électricité, les télécommunications, les transports (routier et ferroviaire) et l'eau.

Le schéma ci-dessous analyse les interactions des réseaux avec les aléas



S’il a été identifié que les réseaux seront plus ou moins vulnérables à différents événements climatiques, il est intéressant de savoir comment se traduisent réellement ces vulnérabilités.

Réseau électrique

Ce réseau peut être impacté sur son ensemble, de la production jusqu’à la livraison chez le client, et par plusieurs risques.

De manière générale, la hausse des températures moyennes va être à l’origine d’une augmentation de la consommation électrique, notamment au travers des climatisations et des ventilateurs. Si la demande dépasse la capacité de production d’électricité, elle peut être à l’origine de pannes et/ou de délestages localisés. De plus, les opérations de maintenance et/ou de réparation peuvent être décalées ou ralenties. En effet, face à des températures extrêmes, les travailleurs voient leur productivité réduite et leur temps de travail limité pour les protéger de la canicule. De plus, dans le cadre de réparation, certaines pièces peuvent être confrontées à l’obsolescence et/ou à des difficultés de remplacement (chaînes d’approvisionnement national ou internationale), les réseaux électriques ayant en moyenne 50 ans d’âge.

La production peut être impactée par plusieurs risques. Il convient dans un premier temps de distinguer deux types de production électrique : les énergies renouvelables et les énergies non renouvelables. La première concerne la production solaire, éolienne et hydroélectrique. La production à l’aide d’énergie non renouvelable concerne principalement, en France, le nucléaire.

La production nucléaire va être impactée notamment par la hausse des températures moyennes d’un côté, qui va participer à la montée en température des installations, et à la sécheresse de l’autre qui va limiter l’approvisionnement en eau, indispensable pour refroidir les réacteurs, tant par insuffisance de débit des rivières et fleuves que par la nécessité de limiter la température des rejets pour préserver la faune aquatique. De plus, au-delà du manque d’eau, la montée des températures fait perdre en efficacité la production hydraulique, ce qui peut entraîner une forte limitation des capacités de production.

Les énergies renouvelables :

- La production solaire est, elle, exposée au risque incendie, aux vents violents et aux tempêtes, et éventuellement aux séismes, qui peuvent endommager ou détruire les panneaux solaires.
- La production hydro-électrique est également soumise à ces risques, mais surtout à la sécheresse qui va limiter l'approvisionnement en eau et de fait les capacités de production hydro-électrique.
- Enfin la production éolienne est soumise aux risques d'incendie et d'absence de vent (canicule), mais elle sera surtout exposée aux vents violents et aux tempêtes, les éoliennes ne pouvant fonctionner si la vitesse du vent est trop élevée.

Le transport et la distribution d'électricité vont être confrontés à d'autres problématiques. En effet, la hausse des températures va réduire la capacité de transport des câbles, moins performants lorsqu'ils chauffent. En parallèle, les différents risques climatiques (incendies, séismes, inondations, les vents violents et les tempêtes) peuvent endommager (déformation des aciers) ou les aléas mentionnés, détruire les infrastructures (pylônes, câbles) et de fait limiter ou interrompre le transport d'électricité.

Il est nécessaire d'identifier avec les acteurs interrogés le seuil de température à partir duquel les réseaux peuvent subir des dommages. **Il est régulièrement évoqué la barre de 40°C dans la littérature.**

La hausse des températures, et les phénomènes de température extrême vont donc impacter la production, par les risques de surchauffe, mais également le transport d'électricité, les câbles étant moins performants. Le transport peut également être dégradé ou interrompu en cas de dégradation sur les infrastructures liées à d'autres événements climatiques. **Le réseau d'électricité est donc particulièrement sensible aux changements climatiques et son fonctionnement est vital pour les autres réseaux.**

Réseau de télécommunication

Le réseau de télécommunication peut dans un premier temps être impacté par une défaillance du réseau électrique, essentiel à son fonctionnement. Une panne électrique peut être à l'origine d'une coupure totale de l'ensemble des communications si jamais les infrastructures (antennes relais, datacenters, etc.) ne sont pas secourues par des groupes électrogènes ou si

la panne est de longue durée. À l'instar du réseau électrique, des températures élevées vont réduire les opérations de maintenance et de réparation.

Les datacenters, s'ils ne sont que peu exposés par la hausse moyenne des températures, le seront plus aux vagues de chaleur, car ils seront plus compliqués à refroidir. Une trop forte température pouvant endommager les infrastructures et nécessiteront un ralentissement ou un arrêt de certaines machines ou serveurs.. Les installations sont également exposées à l'ensemble des risques pouvant les endommager ou les détruire, c'est-à-dire les incendies, les séismes, ou encore les glissements de terrain.

Les antennes-relais, indispensables aux réseaux mobiles, sont également sensibles à l'ensemble des risques pouvant les endommager ou les détruire, séismes et tempêtes en tête. **Les vagues de chaleur peuvent également provoquer des surchauffes des installations et réduire leurs performances ou augmenter le taux de panne.**

Face aux risques de températures extrêmes, les infrastructures et notamment les câbles en cuivre et les fibres optiques peuvent être dégradés et ainsi perturber la qualité de connexion, entraînant des temps de réponse plus longs, voire cesser de fonctionner.

Ces mêmes "câbles", enterrés ou en plein air, sont exposés potentiellement, soit aux risques de séisme, soit aux vents violents et aux tempêtes.

De plus, le réseau télécom dispose très régulièrement d'une dépendance physique et géographique avec le réseau électrique, les lignes étant parfois montées sur les mêmes pylônes, et avec le réseau routier, les pylônes suivant généralement les routes. Il pourra donc être impacté en cas de défaillance sur ces réseaux (chute d'arbres, etc.) .

Le réseau de télécommunication est également particulièrement sensible aux changements climatiques, notamment la montée des températures et les phénomènes de canicule, car les infrastructures techniques ne sont pas prévues pour supporter de telles températures.

À l'instar du réseau électrique, la littérature fait état de 40°C comme valeur limite standard des réseaux aujourd'hui.

Réseau d’eau

Le réseau d’eau est, par définition, particulièrement vulnérable à la montée des températures moyennes, les phénomènes de chaleurs extrêmes, les sécheresses et la baisse des précipitations, car ce sont des événements venant directement réduire les ressources disponibles pour répondre à la demande en eau des populations.

A contrario, l’augmentation et l’intensification des risques de précipitations orageuses, et donc l’arrivée massive d’eau sur un système d’assainissement peuvent surcharger ce dernier et être à l’origine de plusieurs conséquences : débordement entraînant une inondation et endommagement des conduites liées à une surpression.

En parallèle, à l’instar des autres réseaux, le réseau d’eau est sensible aux événements climatiques susceptibles d’endommager ou de détruire ses infrastructures (stations de pompage, conduites d’eau, pompes, etc.) tels que les inondations, glissement de terrain ou encore les incendies.

Il est également dépendant du réseau électrique, indispensable pour mettre en action les différentes stations, et du réseau de télécommunication pour coordonner l’action des machines et assurer un bon traitement des eaux. Il peut être aussi impacté par des canicules sur certains équipements électromécaniques. Là aussi, le réseau est souvent âgé de plusieurs dizaines d’années

Réseau de transport.

Il convient de distinguer au sein de ce réseau les transports routiers et ferroviaires. Le réseau ferroviaire, par ses infrastructures et ses besoins, est plus vulnérable et dépendant que le réseau routier.

En effet, la hausse des températures, et notamment les températures extrêmes, va être à l’origine de la dilatation des voies de chemin de fer. Cette dilatation, liée à la température extérieure et à la température générée par le passage des trains, pourra être maîtrisée en limitant la vitesse de ces derniers. Ainsi, si la circulation n’est pas interdite, elle est en revanche fortement ralentie. Le transport ferroviaire est également vulnérable aux tempêtes et aux fortes pluies qui peuvent être à l’origine d’inondations, de glissements de terrain, de chutes d’objet et d’endommagement des infrastructures ferroviaires.

De plus, le transport ferroviaire est dépendant du réseau électrique et des télécommunications pour fonctionner. Une panne sur un de ces réseaux entraînerait de fait un ralentissement ou une interruption du trafic ferroviaire.

Le réseau routier sera également vulnérable aux événements climatiques, notamment ceux venant à endommager, encombrer ou détruire la voirie ou des ouvrages (ponts, tunnels, etc.). Nous parlons ici d'inondations, de tempêtes ou encore de glissements de terrain. Il sera en revanche moins dépendant des autres réseaux, excepté pour les pompes à essence ou stations de recharge électrique, péages et certains outils de signalisation. De fait, un incident sur le réseau électrique ou les télécommunications pourrait désorganiser le trafic routier, mais ne l'empêchera pas physiquement, sauf destruction de voirie.

En revanche, du fait du lien géographique entre les routes et les réseaux électriques et de télécommunications, un aléa sur le réseau routier aura de fortes occurrences d'impacter le réseau électrique et/ou le les télécommunications.

IV. Les actions à mettre en place

Dans un contexte où l'ensemble des réseaux sont interdépendants et exposés aux risques engendrés par le changement climatique, il est nécessaire que les acteurs concernés (opérateurs et État notamment) prennent des mesures « coordonnées et standardisées » pour assurer la résilience des réseaux, essentiels à la continuité du pays.

À titre individuel, les opérateurs doivent non seulement prendre en compte le changement climatique dans leurs analyses de risque, mais également s'assurer de la robustesse de leurs infrastructures face aux nouveaux défis et viser une résilience en profondeur de leurs réseaux.

Le Haut-Commissariat au Plan suggère 3 axes stratégiques pour renforcer la prise en compte de cette interdépendance. Le premier consiste à renforcer et partager les connaissances sur les impacts du changement climatique sur les réseaux et les interdépendances entre eux.

Cela implique de faciliter l'utilisation d'un même jeu de projections climatiques par l'ensemble des acteurs et de renforcer la connaissance de l'état actuel des infrastructures de réseau et de leurs liens de dépendance. ***Ce renforcement permet à l'ensemble des acteurs de partir avec le même degré de connaissance et les mêmes projections pour construire une analyse de risque complète prenant en compte les interdépendances***.

Le deuxième consiste à mettre en place une gouvernance nationale pour coordonner les efforts de tous les acteurs concernés. Cela implique la création d'une instance de travail rassemblant à minima les gestionnaires de réseaux et de l'État, ainsi que l'inscription dans la loi de la réalisation d'une feuille de route conjointe d'adaptation des réseaux au changement climatique. Cette réunion d'acteurs permettra notamment de coordonner les efforts des acteurs concernés. Les structures de sécurité nationale du PM et des ministères pourraient assurer ce rôle.

***Enfin, le troisième axe consiste à asseoir la vision nationale sur les démarches territorialisées*.** Cela implique de proposer à des territoires d'expérimenter un système d'établissement d'un diagnostic et d'un plan d'action partagés à l'échelle locale, **visant une résilience décentralisée minimum, dans le cadre d'une résilience territoriale bien comprise**.

Il faut aussi être en mesure de remonter et de capitaliser les informations de terrain au sein de chaque opérateur et les intégrer dans un tableau de bord au niveau national. En prenant en compte ces interdépendances dans les stratégies d'adaptation, il sera possible de mieux gérer les risques liés au changement climatique et de renforcer la résilience de ces réseaux d'infrastructures.

Techniquement ces stratégies d'adaptation seront variées, pas exemple – choix de matériaux, composants techniques ou électroniques aptes à supporter des températures extrêmes, autonomie accrue en cas de perte d'électricité pour assurer une autonomie sur au moins 24h, etc.. Mais tout cela implique des demandes exprimées clairement et de manière coordonnée dans les cahiers des charges publics de l'État, des collectivités et des opérateurs eux-mêmes... Une vraie révolution qui ne pourra se faire que sur une vision globale de l'état en la matière.

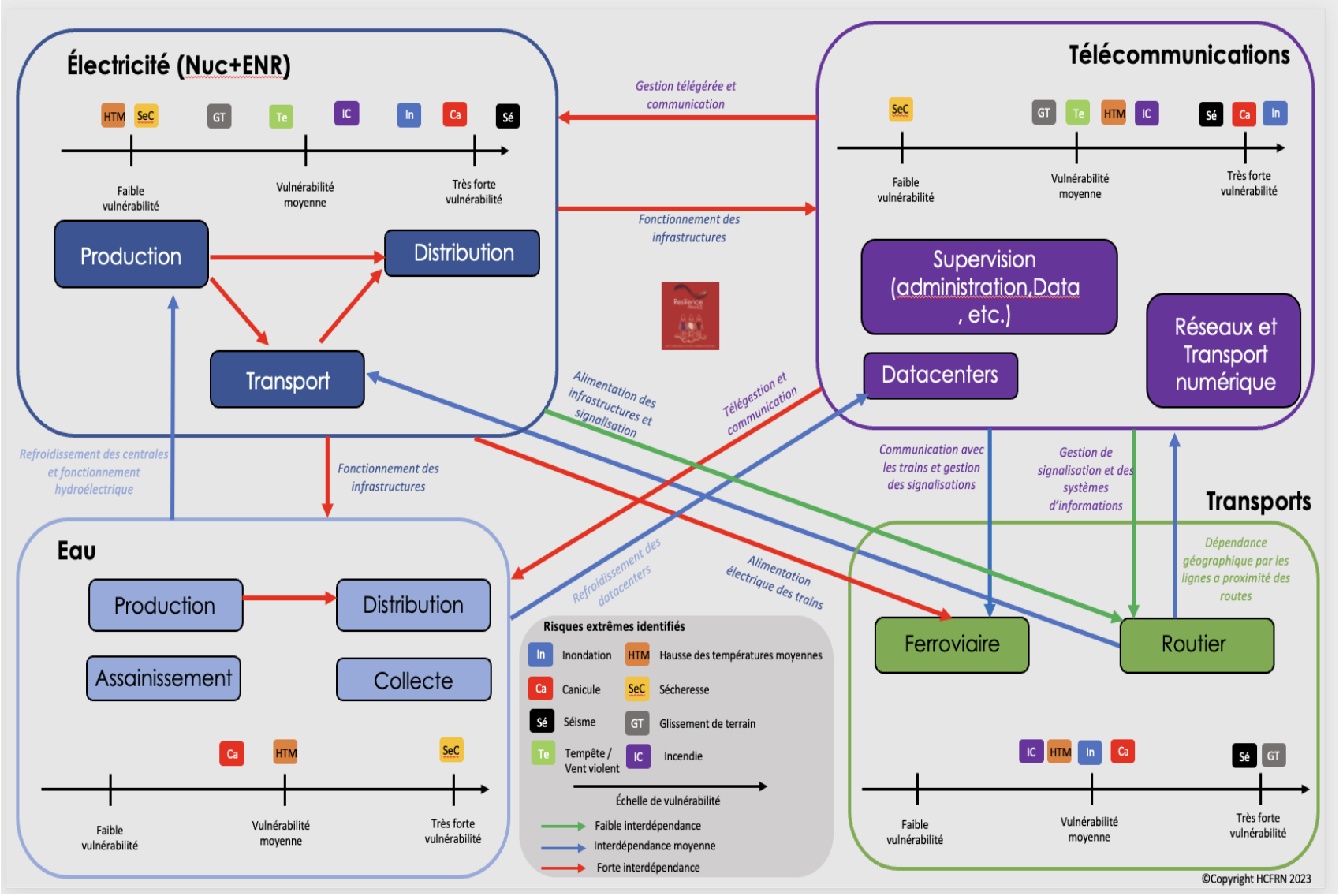
Pour conclure, on peut résumer la vulnérabilité des réseaux au regard du changement climatique en quelques points clés :

- Les infrastructures des réseaux d'électricité, de télécommunications, de transports et d'eau sont vulnérables au changement climatique, en raison notamment de la hausse des températures et de la plus grande fréquence des événements climatiques, intenses ou extrêmes : canicules, sécheresses, pluies, inondations, tempête.

- Les interdépendances constatées entre ces réseaux rendent leur vulnérabilité encore plus grande, car un problème sur un réseau peut impacter les autres par des effet s cascade non maitrisés.

- **Les actions mises en œuvre pour adapter ces réseaux au changement climatique sont encore partielles et ne prennent pas suffisamment une vision globale de la résilience structurelle et organisationnelle de tous les acteurs, et manque d'objectifs chiffrés en termes de « résilience ».**

- **Un effort de normes et de spécifications reste à entreprendre pour le durcissement et l'approche « résilience » de ces réseaux au niveau national et européen.**


Électricité (Nuc+ENR)
HTM SeC GT Te IC In Ca Sé
Faible vulnérabilité
Vulnérabilité moyenne
Très forte vulnérabilité
Production
Distribution
Transport
Gestion télégérée et communication
Fonctionnement des infrastructures
Télécommunications
SeC GT Te HTM IC Sé Ca In
Faible vulnérabilité
Vulnérabilité moyenne
Très forte vulnérabilité
Supervision (administration,Data , etc.)
Datacenters
Réseaux et Transport numérique
Alimentation des infrastructures et signalisation
Télégestion et communication
Refroidissement des centrales et fonctionnement hydroélectrique
Fonctionnement des infrastructures
Communication avec les trains et gestion des signalisations
Gestion de signalisation et des systèmes d'informations
Transports
Dépendance géographique par les lignes a proximité des routes
Eau
Production
Distribution
Assainissement
Collecte
Ca HTM SeC
Faible vulnérabilité
Vulnérabilité moyenne
Très forte vulnérabilité
Refroidissement des datacenters
Alimentation électrique des trains
Risques extrêmes identifiés
In Inondation
HTM Hausse des températures moyennes
Ca Canicule
SeC Sécheresse
Sé Séisme
GT Glissement de terrain
Te Tempête / Vent violent
IC Incendie
Échelle de vulnérabilité
Faible interdépendance
Interdépendance moyenne
Forte interdépendance
Ferroviaire
Routier
IC HTM In Ca Sé GT
Faible vulnérabilité
Vulnérabilité moyenne
Très forte vulnérabilité
©Copyright HCFRN 2023

Annexes

Annexe 1 – Bibliographie

La stratégie de recherche d'informations a été double. Les équipes de veille du HCFRN ont entré plusieurs requêtes booléennes sur nos outils de recherche web pour optimiser les résultats. En parallèle, les mêmes requêtes ont été lancées sur Google Scholar pour rechercher plus spécifiquement les études, mémoires/thèses ou articles scientifiques. Elles ont, pour la plupart, été effectuées en français et en anglais. Le pôle veille a ensuite sélectionné "à la main" les documents les plus pertinents qui relevaient du périmètre considéré.

	A	B	C	D	E	F	G
1	Date	Pays	Source	Titre	Thématique	Sous-thématique	Synthèse
2	2005	Europe	Centre Européen de Prévention du risque innondation	Réduire la vulnérabilité des réseaux urbains aux inondations	réseaux	Inondation	Ce document souligne qu'il existe des outils afin de réduire la vulnérabilité des réseaux. Les premiers sont organisationnels par la mise en place de plans par les différents acteurs.Les seconds sont techniques, ce sont généralement les aménagements qui permettent de mettre les installations vulnérables ou sensibles hors d'eau ou encore des actions mise en oeuvre à la base permettant au réseau de résister au mieux possible. De plus, il est évoqué que lorsque la mise hors d'eau n'est pas possible, la prévision du risque permet néanmoins de réduire les risques et permettre la continuité du service. Enfin, le document conclu qu'il est important d'intégrer les gestionnaires de réseaux dans cette prévention au risque inondation, ces derniers pouvant protéger par la suite leurs propres réseaux. De plus, les associer à la gestion de crise améliore cette dernière.
3	2008	Canada	Gouvernement du Canada	La vulnérabilité des télécommunications mobiles face aux risques naturels	réseaux télécommunication	risque naturel	Le gouvernement du Canada a publié une étude sur la vulnérabilité des réseaux de télécommunication face aux risques naturels. Le rapport met en évidence l'absence de norme commune pour les réseaux municipaux ainsi qu'une faible priorité donnée au concept de "security by design". Un accent est également porté sur l'absence d'interopérabilité, facteur de vulnérabilité dans la conduite des opérations d'urgence.
4	2008	France	Ministère de la transition écologique	Catastrophes environnementalles : Préparer l'évaluation de leurs effets et le RETEX	risque naturel	territoire	Le Ministère de la Transition Écologique a rendu une étude sur les catastrophes NATEC (naturelles et technologiques) en se focalisant sur une analyse des conséquences et sur le retour d'expérience (RETEX). Le ministère dresse un constat assez pauvre en matière de RETEX sur les évènements non majeurs et surtout concernant des risques autres que l'inondation.
5	2012	Canada	École nationale d'administration publique (Québec)	LES DYNAMIQUES ET CARACTÉRISTIQUES INTERORGANISATIONNEL LES DANS UN RÉSEAU D'INFRASTRUCTURES ESSENTIELLES LEUR IMPACT SUR LA COORDINATION ET LA RÉSILIENCE	réseaux	résilience	Ce document de l'école nationale d'administration du Québec, analyse les impacts des organisations sur les infrastructures et leur résilience en temps de crise. Les résultats de la recherche indiquent qu'il existe certains écarts dans les dimensions internes et externes à la résilience au sein des types et des tailles d'organisations ainsi que des secteurs. Cette étude a pour but d'approfondir des réflexions portant sur les principales manières de surmonter les barrières à la résilience au sein des infrastructures essentielles.
6	2013	France	UNIVERSITÉ DE NICE-SOPHIA ANTIPOLIS	ESPACES À ENJEUX ET EFFETS DE RÉSEAUX DANS LES SYSTÈMES DE RISQUES	réseaux	risque naturel	Un doctorant a soutenu sa thèse sur la dépendance des territoires aux réseaux face aux aléas naturels. Il s'intéresse particulièrement aux questions d'interdépendance des réseaux, notamment de la place centrale du système éléctrique dans le fonctionnement et la continuité des autres réseaux. Il illustre ces problématiques par l'analyse de 3 études de cas appliquées à la ville de Marseille, le département du Var et la métropole de Barcelone.
7	2013	France	Institut national polytechnique de Toulouse	Aide à la décision pour l'analyse de la vulnérabilité des réseaux d'infrastructure face aux rises de catastrophes naturelles	réseaux	risque naturel	Un doctorant a présenté sa thèse à l'INP de Toulouse sur la vulnérabilité des réseaux d'infrastructure face aux catastrophes naturelles. Cette thèse a pour ambition d'analyser les impacts sur la population que pose la défaillance des infrastructures - en temps de crise - face aux risques naturels. Elle accorde une importance particulière sur la notion d'interdépendance des réseaux et se propose d'apporter des outils d'analyse pour favoriser la prise de décision.
8	2013	France	EchoGéo (PJ)	Retour critique sur la mobilisation du concept de résilience en lien avec l'adaptation des systèmes urbains au changement climatique	réseaux	changement climatique	Ce document traite du sujet de la résilience des infrastructures face au réchauffement climatique. Le document souligne des problèmes d'opérationnalisation du concept de résilience afin de traiter des risques urbains liés au changement climatique. Le concept de résilience n'est pas jugé assez opérationnel de par sa polysémie et son interprétation ambiguë. Il est souligné l'ambiguïté entre résilience et vulnérabilité notamment.
9	2013	France	École polytechnique de l'université de Tours	UNE DEMARCHE DE GESTION DU RISQUE D'INONDATION : LE PLAN COMMUNAL DE SAUVEGARDE VERS UNE RESILIENCE URBAINE ?	inondation	résilience	L'école polytechnique a mené une étude liant la gestion du risque inondation et la résilience urbaine et se concentrant sur la ville de Nantes. L'étude de cas vise à déterminer si le plan communal de sauvegarde inclut le risque inondation dans les projets d'aménagement urbain.
10	2013	France	UNIVERSITÉ DE NICE-SOPHIA ANTIPOLIS (PJ)	Espaces à enjeux et effets de réseaux dans les systèmes de risques : Région Provence-Alpes-Côte d'Azur, Département du Var, Métropole de Marseille et Métropole de Barcelone	réseaux	risque naturel	Les systèmes prévus pour l'anticipation et la détection des risques sont imprécis, ce qui rend la protection des réseaux d'énergie, de télécommunication, d'assainissement incertaine. La modélisation des systèmes de risques et des zones vulnérables aux aléas climatiques devrait permettre de réduire les risques pesant sur les réseaux qui sont interconnectés et sur lesquels reposent le fonctionnement d'autres secteurs.
11	2014	France	OCDE	Étude de l'OCDE sur la gestion des risques d'inondation : la Seine en Île-de-France	inondation	territoire	Cette étude de l'OCDE se concentre sur la gestion du risque inondation en Ile-de-France en cas de crue majeure de la Seine. La vulnérabilité des réseaux a été exacerbée par l'augmentation de l'urbanisation ainsi que la l'interdépendance des systèmes critiques. Une inondation dans la région aurait des impacts humains, économiques et sociaux. Le fonctionnement des entreprises et des institutions serait aussi affecté.
12	2015	France	Conseil général de l'environnement et du développement durable	Résilience des réseaux dans le champ du MEDDE à l'égard des risques	réseaux	risque naturel	Le Ministère de la Transition Écologique a publié une étude sur la résilience des réseaux face aux risques naturels, faisant suite à un précédent rapport de septembre 2013. Le présent rapport alerte sur le peu d'étude portée sur le rétablissement des réseaux post-crises (RETEX) ainsi que sur l'absence de coordination structurelle entre les différents opérateurs de réseaux.
13	2015	France	École des ingénieurs de la ville de Paris (PJ)	Impact des inondations sur les infrastructures et reseaux techniques et solutions d'amelioration de la resilience des systemes urbains	réseaux	Inondation	Cette étude de l'école des ingénieurs de la ville de Paris analyse cinq grandes villes qui ont vécu des inondations majeures afin d'en discerner les systèmes de défense les plus adéquats selon le niveau de l'inondation (limite, coûts et densité d'occupation au sol). L'étude permet de mieux déterminer la solution adéquate à chaque type d'inondation ainsi que son échelle d'application.
14	2016	Europe	Centre européen de prévention du risque inondation	Le territoire et ses réseaux techniques face au risque d'inondation	réseaux	Inondation	Le CEPRI a réalisé un guide sur la vulnérabilité des réseaux au regard de l'aléa inondation. Il souligne le rôle des gestionnaires de réseaux en cas de défaillance voire de crise majeure ; mais également les contraintes et difficultés identifiées. Le constat indique des problématiques techniques et financières sur l'adaptation des infrastructures face au risque d'inondation.
15	2016	France	École des Mines de Saint-Étienne (en PJ)	Vulnérabilité, résilience et effets cascade entre réseaux techniques : apports de la modélisation systémique et spatiale pour la planification et la gestion de crise au profit des opérateurs de réseau et de la sécurité civile	réseaux	risque naturel	Les réseaux que ce soit d'eau, d'énergie, de transports ou encore de télécommunications sont interdépendants. Par conséquent, une vulnérabilité sur un réseau cause des effets en cascade sur les autres réseaux. Gérer ces effets sont essentiels pour des processus décisionnels et une gestion de crise plus efficaces.
16	2016	Europe	Organization for Security and Co-operation in Europe	Protecting Electricity Networks from Natural Hazards	réseaux énergie	risque naturel	Ce manuel vise à améliorer la résilience des infrastructures électriques vitales face aux risques naturels. Pour empêcher des blackouts qui peuvent avoir des impacts conséquents sur la société, il est nécessaire qu'il y ait une coopération renforcée entre les acteurs clés du secteur.

	A	B	C	D	E	F	G
1	Date	Pays	Source	Titre	Thématique	Sous-thématique	Synthèse
17	2016	France	Sciences eaux et territoires (PJ)	Risque, vulnérabilité, résilience : quels apports pour la gestion patrimoniale des ouvrages de protection et des réseaux urbains?	réseaux	risque naturel	Cet article a pour ambition d'améliorer la défintion de la gestion patrimoniale d'infrastructures par les notions de risque, résilience ainsi que vulnérabilité. Cet article permet de différencier des catégories d'infrastructures ainsi que leur vulnérabilité. Quant à la gestion de crise, celle-ci est aussi notifiée comme importante et il est nécessaire de pratiquer des exercices mobilisant l'ensemble des acteurs afin de formaliser les fonctions d'entrée et de sortie du système et de vérifier les bonnes procédures à adopter. Enfin, il est affirmé que la gestion patrimoniale d'infrastructure contribue à la préparation/l'anticipation des défaillances de l'infrastructure, la résilience renvoie quant à elle au fonctionnement en cas de phénomènes plus exceptionnels. Les auteurs préconisent également une évolution vers une GPI intégrée au sein du territoire et élargie à toutes les organisations en charge de leur gestion et à leurs usagers.
18	2016	États-Unis	Argonne National Laboratory / US Department of Energy	Front-Line Resilience Perspectives: The Electric Grid	réseaux énergie	risque naturel	Ce document du laboratoire national Argonne aborde la question de la résilience du réseau électrique aux Etats-Unis. Il met en avant les capacités du système américain à anticiper, resister, absorber, répondre et s'adapter aux incidents. Il souligne également l'importance de l'Etat et des compagnies dans cette résilience. Ce document identifie plusieurs risques majeurs: les séismes, l'augmentation des températures, les tempêtes, submersions, orages, tempête de neige et grand froid. Face à ces risques, il est soutenu que des mesures de sécurité, de maintenance, de modernisation, de diversification du réseau, de redondance, et d'aides afin d'améliorer la résilience du réseau électrique.
19	2016	Canada	Canadian Electricity Association	ADAPTATION AUX CHANGEMENTS CLIMATIQUES : BILAN DE LA SITUATION ET RECOMMANDATIONS POUR LE SECTEUR DE L'ÉLECTRICITÉ AU CANADA	réseaux énergie	changement climatique	Les réseaux électriques sont vulnérables aux risques climatiques. Ces derniers doivent être mieux pris en compte par les compagnies d'électricité pour améliorer la gestion des risques. Pour garantir l'adaptation des infrastructures aux scénarios climatique, tous les acteurs concernés : les compagnies d'électricité, les exploitants de réseau, les organismes de réglementation et les clients doivent participer à la mise en place d'une gouvernance adaptée.
20	2017	États-Unis	Johns Hopkins University School of Advanced International Studies	The risks of climate and natural disaster related disruption to the electric grid	réseaux énergie	changement climatique	L'université américaine Johns Hopkins a réalisé une étude sur la vulnérabilité du système électrique à l'aune du changement climatique, en attachant une attention particulière aux risques météorologiques. Une approche systématique a été utilisé pour identifier la vulnérabilité intrinsèque du système électrique face aux différents aléas identifiés. La question d'interdépendance des réseaux est également traité à travers un prisme centré sur les connexions du réseau électrique avec les autres réseaux comme celui de l'eau ou du gaz.
21	2017	Europe	Commission européenne	Power grid reovery after natural hazard impact	réseaux énergie	risque naturel	Ce rapport démontre que les réseaux d'électricité sont affectés de façon différente selon le risque naturel. A titre d'exemple, les inondations sont souvent responsable des black-out tandis que les tremblements de terre causent des dommages aux équipements des infrastructures énergétiques. La résilience de ces réseaux est impérative pour limiter les dégradations causées par ces aléas climatiques. Il est donc nécessaire de prévoir les outils qui permettent de se préparer et d'anticiper ces risques ainsi que d'établir des processus pour les réparations sur le moyen et long terme.
22	2017	France	Université Bretagne Loire (PJ)	La résilience des territoires littoraux face au risque de submersion marine. Application sur les territoires de la Charente-Maritime et de la Somme	inondation	territoire	Cette thèse de 2017 soulève le problème de la la vulnérabilité des territoires de la Charente-Maritime et de de la Somme ainsi que leur résilience face au risque de submersion marine. Le document met en avant que la résilience est facteur de l'expérience des territoires. Un organisme et un territoire qui ont déjà été impacté ou ont été impactés plusieurs fois seront plus à même d'être résilient face au risque. Il a également été soulevé que les données concernant le risque de submersion étaient plus abondantes sur un territoire qui a été touché par le risque. Enfin, un territoire impacté par un phénomène de submersion est résilient grâce à la reprise de l'activité économique sur place. La thèse mentionne également des difficultés pour les acteurs à gérer cet événement ainsi que leur manque d'anticipation, de réactivité, de connaissances des mesures post-crise et de réduction de la vulnérabilité. Cette thèse soulève que les acteurs les plus résilients sont les professionnels de la gestion de crise qui en ont une expérience récente. Quant aux moins résilients ce sont les organismes qui n'ont pas d'intérêt porté au risque submersion ou d'expérience passée en lien avec ce risque
23	2017	France	Ministère de la transition écologique	La résilience des territoires aux catastrophes	réseaux	risque naturel	Le texte, se basant sur l'étude d'événements climatiques, veut dresser différents leviers pour promouvoir et développer la résilience au sein des institutions, et notamment les collectivités territoriales, mais également la population. À ce titre, elle identifie 4 leviers : l'articulation grâce aux projets de territoire, la mise en relation des acteurs, l'anticipation et la veille et les capacités d'agir. Chaque levier détaillant un certain nombre d'actions.
24	2018	France	Caisse centrale de réassurance	Les catastopohes naturelles en France	risque naturel	territoire	La CCR a réalisé une étude sur le bilan des catastrophes naturelles en France entre 1982 et 2017. Cette dernière présente des chiffres sur la sinistralité des risques naturels et expose les enjeux de ces aléas sur le territoire.
25	2018	France	Institut méditerranéen du risque, de l''environnement et du développement durable	La résilience urbaine face aux risques, en contexte de changement climatique	réseaux	changement climatique	Ce rapport de Février 2018 vise a présenter les approches de résilience existantes ainsi que leurs problèmes de mise en pratique dans les politiques publiques. Par la suite, le rapport tentera de déterminer des actions afin de rendre l'application du concept de résilience possible. Le document soulève le problème de la non-prise en compte des temporalités longue et courte pour aborder la résilience territoriale dans la plupart des études. Egalement, il a été soulevé un problème concernant la contradiction entre l'approche technique et sociale de la résilience des territoires. En effet, parfois, la résilience infrastructurelle joue défavorablement sur la résilience sociétale.
26	2018	France	Vertigo	Infrastructures critiques, vulnérabilisation du territoire et résilience : assainissement et inondations majeures en Île-de-France	réseaux	Inondation	Cette étude réalisée par deux géographes aborde la question centrale de la vulnérabilité du réseau d'assainissement en cas de crue en Île de France. Ce document affirme que la sortie de crise et le redémarrage constituent un risque systémique en cas de crue. Dans ce cadre, l'importance d'identifier les noeuds critiques qui facilitent la récupération ou l'entrave pour les gestionnaires est soulignée. Est également mentionné la possibilité de 'build back better' par la fenêtre d'opportunité qu'offre le post-catastrophe. Les auteurs mentionnent que ce BBB peut entrer en contradiction avec la résilience et que les stratégies d'adaptation préventives intégrées aux politiques d'aménagement du territoire, notamment dans le cadre des opérations de renouvellement urbain, semblent pour l'instant préférables.
27	2018	Monde	PS-eau	Les services d'eau et d'assainissement face au changement climatique: Quels impacts ? Comment agir ?	réseaux eau	changement climatique	Les aléas climatiques ont compliqué la continuité des services d'eau et d'assainissement. En effet, les sécheresses ainsi que les évènements climatiques extrêmes menacent l'accessibilité et la qualité des ressources en eau. Les infrastructures, équipements et fonctionnement des services d'eau et d'assainissement sont donc vulnérables au changement climatique.
28	2019	France	Agence nationale de la recherche	RISQUES ET CATASTROPHES NATURELS	risque naturel	territoire	De 2010 à 2018, l'Agence Nationale de Recherche a financé 105 projets sur la thématique des risques naturels. Ce rapport entend, après avoir donné au lecteur les clés de lecture et les éléments de définition, présenter une discussion approfondie sur l'apport de ces projets à la connaissance des risques naturels. L'objectif est non seulement de mieux comprendre les aléas mais également les mesures qui peuvent être mises en place pour limiter le risque dans un premier temps et y faire face lorsque la crise survient dans un second temps.

	A	B	C	D	E	F	G
1	Date	Pays	Source	Titre	Thématique	Sous-thématique	Synthèse
29	2019	France	Revue de géographie de Bordeaux (PJ)	Dérèglement climatique et gestion des risques en Polynésie française : conception d'un Observatoire de la résilience	résilience	territoire	Ce document a été réalisé par deux professeurs spécialiste en risque climatique et résilience. Cette étude aborde la question du dérèglement climatique sur le territoire de la Polynésie Française. Il met en avant que le concept de résilience permet de réduire largement les risques, mais celui-ci est très peu pris en compte aujourd'hui. Les auteurs défendent l'importance de la résilience bien qu'elle subit quelques faiblesses notamment de par ses objectifs qui sont mal définis. Ils soutiennent que la résilience doit s'adapter à l'approche systémique d'un territoire afin de prendre en compte toute la complexité de ses dynamiques spatiales et sociales. Ils mettent également en avant que les territories français d'Outre mer sont très concernés par le risque de crues subites mais que celui-ci est mal traité localement et nationalement alors que de nombreux facteurs (géographie, climat, contraintes d'aménagement…) augmentent la vulnérabilité de ces territoires aux crues. De plus, un mauvais ou difficile partage des responsabilités entre les autorités nationales et locales complexifie cette gestion du risque. Selon les auteurs de l'étude , la création d'un observatoire permettra de répondre aux besoins en termes d'avancées scientifiques, techniques, sociales et territoriales, permettant de répondre à un besoin évalué par une solution qui n'existe pas encore en utilisant au maximum les des données et solutions open source, minimisant les coûts.
30	2019	États-Unis	US Department of Energy	Extreme Weather and Climate Vulnerabilities of the Electric Grid: A Summary of Environmental Sensitivity Quantification Methods	réseaux énergie	risque naturel	Le département de l'énergie américain a commandé une étude sur les risques que font peser les catastrophes naturelles sur le réseau électrique national. Ce rapport met en avant que les tempêtes (pluie, vent et neige) ainsi que le gel sont les risques rendant le réseau américain le plus vulnérable. Il est également souligné que l'augmentation de sévérité des évènements extrêmes est une explication de l'augmentation des coupures de courant aux Etats-Unis.
31	2019	France	Presses universitaires de la Méditerranée (PJ)	Retours d'expériences post-catastrophes naturelle	inondation	résilience	Ce document est une compilation de cinq retours d'expérience ainsi que d'articles scientifiques concernant le risque inondation. Cet éditorial a pour but d'exposer l'importance de la prise en compte des RETEX dans la gestion du risque et la mise en place de stratégie de résilience. Ces RETEX permettent d'exposer les enjeux du risque inondation sur les territoires ainsi qu'à aider à la réflexion sur la prévention de ce risque et la mise en place d'outils pour améliorer la continuité des réseaux en cas de crises liées à l'aléa inondation. Il est avancé que la culture du risque, la mise en place d'organismes et de moyens de protection ainsi que de prévention permettent de diminuer le risque.
32	2020	France	Hydroscience journal	Vers une meilleure prise en compte des défaillances en cascade au sein des réseaux franciliens interdépendants face aux crues majeures	réseaux	Inondation	Cet article de recherche publié en 2020 explore les risques pour les réseaux techniques franciliens en cas de crue majeure de la Seine. Dû à l'interdépendance des réseaux en Ile-de-France, il est essentiel d'établir un système d'identification des crues afin d'éviter les défaillances en cascade. Une cartographie des fragilités des réseaux est une des solutions proposées pour contribuer à la gestion du risque.
33	2020	France	Revue européenne de géographie	Le système d'assainissement en Ile-de-France : entre ressource et facteur aggravant pour la gestion d'une inondation majeure	réseaux eau	Inondation	Cet article démontre que les réseaux d'assainissement en Ile-de-France sont vulnérables au risque inondation de la Seine et/ou de la Marne. Les dimensions technique, sociale et territoriale des réseaux contribuent à cette vulnérabilité. En particulier en Ile-de-France, la gestion partagée entre plusieurs acteurs exacerbe la complexité du réseau et de sa gestion en cas de crise.
34	2020	Outre-Mer	Université polynésie française	La résilience urbaine en question : Enjeux, contexte et propositions d'opérationnalisation	résilience	territoire	Cet article se concentre sur le rôle de la résilience dans la gestion des risques. Le concept de résilience a été démocratisé ce qui a conduit à une multiplication des interprétations. Cette diversité des approches complique l'opérationnalisation du concept. Des nouveaux outils tels que des méthodes de mesure de la résilience ou des systèmes d'aide à la décision spatiale permettent de combler ces limitations.
35	2021	France	Presses universitaires de la méditerranée	Résilience et adaptation aux risques « naturels »	résilience	territoire	Cette étude de 2021 aborde la question de la prévention ainsi que de la protection des populations face aux risques naturels. Il est mis en avant que les objets connectés permettent une meilleure alerte de la population de par leur ciblage précis, leur rapidité et leur portée. Il est mentionné que ces moyens sont bien plus efficaces que les moyens traditionnels d'alerte. Dans un soucis d'efficacité, il est important que le système soit uniformisé à l'échelle nationale afin de ne pas multiplier les interfaces et enchevêtrements. Cependant, les système traditionnels ne doivent pas être laissés de coté, la multiplicité des moyens d'alerte garantie la robustesse des systèmes mais aussi d'augmenter la population « alertable ».
36	2021	États-Unis	United States Government Accountability Office	ELECTRICITY GRID RESILIENCE: Climate Change Is Expected to Have Far-reaching Effects and DOE and FERC Should Take Actions	réseaux énergie	changement climatique	Le bureau de la responsabilité gouvernementale des Etats-Unis a publié un rapport en 2021 sur la résilience du réseau électrique. Tous les aspects du réseau tels que la production ou la distribution d'électricité seront impactés par le changement climatique. Les dommages aux infrastructures pourront coûter des millards de dollars aux services publics et aux clients.
37	2021	Canada	HEC Montréal	Les modèles de pôles de résilience climatique et communautaire, à l'échelle nationale et internationale	résilience	territoire	Ce rapport de l'université HEC Montréal explore des modèles de pôles de résilience urbaine à travers des initiatives nationales et internationales. Les systèmes de bonnes pratiques étudiés permettent de combiner plusieurs systèmes et de les adapter au contexte donné. Ainsi, il est possible de créer un modèle pertinent et ajustable à la localité choisie. Ce modèle peut ensuite être utilisé pour réaliser une analyse d'impact de l'écosystème montréalais par exemple.
38	2021	Canada	International Institute for sustainable development	Renforcer la résilience climatique des infrastructures canadiennes : UNE REVUE DE LA LITTÉRATURE POUR ÉCLAIRER LA VOIE À SUIVRE	réseaux	changement climatique	L'Institut international du développement durable a publié un rapport en 2021 sur la résilience climatique des infrastructures bâties canadiennes. Ce rapport offre un panorama sur les solutions d'adaptation de ces infrastructures aux risques naturels. Selon le rapport, la résilience des infrastructures et des collectivités passe aussi par des investissements dans les infrastructures naturelles.
39	2021	USA	DEPARTMENT OF HOMELAND SECURITY	Climate Action Plan	résilience	changement climatique	Ce rapport détaille comment les Etats-Unis comptent construire des sociétés résilientes au changement climatique. Plusieurs réformes et stratégies y sont exposées, précisant comment le pays prévoit de lutter contre les risques naturels tels que les inondations, les feux de forêts, les sécheresses... De plus, les Etats-Unis ont établi un plan pour préparer leur transition énergétique, notamment en renforçant la production industrielle d'énergie propre.
40	2021	USA	FEMA	Resources for Climate Resilience	résilience	changement climatique	Ce rapport fourni une feuille de route pour préparer les nations à développer des techniques de résilience face aux risques climatiques. Ce rapport condense plusieurs programmes pour renforcer les stratégies nationales prévues pour atténuer les risques et effets des évènements climatiques. De plus, les outils disponibles tels que le l'indice de risque national par exemple ainsi que les possibles financements sont précisés pour chaque programme.
41	2022	Chine	Computer networks	Construction of network topology and geographical vulnerability for telecommunication network	réseaux télécommunication	risque naturel	Cette étude réalisée par des étudiants tend à déterminer la vulnérabilité des réseaux de télécommunication aux risques naturels et technologiques. Pour se faire les étudiants auteurs de l'étude tentent de mettre au point des facteurs de vulnérabilités tels que la topologie de la zone, la longueur du réseau, le type de réseau etc. Afin de construire des modèles de probabilité de mise en échec du systèmeafin de prévoir au mieux leur vulnérabilité.
42	2022	Europe	SELF congresses (PJ)	Prévenir et gérer le risque de black-out électrique à l'échelle d'une région : représentations et pratiques d'acteurs institutionnels et privés	réseaux énergie	territoire	Le risque de black-out électrique a été étudié lors du congrès SELF de 2022. Les enjeux de résilience ont été abordés pour définir une stratégie empêchant ou limitant les effets d'un blackout. En effet, un blackout prolongé peut entrainer des conséquences majeures dans d'autres secteurs tels que les transports, l'approvisionnement en eau, les soins médicaux…

	A	B	C	D	E	F	G
1	Date	Pays	Source	Titre	Thématique	Sous-thématique	Synthèse
43	2022	France	Physio-Géo	Leçons tirées de la crue torrentielle catastrophique du 2 octobre 2020 dans la vallée de la Vésubie (Alpes-Maritimes, France)	réseaux	Inondation	Cet article de 2022 utilise le RETEX de la crue torrentielle dans les Alpes-Maritimes de 2020. Les réseaux stratégiques sont exposés au risque inondation ainsi qu'aux mouvements de terrain. Les zones montagneuses ne sont pas adaptées pour le développement d'activités critiques. Ces dernières restent vulnérables aux évènements météorologiques extrêmes dans la bande active de la Vésubie.
44	2022	France	France Stratégie	Risques climatiques, réseaux et interdépendances : le temps d'agir	réseaux	changement climatique	L'agence France Stratégie a publié une note sur la vulnérabilité des réseaux face aux changements climatiques, avec une attention particulière sur la notion d'interdépendance. Le rapport indique par exemple l'importance du critère géographique dans la vulnérablité des réseaux électriques et de télécommunications. Pour cela, il dresse un bilan structuré en 3 axes : Assurer des références partagées ; Mettre en place une gouvernance nationale ; Asseoir la vision nationale sur des démarches territorialisées.
45	2022	USA	FEMA	Mitigation Action Portfolio	résilience	risque naturel	Ce rapport traite de la résilience face aux risques naturels tels que les inondations, ouragans, sécheresses et incendies. Le but est d'éviter une gestion postérieure aux évènempents climatiques et de passer à une préparation en amont des désastres naturels pour prévenir et limiter les risques et dégâts. De plus, ce rapport fournit un cadre pour mettre en place des stratégies afin d'atténuer les dommages causés.
46	2022	USA	FEMA	NATIONAL PREPAREDNESS REPORT	résilience	risque naturel	Ce rapport vise à établir une gestion de crise pour les risques naturels. Ces derniers évoluant rapidement avec le changement climatique, il est essentiel que les pays s'adaptent pour disposer d'une préparation nationale ainsi que d'un pays résilient. Des investissements ciblés ainsi que des techniques permettant la prédiction des risques futures et l'analyse des données d'évènements climatiques précedents sont des éléments clés pour créer des stratégies effectives.
47	2022	USA	DEPARTMENT OF HOMELAND SECURITY	2022 Department of Homeland Security Sustainability Plan	résilience	changement climatique	Ce document tient compte de la stratégie adoptée par les Etats-Unis pour atteindre la neutralité carbone et renforcer la résilience de leur société. Ce document établit une feuille de route afin de prioriser les actions nécessaires pour consolider sa résilience tout en respectant ses engagements de réduction de gaz à effet de serre. Ainsi, le DHS vise à se positionner comme un leader dans la gestion des risques climatiques/ environnementaux.
48	2023	Monde	Earth-Science Reviews	Climate change hotspots and implications for the global subsea telecommunications network	réseaux télécommunication	changement climatique	Cette étude réalisée par des scientifiques et universitaires anglais et américains spécialisés dans le domaine marin aborde la question des effets du changement climatique sur les infrastructures critiques de télécommunications sous-marines comme les cables sous-marins. Les conclusions des chercheurs sont que les conditions des océans vont grandement changer, mais que cela sera très différent à l'échelle locale. Dès lors les futurs emplacements des cables sous-marins et infrastructures de communication devront être sélectionnés précautionneusement au regard des conditions locales tout en prenant en compte les possibles changements futur liés au changement climatique. Dans cette étude onze risques liés au changement climatique et à leur potentiel impact sur les réseaux de télécommunications sous-marins sont mentionnés: Montée du niveau de la mer, marées de tempête, cyclones tropicaux et extratropicaux, érosion côtière et régime de transport des sédiments du fond marin courants océaniques, météo au large, inondation de rivière, glissements de terrain sous-marins, glace de mer arctique et icebergs, déplacement des zones de pêche en raison de l'évolution de l'océan et nouvelles routes maritimes en raison des conditions changeantes.

Annexe 2 – Résultats des questionnaires des opérateurs

Dans le cadre de l'étude, 8 opérateurs ont été interrogés et 5 ont répondu. Ils ont été sélectionnés pour leur importance en tant que services essentiels dans la vie de la nation, et pour lesquels la continuité d'activité de ces services, malgré les événements générés par le changement climatique, est donc primordiale. Les opérateurs interviewés sont les suivants : Électricité de France (EDF), Réseau de Transport d'Électricité (RTE), ENEDIS, GRTGaz, VEOLIA, Total, SNCF et Suez.

Par leurs activités et leur importance, ces opérateurs sont soumis pour la plupart au régime juridique des "Secteurs d'activités d'importances vitales". Ce régime les oblige à assurer un niveau élevé de protection des infrastructures, mais aussi de continuité d'activité et de services.

Nous les avons interrogés, dans un premier temps (Chapitre 1) sur leurs positionnements dans l'écosystème des opérateurs en termes d'interdépendances et sur leurs niveaux de préparation face aux risques et aux menaces. Dans un second temps, nous nous sommes renseignés sur leur niveau de connaissance des vulnérabilités de leurs réseaux par rapport aux autres opérateurs (Chapitre 2). Enfin, dans un troisième temps, nous avons interrogé leur niveau d'organisation interne en cas de survenue d'une crise (Chapitre 3).

L'ensemble de ces questions ont pour objectif d'identifier leur capacité de résilience et de continuité de service en cas d'événement impactant leur propre activité.

Les premières questions se concentrent sur l'aspect technique et l'appréhension des risques amenés par le changement climatique.

I. Résilience structurelle

Nous constatons que la notion de résilience structurelle en elle-même n'est pas spécifiquement connue ou interrogée par toutes les organisations : 40% des

répondants indiquent ne pas la connaître. Les mesures prises dans ce cadre existent néanmoins, mais elles sont en revanche disparates selon les répondants.

En effet, 80% des répondants affirment que si le rapport du GIEC a été pris en compte dans l'analyse des risques, cela n'a pas affecté leur planification.

En revanche, les organisations ont mis en place des actions pour essayer néanmoins d'adapter les infrastructures, processus et matériaux aux défis de demain. Cela se traduit notamment par des investissements intégrant le renforcement de la résilience des réseaux ou encore l'ajout de capteurs plus performants.

Ces investissements, ou l'éventuel remplacement d'infrastructures ont fait l'objet d'un budget spécifique dans 60% des cas.

Nous pouvons supposer que ces opérateurs ont d'ores et déjà anticipé les investissements et les actions nécessaires pour adapter leurs infrastructures aux effets du changement climatique, mais la question demeure de savoir à quelle vitesse et avec quelle synchronisation avec les autres opérateurs en vue d'optimiser la transition et la sécurité des réseaux et des services. Or là, il ne semble pas avoir de « cadre général » pour un tel travail, chaque opérateur travaillant individuellement sa feuille de route de la transition climatique, cela peut poser un problème de cohérence et de fragilité de l'ensemble de l'écosystème « critique ».

Nous avons par la suite interrogé le positionnement de leur entreprise dans l'écosystème des opérateurs de réseaux, en les interrogeant dans un premier temps sur la cartographie d'interdépendance avec les autres réseaux. Seulement un répondant sur les 5 a affirmé qu'il disposait d'une telle cartographie.

En revanche, 80% des répondants travaillent avec les opérateurs en charge des autres réseaux, ce travail se traduisant par un partage d'information sur les vulnérabilités des réseaux, le partage d'un annuaire de crise, ou encore des exercices en commun. Les analyses de risques, données sensibles, restent en interne.

Vient enfin la question des exercices, notamment, incluant une interruption des réseaux liée à une catastrophe naturelle. 60% des répondants jouent cet exercice de manière périodique tout en prévoyant une panne émanant d'un autre réseau. En revanche, les pourcentages s'inversent concernant le scénario du "cygne noir" (avec par exemple plus d'internet, plus d'énergie électrique, des transports perturbés) où seulement 40% des répondants prévoient ce type de scénario dans leur planification.

Enfin, d'un point de vue réglementaire, 100% des répondants ont déclaré avoir pris connaissance des évolutions apportées par la directive Résilience des Entités Critiques et prennent en compte, dans leur analyse de risques, les risques naturels et technologiques majeurs pour évaluer leur résilience et leur continuité d'activité, en accord avec la législation d'importance vitale. Néanmoins il est difficile d'évaluer concrètement cette prise en compte, faute d'indicateurs.

II. Maturité et positionnement

L'ensemble des opérateurs a déclaré avoir procédé à une analyse et une identification des risques, aussi bien chroniques qu'extrêmes. Si cet aspect est plutôt normal pour des organisations de cette importance, il est intéressant de se concentrer sur les risques qui ont été le plus identifiés. Les effets du changement climatique semblent être pris en compte, car les notions de "Canicule", "Sécheresse", "Incendie", "Inondation" et "Tempête" sont les plus évoquées. Ces résultats correspondent aux risques identifiés lors de cette étude.

Les risques tels que le séisme ou le retrait d'argile sont moins représentés, on peut l'expliquer par le fait qu'ils répondent à des positionnements géographiques précis tandis que les risques évoqués précédemment peuvent toucher peu ou prou tout le territoire national.

Face à cette augmentation des risques, nous avons interrogé les opérateurs sur le travail réalisé directement sur les réseaux. Ce travail commence dans un premier temps par une étude des vulnérabilités à ces nouveaux risques. Excepté un opérateur, tous les

autres ont étudié et identifié la vulnérabilité de leurs réseaux face aux risques auxquels ils sont ou seront confrontés. À partir de cette identification, ils ont été en mesure de déterminer, voire de tester pour certains, la robustesse de ces réseaux face à ces risques.

Cependant, lorsque nous les interrogeons sur la valeur de référence à partir de laquelle leurs réseaux fonctionnent en mode dégradé ou deviennent inopérants, **seulement 50% sont en mesure d'affirmer que ces valeurs sont identifiées**. En revanche, il nous a été indiqué que malgré la difficulté de déterminer un seuil précis, ils étaient équipés d'un système et d'outils d'alertes adaptés aux risques auxquels ils sont exposés.

Deux répondants sont en mesure d'identifier les valeurs de références suivantes :

	Température de dysfonctionnement	Durée avant les premiers dysfonctionnements	Vitesse de vent obligeant le mode dégradé	Mètres cubes d'eau obligeant le mode dégradé ??)
Enedis	45°-50°C	6h	120km/h	1m3
Répondant 2	45°-50°C	12h	NR	1m3

En revanche, l'ensemble des réseaux sont maillés afin d'avoir une solution de secours en cas de dysfonctionnement rendant une partie du réseau inopérant, sauf parfois certaines zones géographiques plus enclavées, où ces maillages sont plus réduits.

L'année 2022, au travers des périodes de fortes chaleurs, a été un premier moment charnière pour tester et comprendre la robustesse des dispositifs. La majorité des répondants n'a pas vu sa continuité d'activité mise à mal par ces périodes. Suez nous fait part de difficultés liées à des incidents dans les réseaux souterrains en période de canicule. Ces dernières ont fait l'objet d'un retour d'expérience.

Pour les années à venir, les avis émanant du 6e rapport du GIEC semblent avoir été pris en compte pour adapter et orienter l'évaluation des risques.

Au travers des questionnaires, les opérateurs témoignent d'une politique volontariste dans la prévention des risques. De plus, cette dernière est connectée aux évolutions contemporaines et s'adapte au changement climatique. Nous avons ensuite cherché à comprendre si l'organisation est en mesure de réagir en cas de survenance de ces aléas.

I. Résilience organisationnelle

Si tous les opérateurs disposent d'une direction chargée de l'évaluation des risques, généralement nommée "Direction des risques et de la compliance", ils ne sont que 2 à avoir au sein de cette direction un groupe de travail dédié spécifiquement aux risques pesant sur les infrastructures.

L'ensemble des répondants ont inclus dans leur plan de continuité d'activité une crise émanant d'un autre réseau (perte d'activité électrique ou des télécommunications par exemple).

Lorsque l'aléa survient, la majorité des opérateurs ont un service dédié à la gestion de crise dont l'organisation est structurée. C'est-à-dire avec du personnel formé, une organisation précise et qui s'exerce régulièrement, une chaîne logistique opérationnelle.

Nous avons ensuite interrogé la capacité des organisations à pallier une panne du réseau électrique ou de télécommunications alimentant ses structures de gestion de crise. Si toutes les Hypervisions et SCADA essentiels sont secourus par un groupe électrogène, c'est la durée d'autonomie de ce dernier qui va varier, allant de moins de 12h à plus de 48h. La majorité des répondants se trouvent cependant dans une fenêtre de 2h à 36h. Les résultats sont les mêmes quant aux moyens déployés pour secourir en énergie le centre de crise.

Les autonomies sont décidées en fonction de la criticité des sites et des risques auxquels ils sont exposés. Concernant les télécommunications, la majorité des centres

ont une redondance des lignes entre un accès terrestre (Fibre ou ADSL) et un accès satellite. Certains centres ont un secours via des clés 4G/5G ou des radios, mais ils sont minoritaires.

Si les centres de crises sont secourus au niveau électrique, ce n'est pas le cas de tous les services essentiels de l'organisation. En effet, 50% des répondants ont prévu un groupe électrogène, dont la durée d'action est supérieure à 48h, pour leurs services critiques, tandis que les autres (50 %) n'ont pas prévu de solution de secours d'énergie à leur centre de crise.

La question logistique est essentielle en temps de crise, il est donc nécessaire de s'assurer que la chaîne de valeur (supply chain) puisse assurer le maintien en condition opérationnelle des réseaux face à des perturbations majeures.

À ce sujet, seulement 60% des répondants estiment que leur « supply chain » est en mesure d'assurer la fourniture de pièces pour assurer au moins une fonctionnalité minimale de leur réseau. Cette réponse est souvent motivée par un stock important de pièces pour l'ensemble des répondants, souvent secouru par une multitude de fournisseurs. En parallèle, d'un point de vue ressource humaine, des plans de montée en puissance des effectifs sont prévus pour remettre en état les réseaux, souvent par solidarité géographique.

Si les entreprises sont majoritairement préparées aux risques et aux événements, on ne peut que constater que les niveaux de préparation diffèrent assez largement d'une organisation à une autre.

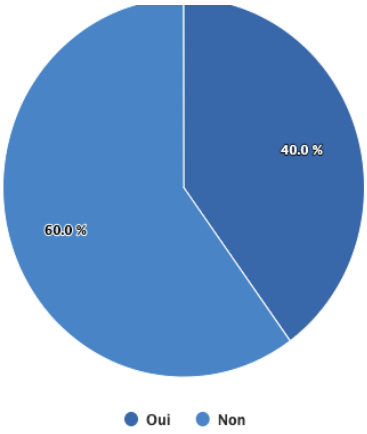
Nous avons souhaité par la suite interroger l'aspect structurel de la résilience. Nous entendons par « résilience structurelle » une *"réduction des vulnérabilités sur le moyen et long terme tel que, l'adaptation au changement climatique, l'adaptation des bâtiments et des réseaux et infrastructures aux aléas et menaces en anticipation d'un évènement, majeur, ainsi que des approches en matière de résilience économique pour l'opérateur affecté (assurances, aides, niveau de capitalisation et de fonds propres – à l'instar des banques et de la réglementation européenne DORA)* .

Si les sujets de réduction de vulnérabilité et d'adaptation au changement climatique sont indéniablement à l'agenda des grands opérateurs, le degré d'investissement et le lien avec le concept de résilience dans le sens ne semblent pas directement corrélés. La politique de gestion des risques et de résilience est souvent traitée relativement indépendamment du concept d'adaptation au changement climatique, aucun des groupes questionnés n'a une approche intégrée de la résilience structurelle et organisationnelle, le concept n'est pas perçu comme complémentaire, mais « séparé ». Or un lien fort existe et doit exister dans la planification des 2 volets de la résilience globale.

Sur le plan de la résilience économique, ce sont des groupes souvent historiquement publics, dont la capitalisation est encore largement sous le regard, voire sous le contrôle de l'État pour certains. Pour d'autres, ce sont des groupes internationaux cotés en bourse et qui gèrent leurs risques au travers des bonnes pratiques financières traditionnelles avec le concours de process de transfert de risques (assurances) et de capitalisation de réserve. Ils ne sont pas soumis aujourd'hui à une réglementation particulière concernant leurs capacité de résilience économique, comme peuvent l'être les banques et établissements d'assurances au travers des traités et règlements Bâle 3 ou Solvency II et bientôt DORA.

Conclusion

Pour conclure, il ressort de ces interviews que les opérateurs, soumis à la législation sur les secteurs d'importance vitale, se préparent à l'intensification des risques existants et à l'arrivée de nouveaux en anticipant les conséquences possibles sur les réseaux. **Cependant, force est de constater que les niveaux de préparation sont très différents pour chaque opérateur.**



En témoigne premièrement, la présence ou non de groupes de travail dédiés aux risques pesant sur les infrastructures *(représenté par le graphique)*.

Deuxièmement, le périmètre de prévention des risques est également un facteur de la différence de préparation, il est loin d'être identique dans chaque entreprise.

Troisièmement, si les organisations ont mis en place des structures de gestion de crise, de continuité d'activité et de logistique appropriées. Les niveaux de formation, de résilience intrinsèque de ces équipes, et d'autonomie dans la durée, sont très variables.

Cela se mesure tant par le nombre de cadres formés et de capacités de turn-over des équipes de gestion de crise sur des crises « longues » voire « très longues », que par la capacité d'autonomie des centres de gestion de crise et des équipes logistiques qui est très variable et indique finalement qu'en absence de normes, chacun a sa propre « approche » métier et en découle son organisation de crise à partir de sa structure opérationnelle classique, ce qui est parfaitement logique, mais avec des niveaux de réponse liés à un évènement majeur de durée ou d'amplitude moyenne, et non sur les scénarios plus pénalisants. ***On constate toujours une résistance psychologique forte à considérer les catastrophes les plus graves comme « possibles ».***

Il est néanmoins intéressant de constater que les organisations qui mènent actuellement des réflexions sur les investissements à réaliser sur leurs réseaux pour les adapter aux changements climatiques sont celles dont l'organisation de résilience organisationnelle semble être la plus robuste.

Mais la disparité entre les opérateurs se retrouve également concernant les contacts avec les autres opérateurs et les exercices.

Ces disparités peuvent tout d'abord s'expliquer par le positionnement métier de l'opérateur et sa place dans la globalité du réseau géré. Un opérateur de la chaîne « énergie électrique » va travailler de manière beaucoup plus étroite entre les 3 grands opérateurs (EDF-RTE-ENEDIS) qu'avec les autres opérateurs d'autres réseaux (eau, Gaz..) Même si les interdépendances existent avec beaucoup.

En conclusion, le détail des questionnaires tend à nous brosser une image plus globale qui nous laisse à penser qu'un travail d'harmonisation des pratiques reste à entreprendre. L'objectif de « résilience globale » doit inclure aujourd'hui le concept de développement durable, mais il s'en distingue dans le sens où il caractérise les idées de vision intersectorielle, d'anticipation, de réduction de la vulnérabilité, et de permanence de service qui doivent être intrinsèques aux choix présents. C'est une vision de long terme sur les grands choix stratégiques avec des actions immédiates pour rendre les organisations plus résilientes aujourd'hui et demain.

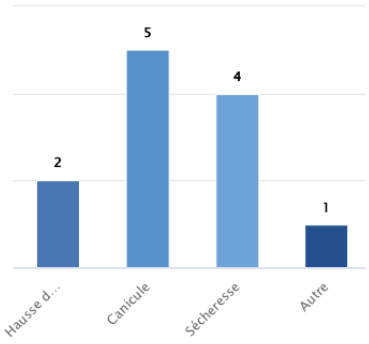
Détails des résultats du questionnaire « opérateurs »

Détail des réponses au questionnaire (si le total est inférieur à 5, cela signifie que certains n'ont pas répondu par volonté ou par absence de connaissances suffisamment précises pour répondre)

1.2. 1 - Avez-vous identifié les risques chroniques, liés au changement climatique, qui menaçent votre organisation ?

	Nombre	Pourcentage
Hausse des températures moyennes	2	40%
Canicule	5	100%
Sécheresse	4	80%
Autre	1	20%
Total	**5**	**100%**

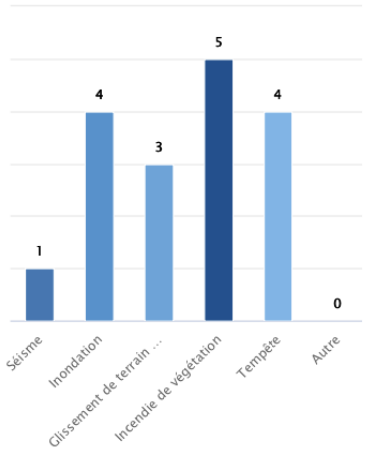
Détail des réponses
Inondations, pluies violentes



1.3. 2 - Avez vous identifié les risques extrêmes, liés au changement climatique, qui menacent votre organisation ?

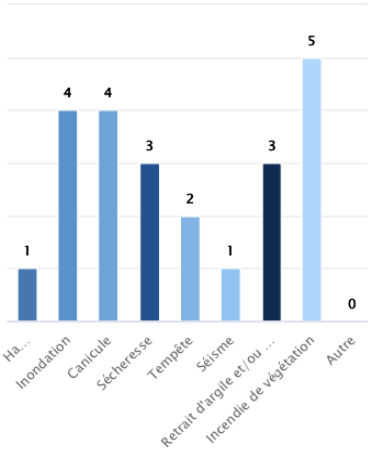
	Nombre	Pourcentage
Séisme	1	20%
Inondation	4	80%
Glissement de terrain et/ou retrait d'argile	3	60%
Incendie de végétation	5	100%
Tempête	4	80%
Autre	0	0%
Total	**5**	**100%**

Détail des réponses



1.4. 3 - Avez-vous identifié la vulnérabilité de vos réseaux face aux risques liés au changement climatique ?

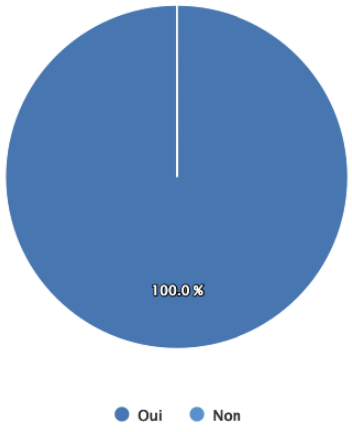
	Nombre	Pourcentage
Hausse des températures moyennes	1	20%
Inondation	4	80%
Canicule	4	80%
Sécheresse	3	60%
Tempête	2	40%
Séisme	1	20%
Retrait d'argile et/ou glissement de terrain	3	60%
Incendie de végétation	5	100%
Autre	0	0%
Total	**5**	**100%**



Détail des réponses

1.5. 4 - Avez-vous testé la robustesse de vos réseaux face aux nouveaux risques liés au changement climatique ?

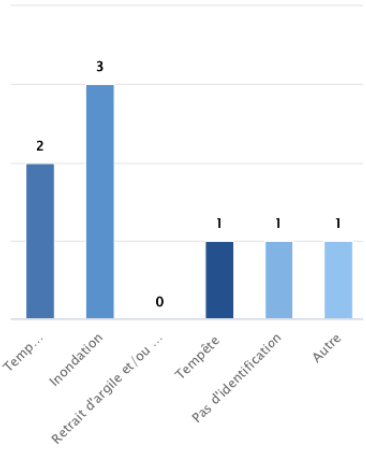
	Nombre	Pourcentage
Oui	5	100%
Non	0	0%
Total	**5**	**100%**



1.7. 4.2 - Avez-vous identifié à partir de quelle valeur de référence vos réseaux fonctionnent en mode dégradé pour les risques suivants ?

	Nombre	Pourcentage
Température / Canicule / Sécheresse	2	40%
Inondation	3	60%
Retrait d'argile et/ou glissement de terrain	0	0%
Tempête	1	20%
Pas d'identification	1	20%
Autre	1	20%
Total	**5**	**100%**

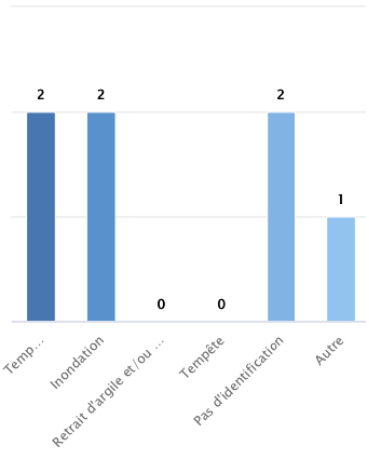
Détail des réponses
cf réponse précédente



1.6. 4.1 - Avez-vous identifié à partir de quelle valeur de référence vos réseaux deviennent inopérants pour les risques suivants ?

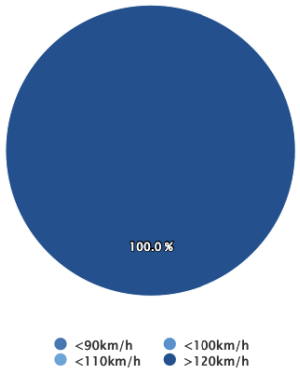
	Nombre	Pourcentage
Température / Canicule / Sécheresse	2	40%
Inondation	2	40%
Retrait d'argile et/ou glissement de terrain	0	0%
Tempête	0	0%
Pas d'identification	2	40%
Autre	1	20%
Total	**5**	**100%**

Détail des réponses
La détermination d'un seuil précis est un exercice très difficile. Nous disposons d'outils d'alerte pour surveiller les risques liés à la canicule pour les réseaux souterrains, et au vent/orages pour les résaux aériens. Des études sur les inondations ont été menées dans les zones sensibles.



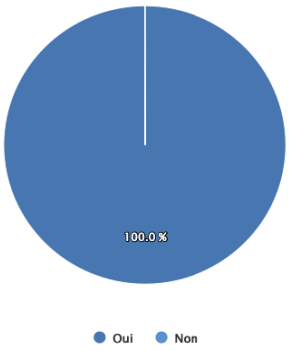
1.10. 4.2.2 - À partir de quelle vitesse de vent les réseaux fonctionnent en mode dégradé ?

	Nombre	Pourcentage
	0	0%
	0	0%
	0	0%
>120km/h	1	100%
Total	**1**	**100%**



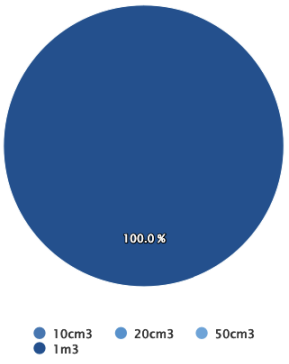
1.12. 5 - Vos réseaux sont-ils maillés, de manière à avoir une solution en cas de dysfonctionnement rendant une partie du réseau inopérant ?

	Nombre	Pourcentage
Oui	5	100%
Non	0	0%
Total	**5**	**100%**



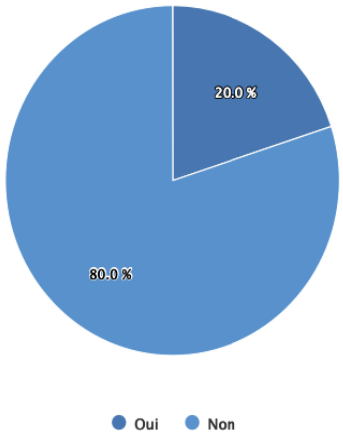
1.11. 4.2.3 - En cas d'inondation, à partir de combien de centimètres cubes d'eau vos réseaux fonctionnent en mode dégradé ?

	Nombre	Pourcentage
10cm3	0	0%
20cm3	0	0%
50cm3	0	0%
1m3	3	100%
Total	**3**	**100%**



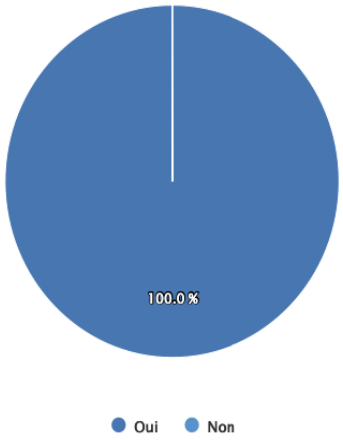
1.13. 6 - L'année 2022 a été marquée par des périodes de fortes chaleurs, également associée à plusieurs vagues de chaleurs. Votre entreprise a-t-elle rencontré des difficultés sur la continuité des réseaux ?

	Nombre	Pourcentage
Oui	1	20%
Non	4	80%
Total	**5**	**100%**



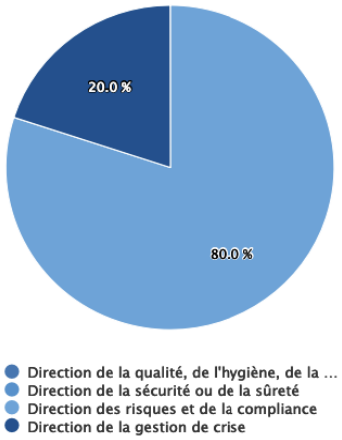
1.14. 6.1 - Un retour d'expérience (RETEX) a-t-il été réalisé ?

	Nombre	Pourcentage
Oui	1	100%
Non	0	0%
Total	**1**	**100%**



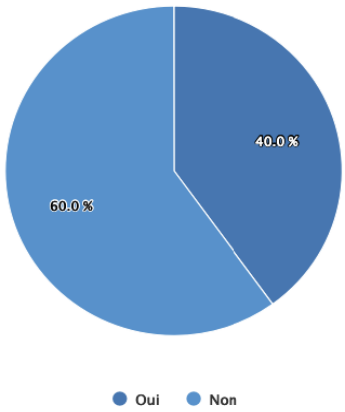
1.17. 8 - Quelle est la direction chargée de l'évaluation des risques ?

	Nombre	Pourcentage
Direction de la qualité, de l'hygiène, de la sécurité et de l'environnement (QHSE)	0	0%
Direction de la sécurité ou de la sûreté	0	0%
Direction des risques et de la compliance	4	80%
Direction de la gestion de crise	1	20%
Total	**5**	**100%**



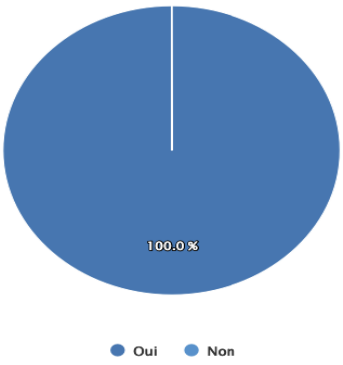
1.18. 9 - Dans cette direction, un groupe de travail dédié spécifiquement aux risques pesant sur les infrastructures existe-t-il ?

	Nombre	Pourcentage
Oui	2	40%
Non	3	60%
Total	**5**	**100%**



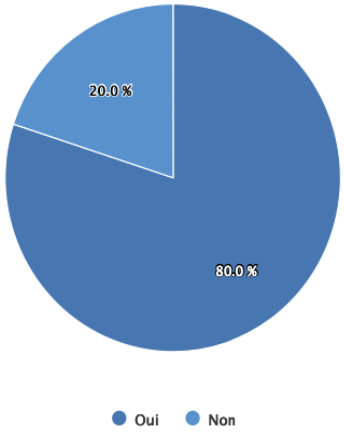
1.16. 7 - Le GIEC a récemment publié son 6e rapport. Votre entreprise a-t-elle pris en compte les avis du GIEC dans l'évaluation de vos risques ?

	Nombre	Pourcentage
Oui	5	100%
Non	0	0%
Total	**5**	**100%**



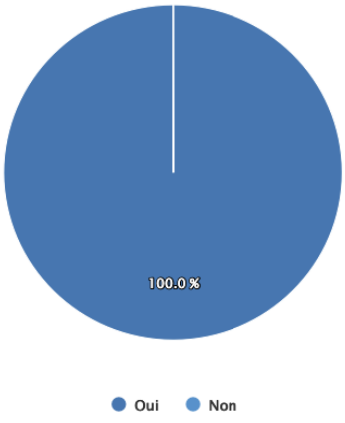
1.19. 10 - Votre entreprise dispose-t-elle d'un service dédié à la gestion de crise ?

	Nombre	Pourcentage
Oui	4	80%
Non	1	20%
Total	**5**	**100%**



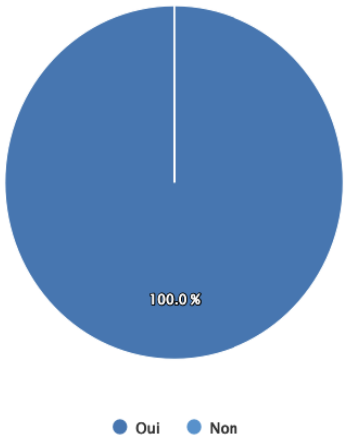
1.20. 10.1 - L'organisation est-elle structurée (formation, logistique, organisation, exercices) ?

	Nombre	Pourcentage
Oui	4	100%
Non	0	0%
Total	**4**	**100%**



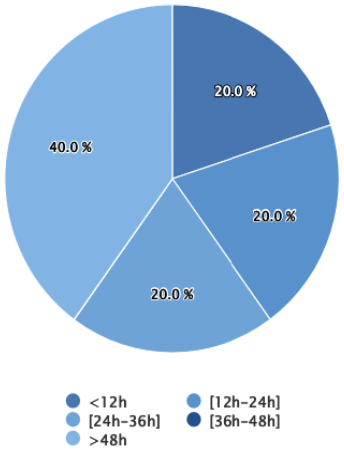
1.21. 11 - En cas de panne électrique, l'hypervision est-elle secourue par groupe électrogène ?

	Nombre	Pourcentage
Oui	5	100%
Non	0	0%
Total	**5**	**100%**



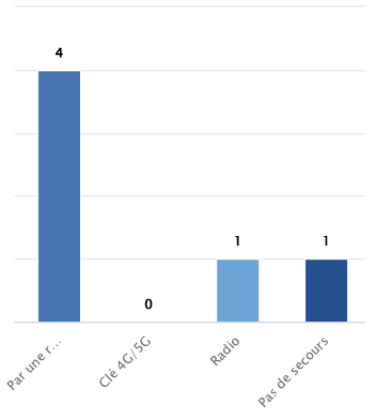
1.22. 11.1 - Quelle est l'autonomie du groupe électrogène ?

	Nombre	Pourcentage
	1	20%
[12h-24h]	1	20%
[24h-36h]	1	20%
[36h-48h]	0	0%
>48h	2	40%
Total	**5**	**100%**



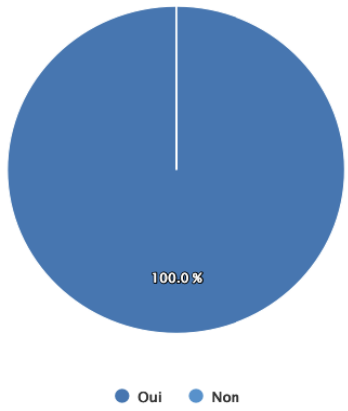
1.23. 12 - Les télécommunications du centre d'hypervision sont-elles secourues ?

	Nombre	Pourcentage
Par une redondance des lignes internet (Fibre/Satellite ou ADSL/ Satellite)	4	80%
Clé 4G/5G	0	0%
Radio	1	20%
Pas de secours	1	20%
Total	**5**	**100%**



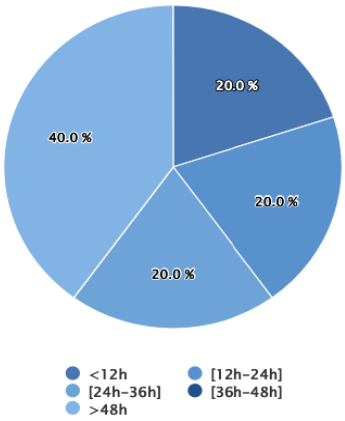
1.24. 13 - En cas de panne électrique, le centre de crise est-il secouru par groupe électrogène ?

	Nombre	Pourcentage
Oui	5	100%
Non	0	0%
Total	**5**	**100%**



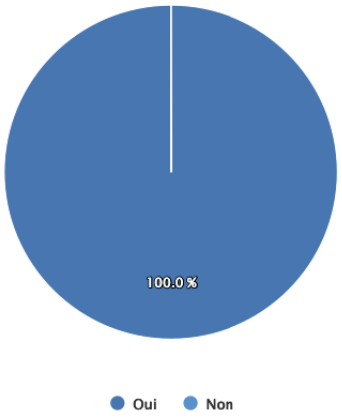
1.25. 13.1 - Quelle est l'autonomie du groupe électrogène ?

	Nombre	Pourcentage
	1	20%
[12h-24h]	1	20%
[24h-36h]	1	20%
[36h-48h]	0	0%
>48h	2	40%
Total	**5**	**100%**



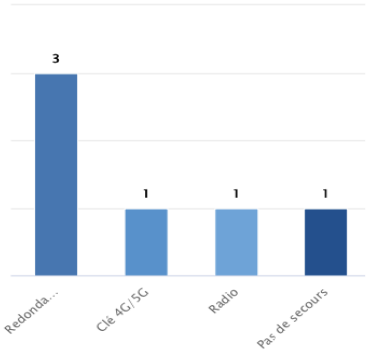
1.27. 15 - Vos plans de continuité d'activité prévoient-ils une crise émanant d'un autre réseau ?

	Nombre	Pourcentage
Oui	5	100%
Non	0	0%
Total	**5**	**100%**



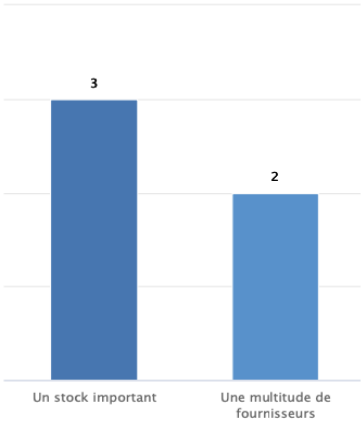
1.26. 14 - Les télécommunications du centre de crise sont-elles secourues ?

	Nombre	Pourcentage
Redondance des moyens d'accès (Fibre/Satellite ou ADSL/ Satellite)	3	60%
Clé 4G/5G	1	20%
Radio	1	20%
Pas de secours	1	20%
Total	**5**	**100%**



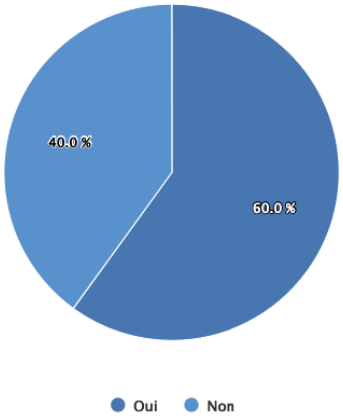
1.29. 16.1 - Ce maintien en condition opérationnelle est-il assuré par :

	Nombre	Pourcentage
Un stock important	3	100%
Une multitude de fournisseurs	2	67%
Total	**3**	**100%**



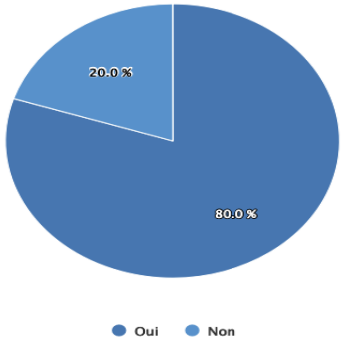
1.28. 16 - La chaine de valeur (supply chain) est-elle assurée pour le maintien en condition opérationnelle de ces réseaux face à des perturbations majeures ?

	Nombre	Pourcentage
Oui	3	60%
Non	2	40%
Total	**5**	**100%**



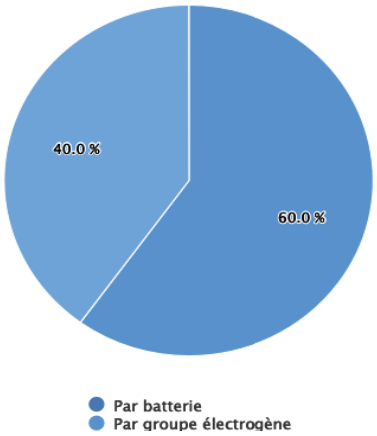
1.30. 17 - En cas d'événement majeur, avez-vous un plan de montée en puissance de vos effectifs de remise en état de vos réseaux ?

	Nombre	Pourcentage
Oui	4	80%
Non	1	20%
Total	**5**	**100%**



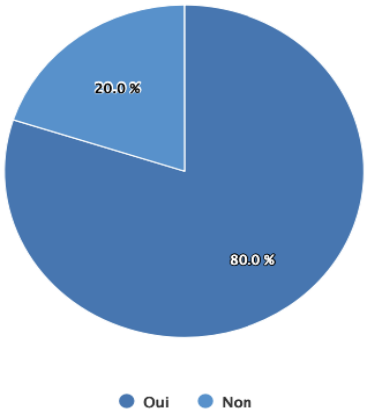
1.31. 18 - En cas de panne électrique, les services essentiels de l'organisation sont-ils secourus ?

	Nombre	Pourcentage
Par batterie	0	0%
Par groupe électrogène	3	60%
Non	2	40%
Total	**5**	**100%**



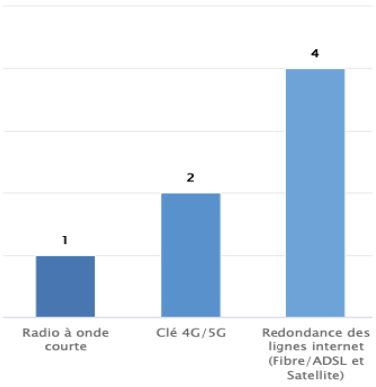
1.34. 19 - En cas de panne des télécommunications, l'organisation a-t-elle des moyens alternatifs ?

	Nombre	Pourcentage
Oui	4	80%
Non	1	20%
Total	**5**	**100%**



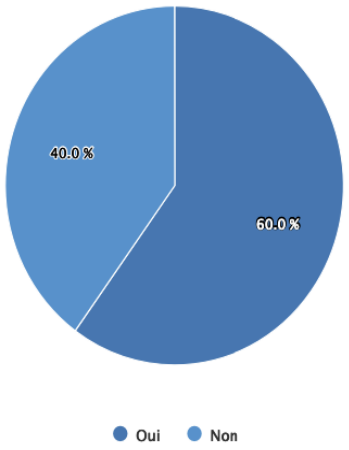
1.35. 19.1 - Quels sont ces moyens alternatifs ?

	Nombre	Pourcentage
Radio à onde courte	1	25%
Clé 4G/5G	2	50%
Redondance des lignes internet (Fibre/ADSL et Satellite)	4	100%
Total	**4**	**100%**



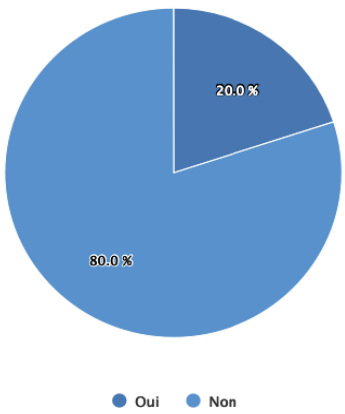
1.36. 20 - La notion de résilience structurelle est-elle connue au sein de l'organisation ?

	Nombre	Pourcentage
Oui	3	60%
Non	2	40%
Total	**5**	**100%**



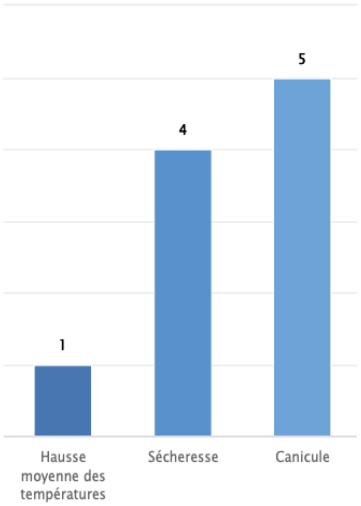
1.37. 21 - Votre planification a-t-elle été mise à jour au regard de la publication du 6e rapport du GIEC ?

	Nombre	Pourcentage
Oui	1	20%
Non	4	80%
Total	**5**	**100%**



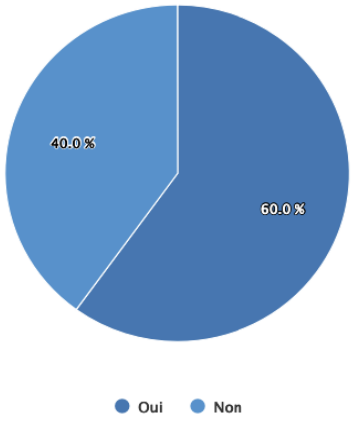
1.38. 22 - Les risques chroniques suivants sont-ils pris en compte par l'organisation et font-ils l'objet de plans spécifiques ?

	Nombre	Pourcentage
Hausse moyenne des températures	1	20%
Sécheresse	4	80%
Canicule	5	100%
Total	**5**	**100%**



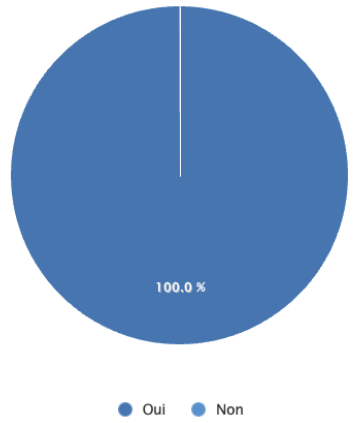
1.39. 23 - Face à la hausse des températures, votre entreprise a-t-elle identifié les actions à mettre en place pour adapter les infrastructures, les processus et les matériaux ?

	Nombre	Pourcentage
Oui	3	60%
Non	2	40%
Total	**5**	**100%**



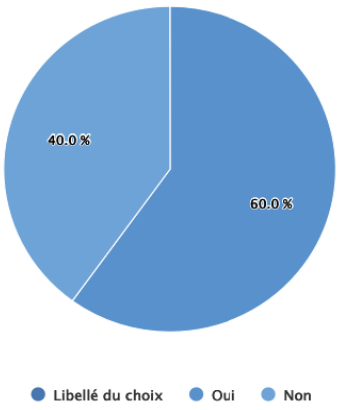
1.14. 9.1 - La collectivité a-t-elle des contacts réguliers avec ces opérateurs ?

	Nombre	Pourcentage
Oui	2	100%
Non	0	0%
Total	**2**	**100%**



1.40. 24 - L'entreprise a-t-elle mené des réflexions pour identifier des solutions techniques adaptées aux défis climatiques de demain ?

	Nombre	Pourcentage
Libellé du choix	0	0%
Oui	3	60%
Non	2	40%
Total	**5**	**100%**

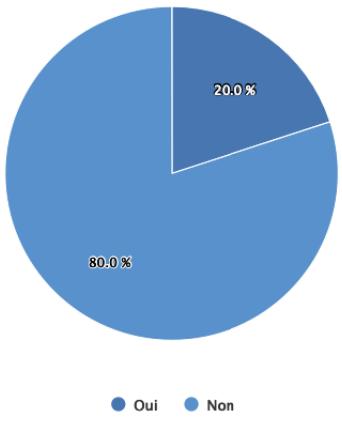


1.41. 24.1 - Pouvez-vous détailler ces réflexions ?

Détail des réponses
Investissements
La trajectoire d'investissement à l'horizon 2040 a été construite en intégrant notamment des actions de renforcement de la résilience des réseaux (canicules, tempêtes).
objets connectés pour mesurer échauffement câbles et calculer la distance au sol

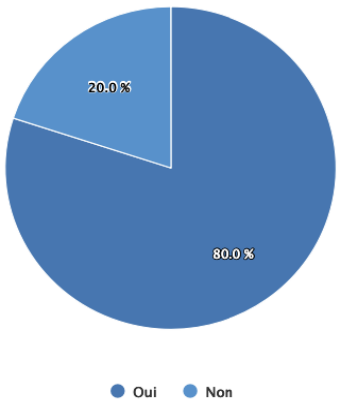
1.43. 26 - Les réseaux sont interdépendants les uns et les autres. Votre entreprise dispose-t-elle d'une cartographie d'interdépendance des réseaux ?

	Nombre	Pourcentage
Oui	1	20%
Non	4	80%
Total	**5**	**100%**



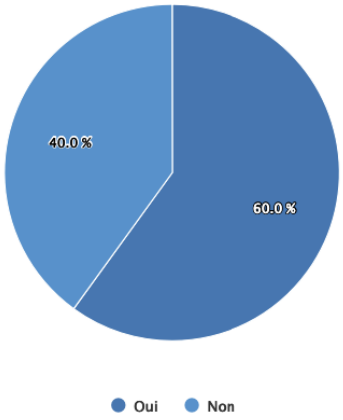
1.45. 27 - Votre entreprise travaille-t-elle avec les opérateurs en charge des autres réseaux ?

	Nombre	Pourcentage
Oui	4	80%
Non	1	20%
Total	**5**	**100%**



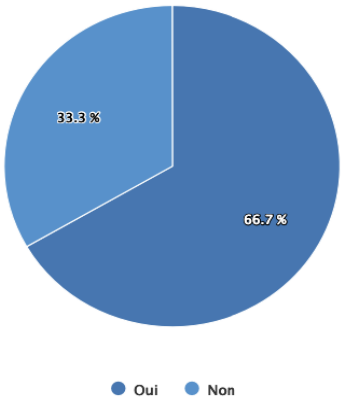
1.47. 28 - Votre entreprise a-t-elle déjà joué un exercice d'interruption des réseaux en raison d'une catastrophe naturelle ?

	Nombre	Pourcentage
Oui	3	60%
Non	2	40%
Total	**5**	**100%**



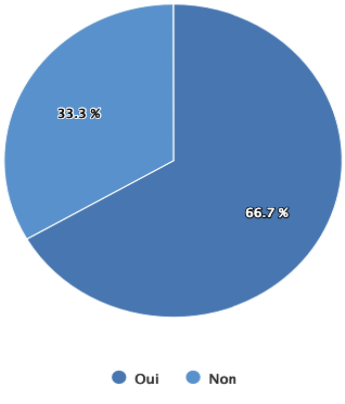
1.48. 28.1 - Cet exercice est-il joué de manière périodique ?

	Nombre	Pourcentage
Oui	2	67%
Non	1	33%
Total	**3**	**100%**



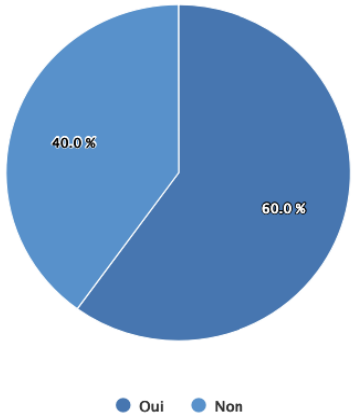
1.49. 28.2 - Cet exercice prévoit-il une panne émanant d'un autre réseau ?

	Nombre	Pourcentage
Oui	2	67%
Non	1	33%
Total	**3**	**100%**



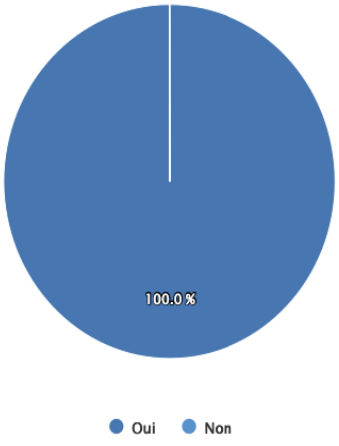
1.39. 23 - Face à la hausse des températures, votre entreprise a-t-elle identifié les actions à mettre en place pour adapter les infrastructures, les processus et les matériaux ?

	Nombre	Pourcentage
Oui	3	60%
Non	2	40%
Total	**5**	**100%**



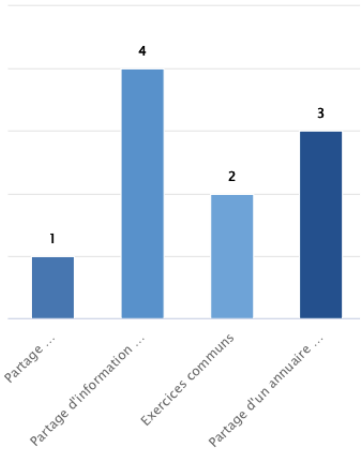
1.51. 30 - La directive Résilience des Entités Critiques a été adoptée par le Parlement et le Conseil Européen. Elle va être transposée prochainement dans le droit français. Avez-vous connaissance des évolutions apportées par ce texte ?

	Nombre	Pourcentage
Oui	5	100%
Non	0	0%
Total	**5**	**100%**



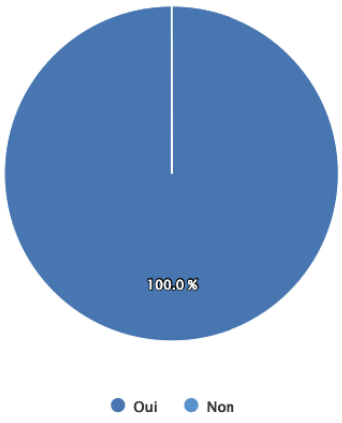
1.46. 27.1 - Ce travail se traduit par :

	Nombre	Pourcentage
Partage des analyses de risques	1	25%
Partage d'information sur les vulnérabilités des réseaux	4	100%
Exercices communs	2	50%
Partage d'un annuaire de crise	3	75%
Total	**4**	**100%**



1.52. 31 - Si vous êtes inclus dans une législation d'importance vitale, avez-vous pris en compte dans votre dispositif les risques naturels et technologiques majeurs pour évaluer votre résilience et votre continuité d'activité ?

	Nombre	Pourcentage
Oui	5	100%
Non	0	0%
Total	**5**	**100%**



Rapport d'interviews de 2 collectivités

Si les opérateurs jouent un rôle essentiel dans la gestion des réseaux, il ne faut pas oublier les collectivités. En effet, ces dernières, au travers de leurs compétences, sont soit opérateurs de réseaux lorsque la gestion de ces réseaux est interne, soit elles délèguent le service sous forme de concessions, le plus souvent à des opérateurs privés.

Certaines collectivités, selon leur taille et leur importance, peuvent être soumises à la législation sur la sécurité des activités d'importance vitale, notamment pour les communes opérant les systèmes "eau potable" (usine et réseau de distribution) avec les obligations qui y sont liées en termes de sûreté et de continuité d'activité.

Ces éléments nous ont conduits à interroger deux collectivités dans le cadre de cette étude : la Ville de Paris et la ville d'Orléans. Ce choix a été motivé par plusieurs facteurs :

- La Ville de Paris pour son statut particulier lié à sa taille, son importance et son organisation notamment avec la Préfecture de Police avec laquelle elle partage la gestion de certaines compétences en matière de gestion de crise et de sauvegarde
- La Ville d'Orléans par sa taille et sa sensibilité aux risques majeurs

Nous les avons interrogés dans un premier temps (Chapitre 1) sur la gestion de leurs services essentiels, à savoir la gestion de l'eau, des déchets, ainsi que sur la gestion des transports urbains, et leurs rapports avec les fournisseurs de services essentiels tels que l' énergie électrique, et les télécommunications

Dans un deuxième temps (Chapitre 2) nous nous sommes concentrés sur la planification et leur organisation pour répondre aux événements majeurs auxquels elles pourraient être confrontées. Enfin, dans un troisième et dernier temps (Chapitre 3), c'est leur maturité dans l'analyse et l'évolution des risques qui a été interrogée.

I. Résilience structurelle et organisationnelle

Les questions ont porté sur huit services essentiels pour les populations et les pouvoirs publics: l'eau potable, l'eau propre, l'assainissement, les déchets, l'alimentation électrique, les moyens de télécommunication, les transports routiers et ferroviaires ainsi que l'approvisionnement en nourriture.

L'objectif est non seulement d'identifier le mode de gestion de chacun de ces services (gestion interne, déléguée ou indépendante (simple client), mais également les vulnérabilités auxquelles ces services sont confrontés et les mesures mises en place ou envisagées pour répondre à ces situations de risques ou de crise.

1. Eau potable et eau propre

Par définition, et comme expliqué dans le présent rapport, la gestion de l'eau est fortement dépendante de l'approvisionnement en électricité, pour le fonctionnement des infrastructures, et aux télécommunications pour la télégestion et la communication.
Les deux collectivités proposent deux modes de gestion différents : la Ville de Paris est en régie via "Eau de Paris" tandis qu'Orléans, au travers de la Métropole, a délégué sa gestion de l'eau à un opérateur privé.

La ville d'Orléans, en faisant le choix de la délégation, se déleste de l'analyse des risques, responsabilité du prestataire. À Orléans, c'est Suez qui a l'exploitation de l'eau potable et des usines de production. Les réseaux et les usines sont, au-delà des risques naturels ou sécuritaires pouvant endommager les infrastructures obligeant un fonctionnement en mode dégradé ou une coupure de service, exposés aux risques d'une coupure d'approvisionnement électrique ou de télécommunications.

Il relève de la responsabilité de l'opérateur de prendre les dispositions nécessaires dans **le cadre de son cahier des charges**, pour assurer une continuité électrique d'urgence

via des groupes électrogènes et des contrats adéquats avec le prestataire électrique pour une remise en état rapide des installations et de la fourniture de courant. Il en va de même pour les télécommunications. Pour limiter les risques liés à une rupture physique ou à une perte d'énergie sur une partie du réseau d'eau, ce dernier est redondant.

En revanche, de son côté, la municipalité a pris ses dispositions pour s'assurer d'un approvisionnement en cas de coupure d'eau potable auprès de son délégataire. Suez doit fournir, dans un délai maximum de 12h, de l'eau en bouteille à la population. Concernant l'approvisionnement en eau propre, également délégué, le contrat prévoit une solution de secours en 12h à 24h.

Dans ce cadre, **la ville et la métropole d'Orléans ont la responsabilité initiale de l'approvisionnement en eau. Mais en faisant le choix de la délégation auprès de Suez, elles transfèrent la responsabilité de l'approvisionnement à l'opérateur, même si elles demeurent responsables des opérations**.

La Ville de Paris a fait le choix de conserver la gestion de l'eau via une régie de "Eaux de Paris". Elle est donc, via sa régie « Eau de Paris », "opérateur de réseau".

Concernant les interdépendances, le réseau d'eau est redondant et surtout fonctionne de manière gravitaire limitant son exposition au réseau électrique et aux télécommunications, aux pompes de relevage. Une panne de courant ou de télécommunication pourrait entraîner un fonctionnement en mode dégradé, mais n'entraînera pas nécessairement un arrêt complet du réseau d'eau. En revanche, les usines de traitement sont-elles soumises aux risques de perte électrique et de télécommunications.

La commune dispose cependant de son propre système de surveillance et d'alerte des incidents et dispose de plans particuliers face aux risques. La situation de Paris oblige Eaux de Paris a avoir des documents formalisés (Plans de Continuité d'Activité/Plans Particuliers d'Interventions Inondation) et d'une connaissance de son exposition en cas de crue majeure de la Seine ou de la Marne.

Si la commune estime ce risque comme globalement bien maîtrisé, il persiste des interrogations. En effet, des réflexions vont être engagées pour réfléchir à des solutions alternatives en cas de rupture d'approvisionnement et pour clarifier les rôles entre la commune, l'opérateur Eau de Paris, la Métropole, et la Préfecture de Police.

2. Gestion des déchets

La gestion des déchets peut être divisée en trois phases : la récupération, l'évacuation et le traitement. La récupération et le traitement sont dépendants de la praticité ou non des routes et de la disponibilité ou non des carburants. Tandis que le traitement est lui dépendant de l'alimentation électrique et des télécommunications. Ces interdépendances sont existantes, quel que soit le choix fait par la collectivité concernant la gestion de ses déchets.

La ville d'Orléans a conservé cette compétence et est de fait responsable de l'identification des risques, de la mise en place d'un système de surveillance et de l'élaboration de plans d'urgence face aux risques. Elle affirme être en mesure de pouvoir assurer l'évacuation, la récupération et le traitement des ordures ménagères y compris lors d'événements majeurs, mais également de gérer les déchets post-catastrophe qui peuvent présenter des caractéristiques particulières (taille, toxicité, poids, etc.).

En cas de perte d'un réseau entraînant l'arrêt des usines de traitement, deux solutions sont possibles : le stockage des déchets, le temps de la réparation et/ou le délestage vers d'autres usines partenaires.

De son côté, la Ville de Paris a une organisation particulière. En effet, il y a une délégation partielle : le traitement et la valorisation sont assurés par Syctom (syndicat mixte) tandis que la collecte se fait en régie pour certains arrondissements et en délégation vers des opérateurs privés pour les autres.

De fait, les activités les plus sensibles aux autres réseaux, à savoir le traitement et la valorisation, relèvent de la responsabilité des opérateurs délégués qui en sont chargés. De l'analyse de risque au PCA en passant par la gestion de crise, les opérateurs sont en charge d'assurer la continuité d'activité, mais comment ces actions sont-elles notées ou évaluer par la collectivité, la question de la formalisation de ces actions demeure.

Concernant l'évacuation des déchets post-catastrophe, lorsque cela relève des opérateurs privés, des accords sont prévus avec des opérateurs privés selon le type de déchets qui peuvent nécessiter des équipes mobiles spécialisées. La commune a également les moyens humains et techniques pour assurer une partie de la récupération, de l'évacuation et du traitement de ces déchets, il est cependant relevé un risque de désorganisation en cas de crue majeure.

Si la récupération des déchets est principalement soumise aux transports (routes et carburants), le traitement et la valorisation de ces derniers sont particulièrement exposés au risque électrique et dans une moindre mesure aux télécommunications. Ces éléments étant délégués par les deux collectivités, **la responsabilité de trouver des solutions lors de la rupture d'approvisionnement relève des opérateurs et ils dépendent des exigences de la commune dans son cahier des charges auprès des opérateurs privés et du prix que la commune est prête à payer pour ces sujétions.**

3. Alimentation électrique

L'alimentation électrique est dépendante des télécommunications, pour sa gestion, mais également de l'approvisionnement en eau pour assurer le refroidissement des centrales et le fonctionnement des ouvrages hydro-électriques.

La question de l'alimentation électrique ne dépend pas directement des collectivités, étant donné qu'elles ne sont pas gestionnaires de ces réseaux, en revanche elles peuvent prendre des mesures pour, si ce n'est éviter une coupure, avoir des solutions de secours lorsqu'elles surviennent.

Ces mesures se divisent en deux phases : l'identification des bâtiments abritant les services essentiels et leur raccordement à des secours en groupe électrogène (et carburant).

La ville d'Orléans, d'après le questionnaire, a fait le choix de ne pas couvrir ses bâtiments essentiels par des groupes électrogènes. Nous n'avons pas d'information quant à une redondance des raccordements électriques pour limiter le risque de coupure.

La Ville de Paris quant à elle a identifié ses bâtiments critiques et les a couverts avec des groupes électrogènes. À titre d'exemple, ces bâtiments sont l'Hôtel de Ville, les datacenters municipaux, des usines de gestion d'eaux usées ou encore les EHPAD. L'autonomie de ces groupes est très variable, *"de 2h pour certains sites à 120h pour certains EPHAD"*.

4. Télécommunications

Les télécommunications sont dépendantes du réseau électrique, pour le fonctionnement des installations critiques (relais, fibres, antennes GSM, datacenters, etc.) et de l'approvisionnement en eau pour le refroidissement de certains datacenters.

La question des télécommunications est identique à celle de l'alimentation électrique, si les communes ne sont pas directement maîtres des réseaux, elles peuvent prendre des mesures pour limiter leur exposition aux risques de coupure et trouver des solutions alternatives.

Dans ce cadre, la ville d'Orléans dispose de deux moyens alternatifs : des radios VHF ainsi qu'une mise à disposition de clés 4G et 5G. En plus, elle a un contrat avec son opérateur pour une remise en état des communications dans un délai de 2h à 6h, quelle que soit l'origine de la panne.

Concernant les télécommunications, la Ville de Paris a l'avantage de travailler en collaboration avec la Préfecture de Police et les opérateurs présents à proximité. De fait, plusieurs moyens alternatifs sont prévus en cas de perte des moyens "classiques" :

- Liaisons radio partagées avec la RATP ;
- Redondance des lignes internet et des antennes relais ;
- Fibre sécurisée partagée avec la Préfecture de Police.

5. Transports

Les transports routiers sont relativement indépendants vis-à-vis des autres réseaux. En effet, bien qu'il existe un besoin électrique pour l'alimentation des signalisations et des télécommunications pour assurer la surveillance du réseau et gérer les systèmes d'information, une perte de ces réseaux entraînera un fonctionnement en mode dégradé, avec un risque d'accident, mais n'empêchera pas les usagers d'utiliser la route.

Les deux collectivités ont identifié et hiérarchisé les routes qui sont sous leur supervision. De fait, elles sont en mesure de les remettre rapidement en cas de crise. **La Ville de Paris a identifié les températures de 35°C à 40°C comme étant problématique pour l'état des routes. Face à ce risque de détérioration, renforcé par le réchauffement climatique, plusieurs pistes sont évoquées et testées :**

- Diversification des matériaux pour limiter le goudron
- Limitation des poids lourds à certains horaires
- Analyse des ponts et du goudron pour identifier leurs faiblesses

Pour alimenter ces travaux et hiérarchiser les efforts à faire, la Ville a à sa disposition une carte des températures des surfaces pour identifier les îlots de chaleur.

6. Résilience alimentaire

L'alimentation dispose d'un statut particulier selon la nature des aliments. En effet, les produits frais/froids ont de fait une dépendance au réseau électrique garant du maintien de la chaîne du froid à températures des produits concernés.

L'ensemble des produits alimentaires, selon leur origine, est dépendant des moyens de transports routiers et ferroviaires pour arriver sur le lieu de destination.

Dans le cas d'une coupure d'approvisionnement, comme ça a pu être le cas pour certaines communes dans les Alpes-Maritimes lors de la Tempête Alex, il est intéressant de constituer des réserves pour assurer une solution de secours immédiate aux citoyens.

Dans ce domaine, la Ville d'Orléans est en mesure d'assurer un approvisionnement pendant 48h.

De son côté, la Ville de Paris n'a pas été en mesure de répondre à la question, la compétence étant partagée avec la Préfecture de Police.

En qualité d'opérateurs réseaux, que les services soient délégués ou gérés en interne, s'assurer de la bonne prise en compte de l'ensemble des risques (naturels, sécuritaires et liés aux autres réseaux) par leurs services ou par l'opérateur en charge du réseau.

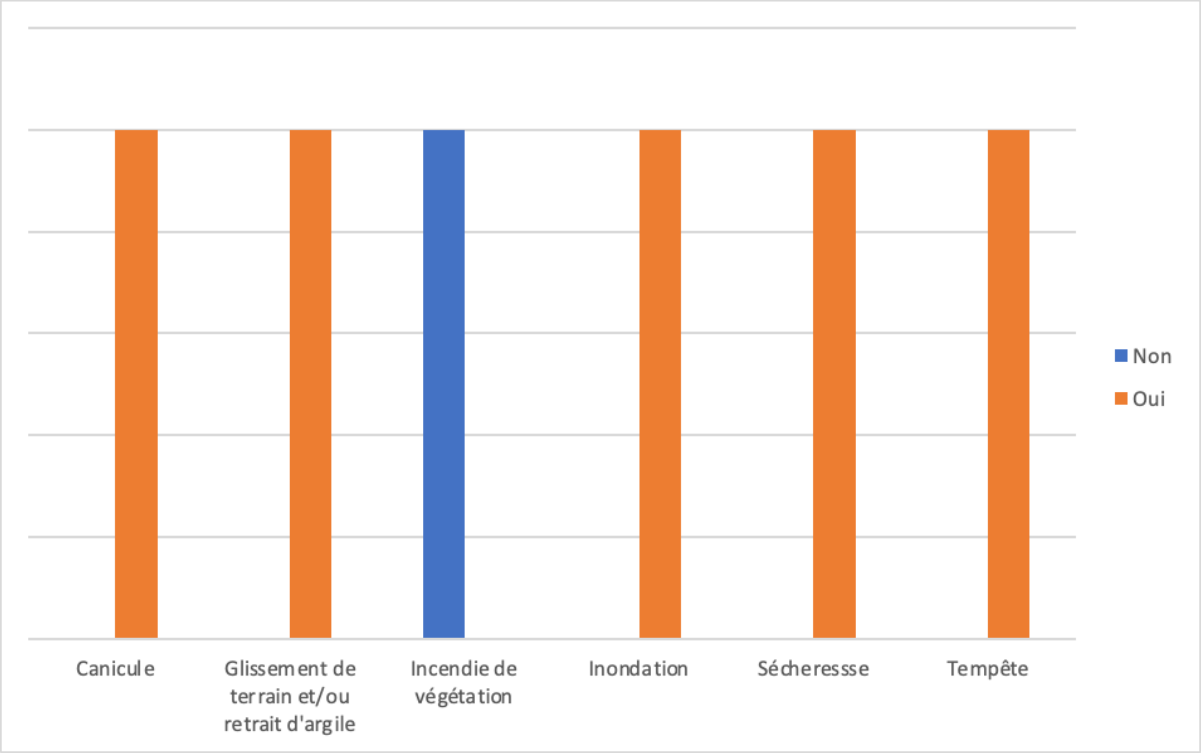
Au-delà de l'étude de l'interdépendance des réseaux, les collectivités se doivent d'identifier les risques naturels ou technologiques auxquels leurs infrastructures sont exposées et de se préparer à la survenue d'une crise.

II. Planification et organisation

Cette partie traite de la capacité des collectivités interrogées à faire face aux risques et aux potentielles crises. **La première étape consiste de fait à la préparation à la crise via l'élaboration d'un Plan Communal de Sauvegarde, réalisé par les deux**

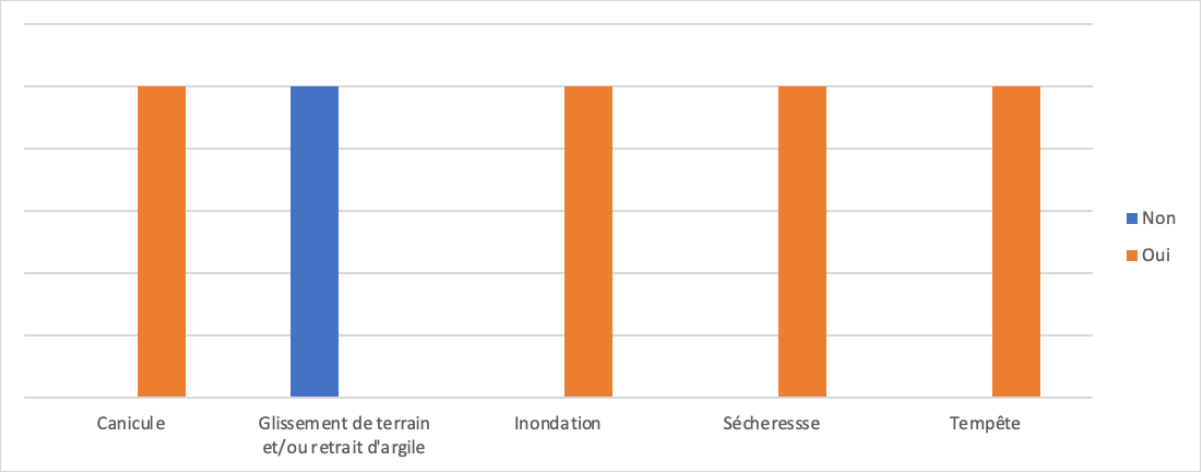
communes. *À noter que celui de la Ville de Paris est en cours de révision en partenariat avec la Préfecture de Police.*

De manière plus spécifique, les collectivités peuvent établir des plans particuliers adaptés à chaque risque. La Ville de Paris couvre presque tous les risques menaçant son territoire :



Corrélation entre les plans particuliers et les risques identifiés de la Ville de Paris.

La ville d'Orléans dispose, elle aussi, de plans particuliers, couvrant un large éventail de risques, y compris certains n'étant pas identifiés précédemment comme des risques majeurs pour le territoire, mais ne prenant pas en compte un risque identifié : le retrait d'argile :



Corrélation entre les plans particuliers et les risques identifiés par la ville d'Orléans.

Au-delà de l'identification des risques, il convient d'assurer une capacité à répondre aux défis imposés par les événements. Cela se traduit par un "supply chain" dimensionnée aux risques auxquels le territoire est exposé et sa capacité à maintenir en condition opérationnelle (MCO) les réseaux dont la collectivité a la gestion.

Le maintien en condition opérationnelle (MCO) vise à assurer une disponibilité optimale des matériels, afin de satisfaire les objectifs des contrats opérationnels définis des dits réseaux (cahier des charges). Si les deux collectivités estiment que leur supply-chain est en mesure d'assumer des perturbations majeures, notamment grâce à un stock conséquent ou des accords de fourniture contractuellement assurés permettant de remplacer les pièces défectueuses rapidement. Il est important de « chiffrer » le niveau de disponibilité de ces équipements et donc des services associés, ce qui n'est jamais clairement communiqué et qui est un point clé de l'analyse du niveau de résilience d'un système ou réseau. Il conviendrait d'analyser plus avant ces questions dans le cadre des obligations contractuelles des parties.

En parallèle, les répondants ont signalé avoir également conclu des partenariats avec d'autres collectivités pour obtenir de l'assistance en cas de crise majeure.

Enfin d'un point de vue plus global et budgétaire, les collectivités ont identifié les coûts de préparation à une crise, qu'il s'agisse du matériel spécifique ou le fonctionnement. Ces investissements sont réalisés, mais s'intègrent

généralement dans les budgets au sein des différents services opérationnels, il n'y a pas le plus souvent pas de budget particulier et visible dédié à ces dépenses de préparation, ce qui est un vrai problème pour évaluer l'effort réalisé.

Les collectivités font preuve d'une certaine maturité dans la planification et la préparation des crises en rédigeant ou en reprenant les plans nécessaires (PCS-PICS-PRA-PCA..), en incluant les conséquences de dommages sur les réseaux, mais également en intégrant les évolutions enregistrées dans la gestion des risques en déterminant pour les futurs acquisitions ou investissements, les sujétions à prendre en compte pour les futurs réseaux ou infrastructures sensibles.

III. Maturité et positionnement dans l'écosystème

Les deux collectivités ont procédé à une identification des risques, aussi bien chroniques qu'extrêmes, auxquels elles peuvent être exposées. On constate que les deux collectivités subissent, ou vont subir, les effets du changement climatique tel que définis dans l'étude ci-avant: une augmentation de la température globale et une multiplication des événements considérés comme extrêmes (inondation, glissement de terrain, tempête,).

Face à cette augmentation des risques, on constate une montée en puissance des dispositifs de prévention, qui commence dans un premier temps par une identification des services essentiels et, dans un second temps, à une étude de la vulnérabilité de ces derniers aux conséquences du changement climatique. À ce titre, les deux collectivités ont également identifié les valeurs de référence à partir desquelles leurs services pouvaient commencer à fonctionner en mode dégradé. **Cette étude n'a pas été poussée jusqu'aux valeurs qui rendent inopérants les services, excepté pour les données recensées dans la Mission d'Information et d'Évaluation "Paris à 50°C".**

L'année 2022, au travers des périodes de fortes chaleurs, a été un premier moment charnière pour tester et comprendre la robustesse des dispositifs. Aucune des deux

collectivités n'a constaté de difficultés majeures pour assurer la continuité de ses services essentiels. Cependant, la Ville de Paris constate une inégalité territoriale avec des dispositifs qui ont du mal à toucher les populations éloignées du service public et cela se traduit par une mortalité plus élevée dans les quartiers populaires avec des logements peu ou pas rénovés. Mais cette difficulté est liée, non pas à la vulnérabilité particulière des réseaux, mais à une fragilité des populations plus précaires et des difficultés à adopter de bons comportements.

Concernant les réseaux ne relevant pas de la responsabilité des collectivités, il existe tout de même un lien entre les opérateurs et les responsables locaux. Les communes disposent d'une cartographie de l'ensemble des réseaux présents sur leur territoire : réseau électrique basse et haute tension, réseau d'eau potable et d'assainissement, réseau routier communal, réseau ferroviaire et réseau de télécommunication (fibre/ADSL). De plus, elles ont accès grâce aux contacts, réguliers, qu'elles ont avec les opérateurs de ces réseaux, à une certaine connaissance des vulnérabilités de ces derniers face aux risques du territoire. Cet échange va même, dans le cas de la Ville de Paris, a un partage des analyses de risques avec les opérateurs.

Si on peut constater des petites différences, normales considérant que les deux communes sont des entités différentes dotées de la libre administration, on peut néanmoins affirmer que ce sont des organisations matures qui intègrent la notion du risque et ses évolutions liées au changement climatique. Pour ce faire, elle s'intègre dans l'écosystème d'opérateurs qui ont en charge les réseaux indispensables à la vie de leur territoire.

Conclusion

Il convient de garder à l'esprit lors de l'analyse de la différence de taille et de moyens entre la Ville de Paris et la ville d'Orléans. Si les deux villes présentent une préparation et une appréhension des risques auxquels leurs réseaux sont exposés, force est de constater qu'il y a des écarts au sein de cette préparation. Cet écart peut s'expliquer par les moyens, mais également par la volonté politique des décideurs locaux, car, en vertu du principe de libre administration des collectivités territoriales, chaque pouvoir

exécutif local décide du détail du niveau de préparation de sa collectivité, à partir où le socle légal en matière de prévention et de sauvegarde est assuré.

Au même titre que les opérateurs, les collectivités, lorsqu'elles gèrent des réseaux de grande importance, peuvent être intégrées dans la réglementation des secteurs d'activités d'importances vitales et le seront de facto dans celle de la Résilience des Entités Critiques, dont la traduction dans la législation nationale devrait être publiée au cours de l'année 2024.

Ces législations obligent les opérateurs réseau, donc les collectivités, à assurer la continuité d'activité des services essentiels en temps de crise.

Dans ce contexte, la préparation globale des entités est essentielle et cette dernière passe par :

- L'anticipation des risques renforcés ou apportés par le changement climatique ;
- L'adaptation des infrastructures réseau aux effets du changement climatique ;
- L'appréhension complète de l'écosystème dans lequel les opérateurs évoluent, à savoir les interdépendances des réseaux, les opérateurs responsables et les risques auxquels ils sont confrontés ;
- La capacité à réagir et à affronter une crise.

Des pistes d'améliorations sont possibles, l'entretien avec la Ville de Paris les a conduits à engager des réflexions sur des risques qu'ils n'avaient pas envisagées et à s'interroger sur la répartition des rôles et des responsabilités avec les parties prenantes, notamment la Préfecture de Police qui joue un rôle majeur dans la prévention des risques et la gestion de crise sur l'île de France.

L'interrogation porte plus largement sur la capacité des petites communes, ayant de fait un budget plus réduit, à avoir un niveau de préparation suffisant pour assurer la continuité de leurs services essentiels en cas d'événement majeur. Le nouveau rôle des intercommunalités, au travers des nombreux transferts de compétences et des PICS introduits par la Loi Matras pourra être une solution en proposant un échelon avec plus de moyens et une capacité de coordination et de soutien entre les collectivités, mais

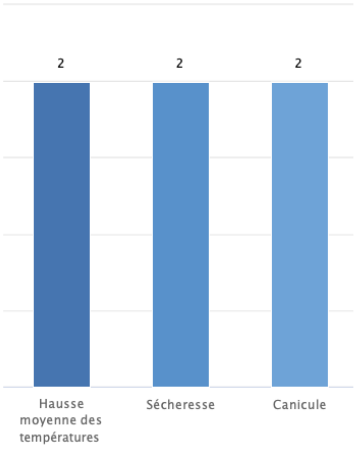
des règles claires sur les niveaux de résilience technique à atteindre devront être édictés par les pouvoirs publics pour assurer cette résilience. .

Détails des résultats du questionnaire « collectivités »

Détail des réponses au questionnaire (si le total est inférieur à 5, cela signifie que certains n'ont pas répondu par volonté ou par absence de connaissances suffisamment précises pour répondre)

1.2. 1 - Avez-vous identifié les risques chroniques liés au changement climatique qui menacent votre territoire ?

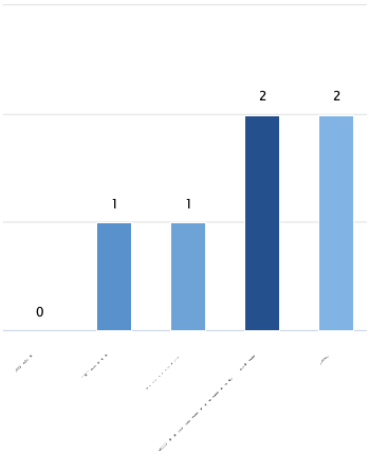
	Nombre	Pourcentage
Hausse moyenne des températures	2	100%
Sécheresse	2	100%
Canicule	2	100%
Total	**2**	**100%**



1.3. 2 - Avez-vous identifié les risques extrêmes liés au changement climatique qui menacent votre territoire ?

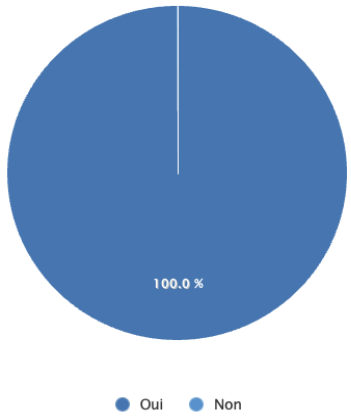
	Nombre	Pourcentage
Séisme	0	0%
Tempête	1	50%
Inondation	1	50%
Glissement de terrain et/ou retrait d'argile	2	100%
Autre	2	100%
Total	**2**	**100%**

Détail des réponses
Gonflement rétractation argile
Incendie de végétation / Sécheresse



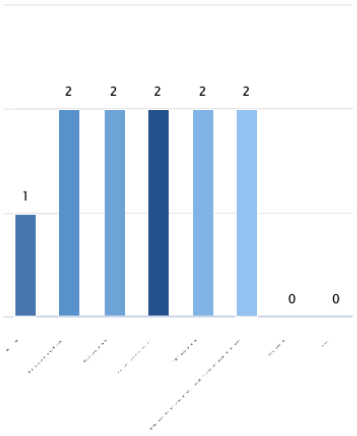
1.4. 3 - La collectivité a-t-elle identifié ses services essentiels ?

	Nombre	Pourcentage
Oui	2	100%
Non	0	0%
Total	**2**	**100%**



1.5. 3.1 - La collectivité a-t-elle étudié la vulnérabilité de ses services essentiels aux risques suivants

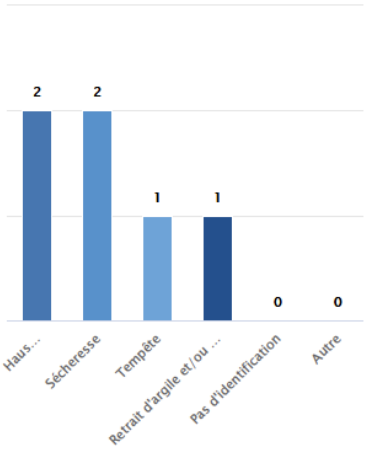
	Nombre	Pourcentage
Hausse des températures moyennes	1	50%
Inondation	2	100%
Canicule	2	100%
Sécheresse	2	100%
Tempête	2	100%
Retrait d'argile et/ou glissement de terrain	2	100%
Séisme	0	0%
Autre	0	0%
Total	**2**	**100%**



Détail des réponses

1.6. 4 - La collectivité a-t-elle identifié à partir de quelle valeur de référence les services essentiels fonctionnent en mode dégradé face aux risques suivants :

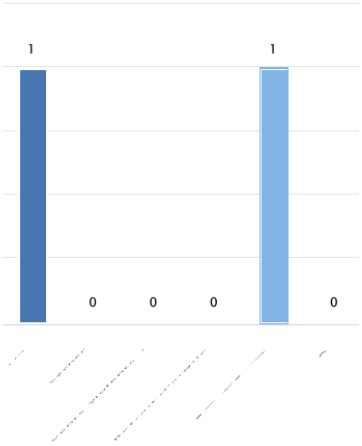
	Nombre	Pourcentage
Hausse des températures / Canicule	2	100%
Sécheresse	2	100%
Tempête	1	50%
Retrait d'argile et/ou glissement de terrain	1	50%
Pas d'identification	0	0%
Autre	0	0%
Total	**2**	**100%**



Détail des réponses

1.7. 5 - La collectivité a-t-elle identifié à partir de quelle valeur de référence les services essentiels deviennent inopérants face aux risques suivants :

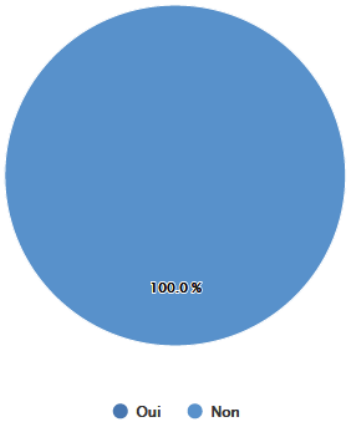
	Nombre	Pourcentage
Hausse des températures / Canicule	1	50%
Sécheresse	0	0%
Vents violents / Tempête	0	0%
Retrait d'argile et/ou glissement de terrain	0	0%
Pas d'identification	1	50%
Autre	0	0%
Total	**2**	**100%**



Détail des réponses

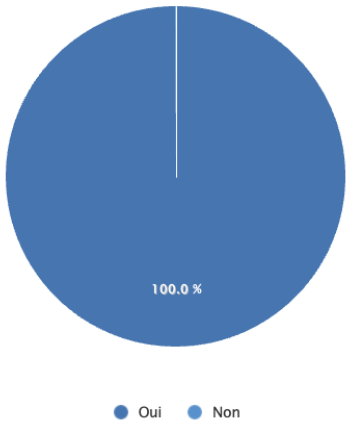
1.8. 6 - L'année 2022 a été marquée par des périodes de fortes chaleurs, également associé à plusieurs vagues de chaleurs. Votre collectivité a-t-elle rencontré des difficultés sur la continuité des services essentiels ?

	Nombre	Pourcentage
Oui	0	0%
Non	2	100%
Total	2	100%



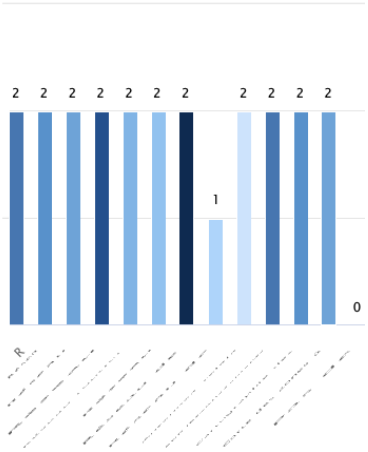
1.9. 6.1 - Un retour d'expérience (RETEX) a-t-il été réalisé ?

	Nombre	Pourcentage
Oui	1	100%
Non	0	0%
Total	1	**100%**



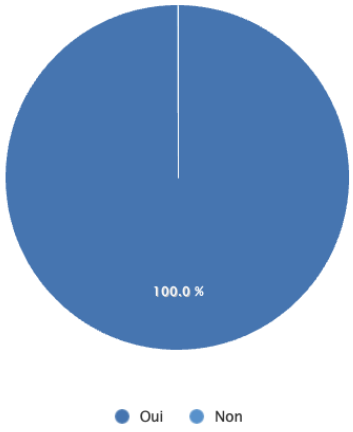
1.11. 7 - La collectivité a-t-elle une cartographie des réseaux présents sur son territoire ?

	Nombre	Pourcentage
Réseaux électrique haute tension	2	100%
Réseau électrique basse tension	2	100%
Réseau d'eau potable	2	100%
Réseau d'assainissement d'eau	2	100%
Réseau routier communal	2	100%
Réseau ferroviaire	2	100%
Réseau de télécommunications fibre	2	100%
Réseau de communication ADSL	1	50%
Antennes relais 3/4/5G	2	100%
ERP (Etablissements recevants du public)	2	100%
Cartographie des personnes à risques (malades chroniques, personnes âgées...)	2	100%
Carte des zones à risques naturels ou technologiques	2	100%



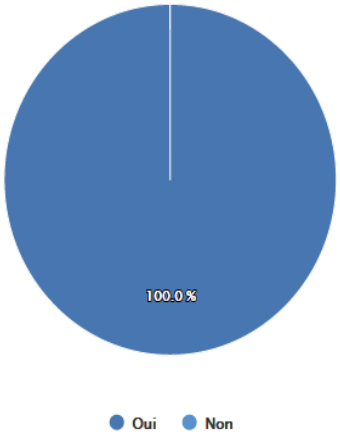
1.12. 8 - La collectivité a-t-elle identifié les vulnérabilités des réseaux aux risques menaçant le territoire ?

	Nombre	Pourcentage
Oui	2	100%
Non	0	0%
Total	**2**	**100%**



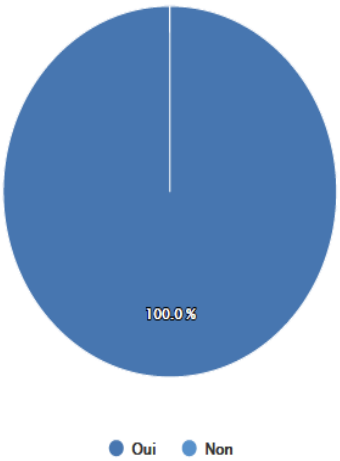
1.13. 9 - La collectivité a-t-elle identifié les opérateurs de réseaux qui ont une activité sur son territoire ?

	Nombre	Pourcentage
Oui	2	100%
Non	0	0%
Total	2	100%



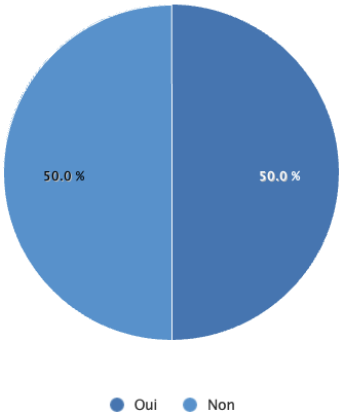
1.14. 9.1 - La collectivité a-t-elle des contacts réguliers avec ces opérateurs ?

	Nombre	Pourcentage
Oui	2	100%
Non	0	0%
Total	2	100%



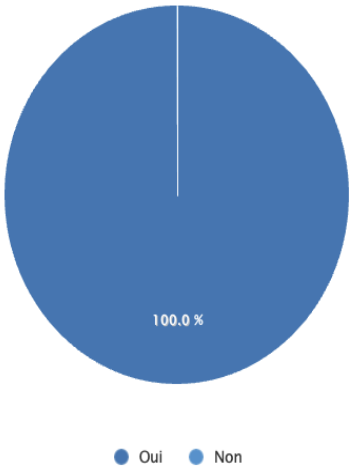
1.15. 9.2 - La collectivité partage-t-elle des analyses de risques avec les opérateurs réseaux ?

	Nombre	Pourcentage
Oui	1	50%
Non	1	50%
Total	**2**	**100%**



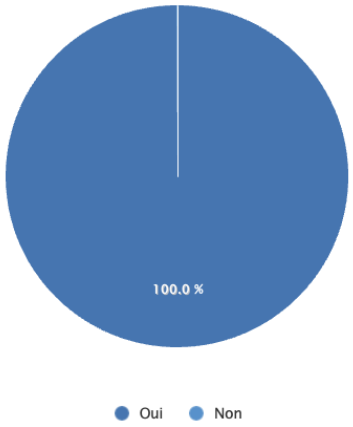
1.16. 10 - La collectivité a-t-elle un Plan Communal de Sauvegarde (PCS) ?

	Nombre	Pourcentage
Oui	2	100%
Non	0	0%
Total	**2**	**100%**



1.17. 10.1 - Ce PCS intègre-t-il les conséquences d'une catastrophe naturelle sur les réseaux d'infrastructures qui sont sur son territoire ? (analyse de risques)

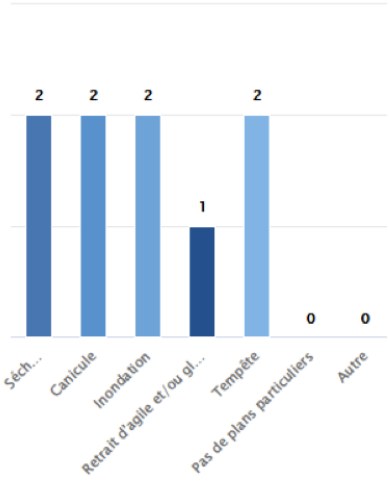
	Nombre	Pourcentage
Oui	2	100%
Non	0	0%
Total	**2**	**100%**



1.18. 11 - La collectivité dispose-t-elle de plans particuliers pour les risques suivants ?

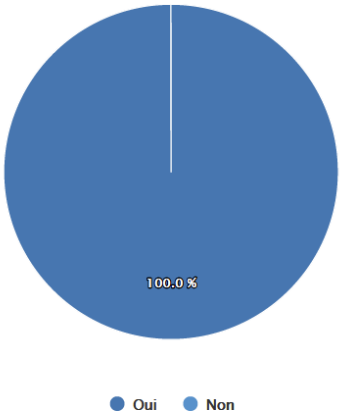
	Nombre	Pourcentage
Sécheresse	2	100%
Canicule	2	100%
Inondation	2	100%
Retrait d'agile et/ou glissement de terrain	1	50%
Tempête	2	100%
Pas de plans particuliers	0	0%
Autre	0	0%
Total	2	100%

Détail des réponses



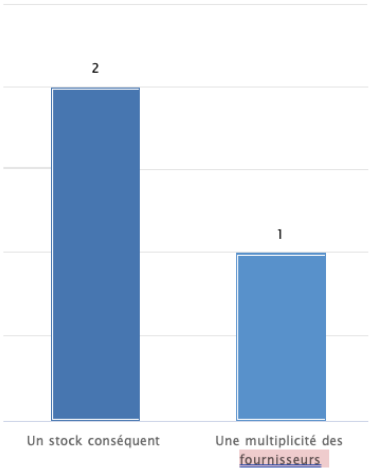
1.19. 12 - La chaine de valeur (supply chain) est-elle assurée pour le maintien en condition opérationnelle des réseaux dont la collectivité à la gestion face à des perturbations majeures ?

	Nombre	Pourcentage
Oui	2	100%
Non	0	0%
Total	2	100%



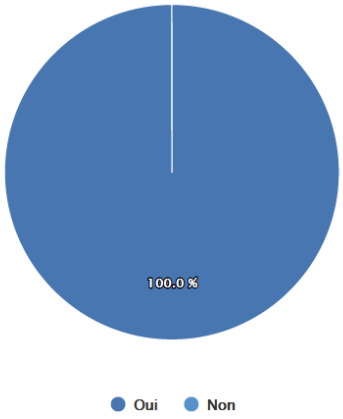
1.20. 12.1 - Ce maintien est assuré par

	Nombre	Pourcentage
Un stock conséquent	2	100%
Une multiplicité des fournisseurs	1	50%
Total	**2**	**100%**



1.21. 13 - La collectivité a-t-elle des partenariats avec d'autres collectivités pour obtenir de l'assistance en cas de crise ?

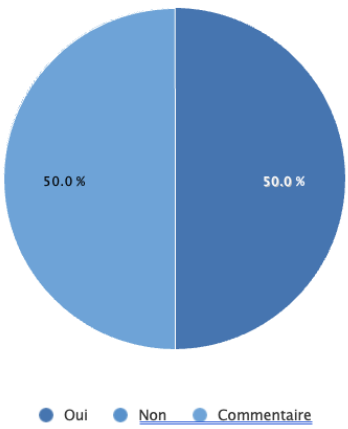
	Nombre	Pourcentage
Oui	2	100%
Non	0	0%
Total	2	100%



1.22. 14 - La collectivité a-t-elle évalué le coût de la préparation à une crise et établi un budget dédié pour les investissements nécessaires (matériel spécifique : radio, informatique,etc..) et le fonctionnement (personnel, alerte, exercice, abonnement etc..) ?

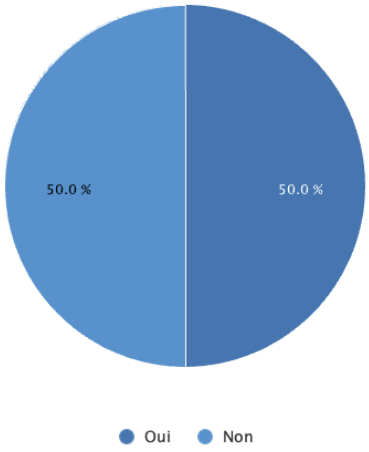
	Nombre	Pourcentage
Oui	1	50%
Non	0	0%
Commentaire	1	50%
Total	**2**	**100%**

Détail des réponses
Identifications budgétaires des coûts qui prennent place dans un débat et des concertations budgétaires plus larges



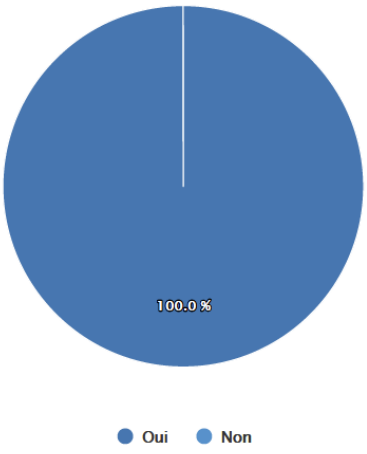
1.23. 15 - La collectivité a-t-elle délégué sa gestion de l'eau potable ?

	Nombre	Pourcentage
Oui	1	50%
Non	1	50%
Total	**2**	**100%**



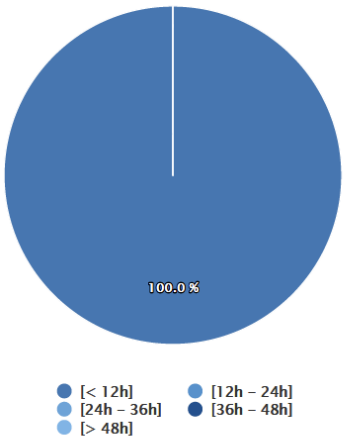
1.24. 15.1 - Ce contrat de délégation prévoit-il une assurance d'approvisionnement en cas de crise ?

	Nombre	Pourcentage
Oui	1	100%
Non	0	0%
Total	1	100%



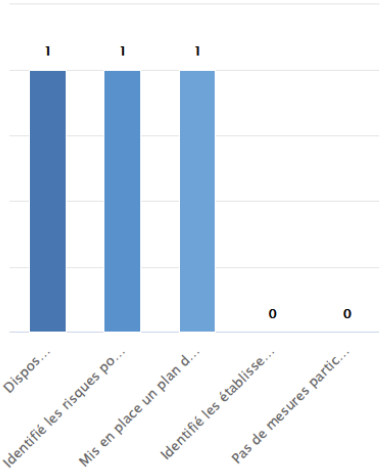
1.25. 15.2 - Quels sont les délais contractuels maximums dans lesquels l'entreprise doit-elle fournir une solution de secours en cas de rupture d'approvisionnement en eau potable ?

	Nombre	Pourcentage
[< 12h]	1	100%
[12h - 24h]	0	0%
[24h - 36h]	0	0%
[36h - 48h]	0	0%
[> 48h]	0	0%
Total	1	100%



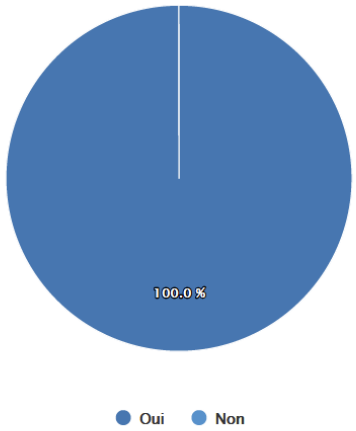
1.26. 15.3 - Concernant l'approvisionnement en eau potable, la collectivité a-t-elle ?

	Nombre	Pourcentage
Dispose d'un système de surveillance et d'alerte pour détecter les incidents	1	100%
Identifié les risques pouvant affecter l'approvisionnement en eau	1	100%
Mis en place un plan d'urgence face à ces risques	1	100%
Identifié les établissements critiques dépendants de l'approvisionnement en eau potable et pris des mesures spécifiques pour assurer leur continuité de service en cas de crise	0	0%
Pas de mesures particulières	0	0%
Total	1	100%



1.27. 16. La collectivité a-t-elle identifié les établissements critiques dépendants de l'approvisionnement en eau potable et pris des mesures spécifiques pour assurer leur continuité de service en cas de crise ?

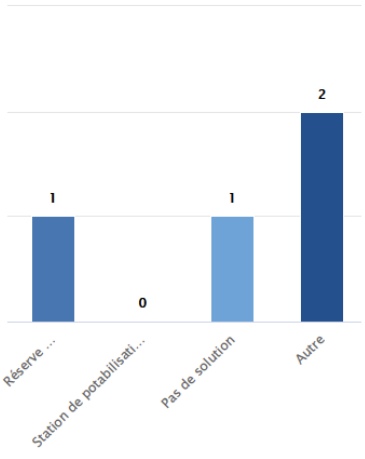
	Nombre	Pourcentage
Oui	2	100%
Non	0	0%
Total	2	100%



1.28. 17 - Comment la collectivité assure-t-elle son approvisionnement en eau potable en cas de crise ?

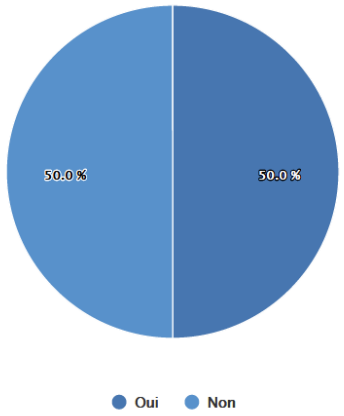
	Nombre	Pourcentage
Réserve d'eau en bouteille	1	50%
Station de potabilisation mobile : Eau potable en sachet	0	0%
Pas de solution	1	50%
Autre	2	100%
Total	2	100%

Détail des réponses
Redondance du réseau
Travail en cours avec la PP et Eau de Paris



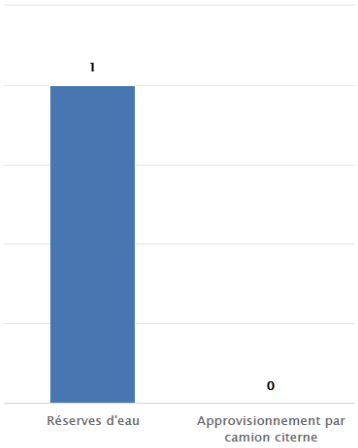
1.29. 18. La collectivité a-t-elle délégué sa gestion d'approvisionnement en eau propre ?

	Nombre	Pourcentage
Oui	1	50%
Non	1	50%
Total	2	100%



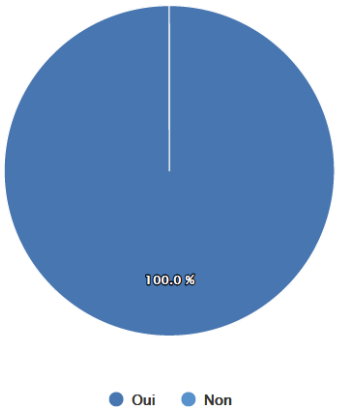
1.30. 18.1 - Concernant l'approvisionnement en eau propre, la commune a-t-elle des solutions en cas de crise ?

	Nombre	Pourcentage
Réserves d'eau	1	100%
Approvisionnement par camion citerne	0	0%
Total	1	100%



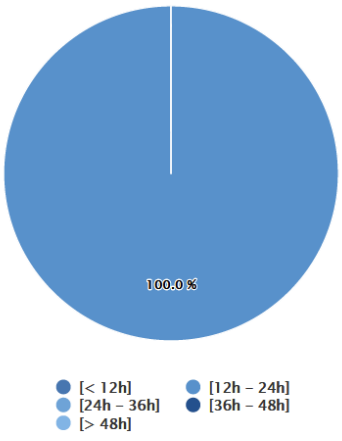
1.31. 18.2 - Ce contrat prévoit-il des solutions d'approvisionnement en eau propre en cas d'événements majeurs ?

	Nombre	Pourcentage
Oui	1	100%
Non	0	0%
Total	1	100%



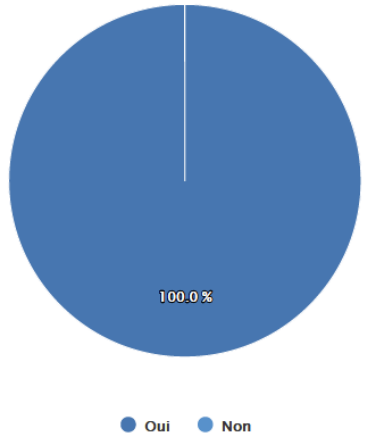
1.32. 18.3 - Quels sont les délais contractuels maximums dans lesquels l'entreprise doit-elle fournir une solution de secours en cas de rupture d'approvisionnement en eau propre ?

	Nombre	Pourcentage
[< 12h]	0	0%
[12h - 24h]	1	100%
[24h - 36h]	0	0%
[36h - 48h]	0	0%
[> 48h]	0	0%
Total	1	100%



1.33. 19 - La collectivité a-t-elle délégué sa gestion de l'assainissement ?

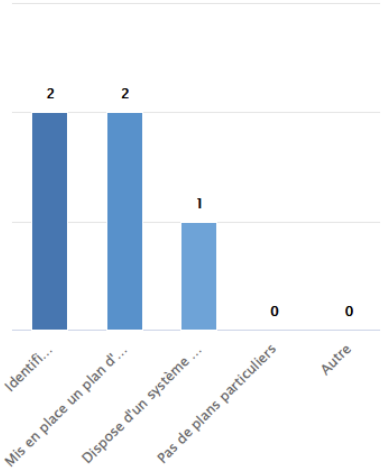
	Nombre	Pourcentage
Oui	2	100%
Non	0	0%
Total	2	100%



1.34. 20 - Concernant la gestion des déchets, la collectivité a-t-elle ?

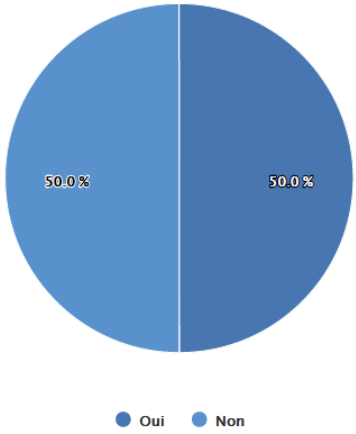
	Nombre	Pourcentage
Identifié les risques pouvant affecter la gestion des déchets	2	100%
Mis en place un plan d'urgence face à ces risques	2	100%
Dispose d'un système de surveillance et d'alerte pour détecter les incidents	1	50%
Pas de plans particuliers	0	0%
Autre	0	0%
Total	2	100%

Détail des réponses



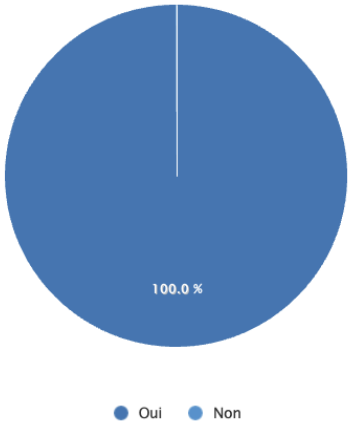
1.35. 21 - La collectivité a-t-elle délégué sa gestion des déchets ?

	Nombre	Pourcentage
Oui	1	50%
Non	1	50%
Total	**2**	**100%**



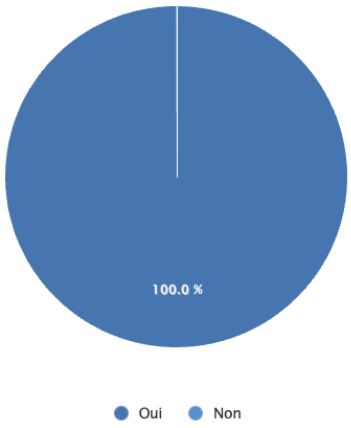
1.36. 21.1 - Cette délégation prévoit-elle que l'entreprise évacue également les déchets post-catastrophes ?

	Nombre	Pourcentage
Oui	2	100%
Non	0	0%
Total	**2**	**100%**



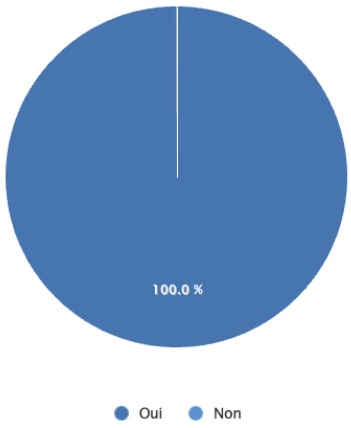
1.37. 21.2 - La délégation prévoit-elle que l'entreprise évacue les déchets ménagers même en cas d'événement majeur ?

	Nombre	Pourcentage
Oui	2	100%
Non	0	0%
Total	**2**	**100%**



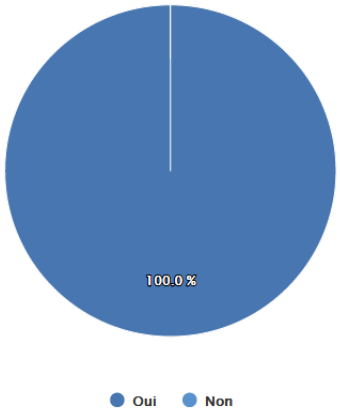
1.38. 21.3 - La collectivité effectue-t-elle des contrôles auprès des entreprises en charge des déchets pour s'assurer que les termes du contrat de délégation sont respectés ?

	Nombre	Pourcentage
Oui	2	100%
Non	0	0%
Total	**2**	**100%**



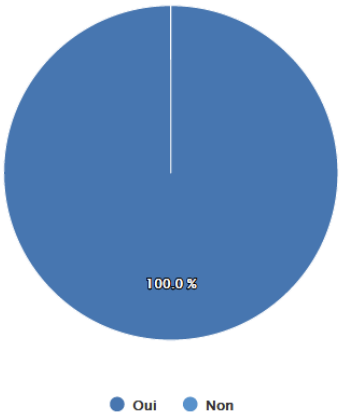
1.39. 21.4 - La collectivité a-t-elle les moyens matériels et humains pour assurer la récupération, l'évacuation et le traitement des déchets post-catastrophes ?

	Nombre	Pourcentage
Oui	1	100%
Non	0	0%
Total	1	100%



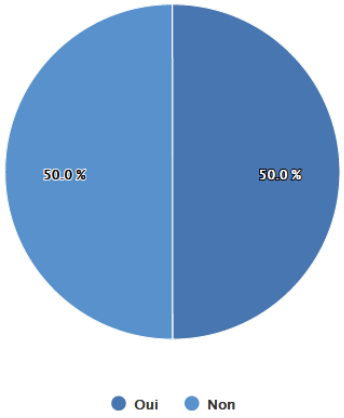
1.40. 21.5 - La collectivité a-t-elle les moyens d'assurer la récupération et le traitement des ordures ménagères y compris lors d'événements majeurs ?

	Nombre	Pourcentage
Oui	1	100%
Non	0	0%
Total	1	100%



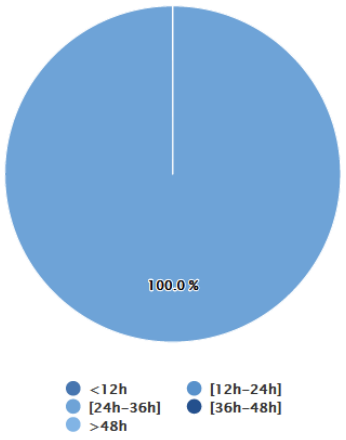
1.41. 22 - En cas de panne électrique, les établissements "critiques" sont-ils alimentés par groupe électrogène ?

	Nombre	Pourcentage
Oui	1	50%
Non	1	50%
Total	2	100%



1.42. 22.1 - Quelle est l'autonomie du groupe éléctrogène ?

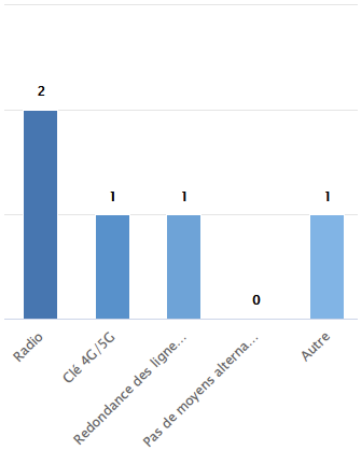
	Nombre	Pourcentage
	0	0%
[12h-24h]	0	0%
[24h-36h]	1	100%
[36h-48h]	0	0%
>48h	0	0%
Total	1	100%



1.43. 23 - En cas de perte de télécommunication, la commune dispose-t-elle de moyens alternatifs ?

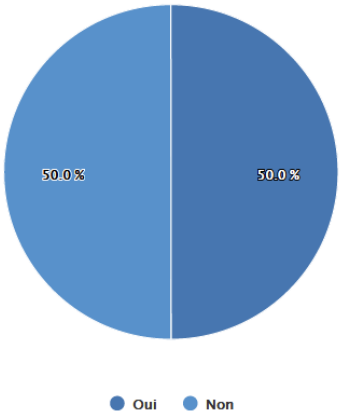
	Nombre	Pourcentage
Radio	2	100%
Clé 4G/5G	1	50%
Redondance des lignes internet (Fibre/ADSL et Satellite)	1	50%
Pas de moyens alternatifs	0	0%
Autre	1	50%
Total	2	100%

Détail des réponses
Redondance des antennes / Fibre sécurisée avec la PP



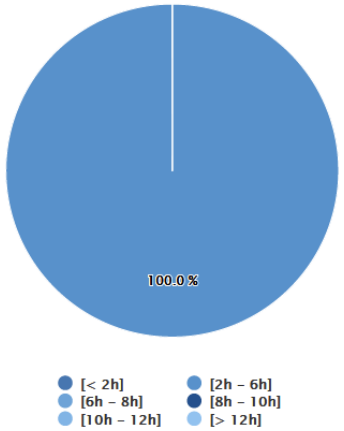
1.44. 24 - Le contrat avec l'opérateur télécom prévoit-il une durée maximum de remise en état des télécommunications en cas d'événement majeur ?

	Nombre	Pourcentage
Oui	1	50%
Non	1	50%
Total	2	100%



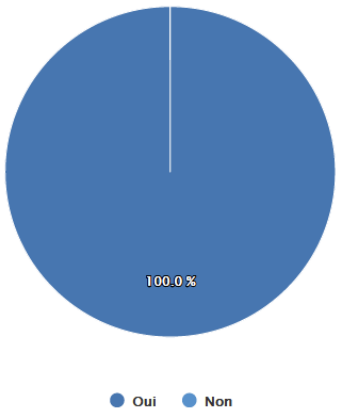
1.45. 24.1 - Quels sont les délais contractuels maximums dans lesquels l'opérateur doit-il fournir une solution de secours en cas de perte de télécommunications ?

	Nombre	Pourcentage
[< 2h]	0	0%
[2h - 6h]	1	100%
[6h - 8h]	0	0%
[8h - 10h]	0	0%
[10h - 12h]	0	0%
[> 12h]	0	0%
Total	1	100%



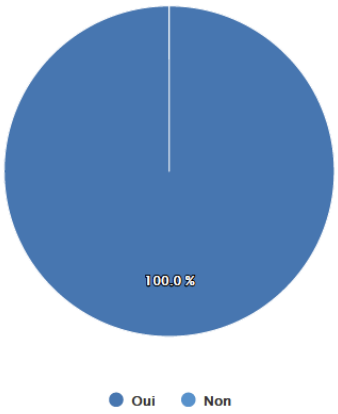
1.46. 25 - La collectivité a-t-elle identifié et cartographié les routes communales sous sa supervision ?

	Nombre	Pourcentage
Oui	2	100%
Non	0	0%
Total	2	100%



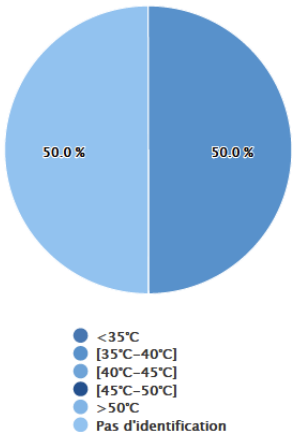
1.47. 25.1 - Parmi ses routes, la collectivité a-t-elle hiérarchisé les voiries pour savoir lesquelles elle doit rétablir en premier lieu ?

	Nombre	Pourcentage
Oui	2	100%
Non	0	0%
Total	2	100%



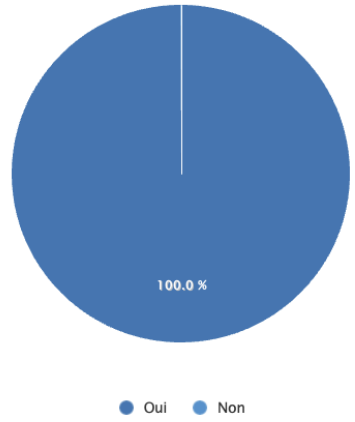
1.48. 26 - La collectivité a-t-elle identifié le seuil en degrés à partir duquel les routes peuvent être endommagées ?

	Nombre	Pourcentage
	0	0%
[35°C-40°C]	1	50%
[40°C-45°C]	0	0%
[45°C-50°C]	0	0%
>50°C	0	0%
Pas d'identification	1	50%
Total	2	100%



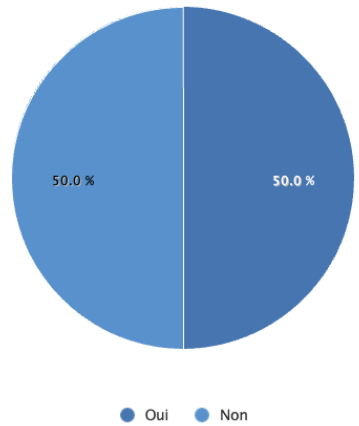
1.49. 27 - La collectivité a-t-elle cartographié les chemins de fers présents sur son territoire ?

	Nombre	Pourcentage
Oui	2	100%
Non	0	0%
Total	**2**	**100%**



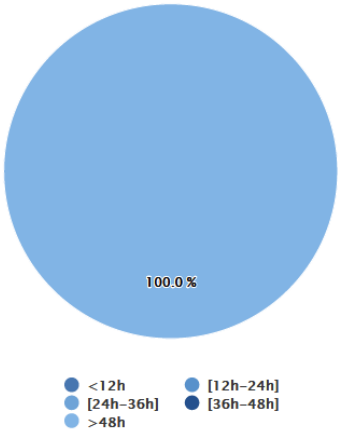
1.50. 28 - La collectivité est-elle en mesure d'approvisionner sa population en nourriture en cas de coupure des voies d'approvisionnement ?

	Nombre	Pourcentage
Oui	1	50%
Non	1	50%
Total	**2**	**100%**



1.51. 28.1 - Pendant quelle durée ?

	Nombre	Pourcentage
	0	0%
[12h-24h]	0	0%
[24h-36h]	0	0%
[36h-48h]	0	0%
>48h	1	100%
Total	1	100%



Fin du questionnaire

Association
Française
pour la Prévention
des Catastrophes
Naturelles et Technologiques

AFPCNT

Mieux comprendre, mieux prévenir

CAHIER DES CHARGES

Objet :

Étude socle en vue de réflexions d'un groupe de travail AFPCNT

sur la résilience des réseaux

Date limite de remise des offres : 20/12/2022 à 14h00

SOMMAIRE

1- Présentation de l'AFPCNT……. 3
2- Contexte général……. 3
3- Périmètre et contenu de la prestation……. 3

1- PRÉSENTATION DE L'AFPCNT

L'Association française pour la prévention des catastrophes naturelles et technologiques est une association régie par la loi du 1er juillet 1901. Elle a été créée fin 2000 pour poursuivre l'action du Comité français de la Décennie internationale de prévention des Catastrophes Naturelles (DIPCN), en tant que centre national de réflexion collective transversale et multirisque sur la problématique des risques naturels et acteur reconnu de la coopération internationale dans ce domaine.

Soutenue par le Ministère de la Transition écologique et de la cohésion des territoires, elle rassemble des scientifiques, experts, universitaires, élus nationaux et locaux, collectivités territoriales, associations, entreprises ainsi que des représentants de l'État.

S'appuyant sur son acquis, face au nouveau contexte mondial des risques et à l'évolution rapide de la gouvernance à tous niveaux, l'AFPCNT vise à constituer une plateforme permanente transversale et multirisques d'acteurs (personnes morales et physiques) impliqués dans la prévention et la gestion des risques de catastrophes et la réduction de leurs conséquences.

Pour ce faire, elle organise des rencontres et des débats, de niveau national, européen et international entre les pouvoirs publics et les divers acteurs de la société civile et se donne pour objectif de déployer de manière équilibrée ses activités suivant les 4 grandes missions suivantes :

- Animation et gestion des réseaux d'acteurs
- Animation scientifique et technique
- Animation territoriale et intersectorielle
- Action internationale et européenne

Plus d'informations sur : www.afcpnt.org

Sur la période 2022-2025, le projet associatif sKarabée vise à développer la culture du risque et de la résilience en France. Il comprend cinq grandes priorités :

- Contribuer à faire du 13 octobre un rdv national incontournable en matière de prévention des risques naturels et technologiques
- Travailler sur la résilience des territoires et des organisations
- Mobiliser et animer le réseau ultramarin
- Favoriser la montée en compétences des acteurs
- Poursuivre les réflexions de fond et développer les partenariats nationaux et internationaux

2- CONTEXTE GÉNÉRAL

Dans le cadre de son projet associatif sKarabée ainsi que de la Convention Pluriannuelle d'Objectifs établie conjointement avec le Ministère, l'AFPCNT se donne pour mission de conforter et de développer les démarches visant à la résilience des territoires et des organisations aux risques majeurs.

Dans cet esprit, l'association prévoit de mettre en place un dispositif de reconnaissance des démarches en faveur de la résilience des territoires et des organisations face aux risques naturels et technologiques. En lien avec le développement d'une approche stratégique de la résilience aux catastrophes naturelles et technologiques sous l'angle du *Build Back Better*, l'AFPCNT souhaite proposer des approches visant à la résilience territoriale des réseaux et des infrastructures. Cette perspective ouvre sur la mise en place d'un groupe de travail.

3- PÉRIMETRE ET CONTENU DE LA PRESTATION

3.1. Périmètre de la prestation d'étude

Les territoires, les entreprises et la population sont fortement tributaires des réseaux en matière d'énergie, de télécommunications, de transports ou de services urbains.

En cas de catastrophe naturelle ou technologique, les réseaux peuvent subir des dommages, entraînant parfois des effets en cascade. Les dégâts subis peuvent s'avérer dommageables et coûteux pour les opérateurs ou les collectivités qui les ont en charge.

Une des catastrophes de forte intensité connue de tous, ayant porté des conséquences dramatiques pour les réseaux a été la tempête Sandy. Les inondations majeures provoquées par cette tempête à New York ont engendré notamment la paralysie des infrastructures souterraines de transport. Ainsi, sept tunnels, huit stations de métro et une gare de triage ont été gravement inondés (EXAMO, 2012).

En France, les tempêtes Lothar et Martin de décembre 1999 ont été fortement destructrices. Elles ont entraîné la rupture d'axes routiers et surtout du réseau électrique. 459 pylônes de haute ou très haute tension, 6 979 supports de moyenne tension et 1 806 km de lignes électriques ont été détruits. Le coût total de réparation a été évalué à environ 1,37 Milliards d'euros (CGEDD, 2013).

En cas de catastrophe, les réseaux locaux peuvent également être endommagés. Pendant l'inondation de Nîmes en 1988, il n'y avait plus ni électricité, ni gaz ni téléphone : 65 000 lignes téléphoniques ont été coupées, 6 km de réseau d'éclairage urbain ont été détruits et 50% des habitants de la ville ont été privés d'eau potable (CEPRI, 2016).

Le temps de rétablissement des réseaux impose une suspension des services et activités ou leur fonctionnement en mode dégradé. Ces conditions complexifient la gestion de crise, aggravent les conditions de vie des citoyens et provoquent des pertes économiques.

Les défaillances des réseaux posent par conséquent des questions aux opérateurs en termes de robustesse de leurs installations et ouvrages et aux gestionnaires des territoires en termes de résilience.

L'AFPCNT s'est de longue date investie sur la question de la défaillance de réseaux.

L'objectif est de réactiver des travaux sur le sujet sur la base d'une analyse actualisée des besoins auxquels il faut répondre en matière de culture du risque et de la résilience.

Dans la perspective de la mise en place d'un nouveau groupe de travail sur le sujet, une prestation d'étude est souhaitée pour éclairer ces besoins.

3.2. Contenu de la prestation d'étude

La prestation consiste en la réalisation d'un état des lieux sur le sujet de la résilience des réseaux et des infrastructures dans un contexte territorial. Cet état des lieux vise à identifier les enjeux et les défis clés aujourd'hui dans ce domaine (notamment à la lumière du retour d'expérience de crises récentes) en tenant compte du changement climatique.

Il s'agira également de recenser quelques approches pragmatiques, concrètes et performantes qu'il serait utile de faire connaître auprès des acteurs des territoires français.

Les réseaux considérés sont les réseaux de transport, d'énergie, de télécommunications et les réseaux urbains : eau, chaleur...

Le contenu de la prestation est décomposé comme suit :

- Réalisation d'une bibliographie nationale et internationale sur la résilience des réseaux face aux risques naturels et technologiques majeurs
- Réalisation de 10 interviews de professionnels sur la base d'un questionnaire à proposer et à valider avec l'AFPCNT
- Rédaction d'un rapport de synthèse illustré
- Participation à des réunions techniques (3 réunions prévues)

3.3. Livrables

A. Synthèse bibliographique

Il est demandé au prestataire d'études de réaliser une analyse bibliographique nationale et internationale ciblée sur les missions de l'AFPCNT de développement de la culture du risque et de la résilience. Cette analyse permettra de disposer d'un premier état des lieux quant aux enseignements de crises récentes et sur des démarches clés pragmatiques, concrètes et performantes d'approche et d'augmentation de la résilience des réseaux et infrastructures. Des études de cas d'exemples emblématiques pourront être insérées.

La liste et les documents sources analysés seront fournis par le prestataire à l'AFPCNT.

Cette analyse couvrira les travaux menés récemment par l'AFPCNT.

L'analyse conduira à la rédaction par le prestataire d'une synthèse bibliographique structurée et illustrée.

B. Interviews

Le prestataire réalisera dix interviews auprès de professionnels œuvrant dans le domaine de la résilience et des réseaux et infrastructures.

La liste de professionnels à interviewer et le projet de questionnaires seront proposés par le prestataire à l'AFPCNT. Les interviews seront ciblées en particulier sur des membres ou des partenaires de l'AFPCNT pertinents sur le sujet.

Les échanges seront enregistrés, avec accord de la personne interviewée. Les enregistrements audios seront la propriété de l'AFPCNT, commanditaire de la prestation.

Chacun des échanges fera l'objet d'une synthèse écrite rédigée par le prestataire et validé auprès du professionnel interviewé.

C. Rapport de synthèse

Le prestataire d'études rédigera un projet de rapport de synthèse global qu'il transmettra ensuite à l'AFPCNT au plus tard trois mois après le début des travaux. Ce rapport établira des propositions d'orientations de travaux à venir dans le champ de l'AFPNCT. Des échanges, des compléments et des consultations organisées par l'AFPCNT permettront de disposer de retours à intégrer par le prestataire dans le rapport de synthèse dans sa version finale.

3.4. Calendrier

L'ensemble de la prestation doit impérativement être produit suivant les délais prévus dans le présent cahier des charges. Le planning récapitulatif sera le suivant :

9 janvier 2023	L'AFPCNT présente le cahier des charges au prestataire
6 mars 2023	Date limite pour remettre le rapport d'état des lieux bibliographique
31 mars 2023	Date limite pour remettre le rapport de restitution des interviews
9 avril 2023	Date limite pour remettre le rapport de synthèse projet
30 avril 2023	Date limite pour remettre le rapport de synthèse final

Les réunions de travail prévues seront programmées d'un commun accord entre l'AFPCNT et le prestataire au fur et à mesure de l'avancement de l'étude.

3.5. Candidatures

Délai de remise des candidatures

Les propositions devront être adressées au plus tard le **20 décembre 2022 à 12h00** impérativement par courriel à l'AFPCNT, commanditaire : contact@afpcnt.org. Passé ce délai, les propositions ne seront pas examinées.

Un courriel de confirmation de réception de l'offre par l'AFPCNT commanditaire sera adressé à chaque candidat. La proposition retenue et les propositions non retenues, feront l'objet d'une information par l'AFPCNT commanditaire dans les mêmes modalités.

Contenu des candidatures

Les propositions devront comprendre une note technique explicitant la façon de travailler et le rendu envisagés ainsi qu'un devis détaillé.

Le montant sera présenté en € HT, avec l'indication de la TVA et de son taux, ainsi que du montant total en € TTC. Le mon

En outre, les candidats pourront joindre à leur offre tout document qu'ils jugeront utile à l'analyse de l'offre (site web, prestation similaire, visuel ou plaquette de présentation…).

Financement disponible : moins de 25,000 euros HT.

Période de réalisation souhaitée : 9 janvier 2023 – 30 avril 2023

3.6. Critères de choix des offres

L'AFPCNT analysera les offres selon les critères de sélection définis dans le règlement de consultation.