Conseil de la radiodiffusion et des télécommunications canadiennes
Canadian Radio-television and Telecommunications Commission
Canada

Rapport sur les points de référence pour l'analyse de la résilience dans les télécommunications

Le 30 juin 2023

RAPPORT SOUMIS PAR : Gartner Canada Co.

Gartner Canada Co.
1565, avenue Carling, Ottawa (Ontario) K1Z 8P9, Canada
www.gartner.com

ISBN : 978-0-660-68925-8
N° de cat.: BC92-128/2023F-PDF

Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC)
Ottawa (Ontario)
Canada
K1A ON2
Téléphone : 819-997-0313
Appel sans frais : 1-877-249-2782 (au Canada uniquement)
https://applications.crtc.gc.ca/contact/fra/librairie

Also available in English.

Un rapport pour Innovation, Sciences et Développement économique Canada (ISDE) et le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC)

Rapport de l’analyse comparative de la résilience des services de télécommunication

Le 30 juin 2023
Mission : 330081153

Table des matières

1.0 Résumé

1.0 Résumé

Dans le cadre du programme de fiabilité des réseaux de télécommunications, Innovation, Sciences et Développement économique Canada (ISDE), en collaboration avec le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC), étudie les approches possibles afin de promouvoir la fiabilité des réseaux de télécommunications.

ISDE et le CRTC ont demandé du soutien pour entreprendre une étude en vue de compiler et d'évaluer les différentes approches des gouvernements étrangers, des organismes de réglementation et de l'industrie afin d'améliorer la fiabilité et la résilience à l'égard de toutes les causes de pannes de réseau. Les obligations réglementaires, les lignes directrices et les mesures de conformité prévues ou prises par les gouvernements étrangers doivent être évaluées afin de déterminer leur applicabilité au Canada.

ISDE, en collaboration avec le CRTC, a demandé à Gartner d'effectuer une analyse comparative indépendante menée par un tiers et de comparer le Canada aux cadres internationaux de fiabilité des télécommunications de certaines administrations.

L'objectif de cette mission était de fournir un ensemble complet d'approches politiques disponibles et appropriées pour une mise en œuvre au Canada. Gartner a apporté son soutien en matière de critères de référence à ISDE dans son analyse des implications de la résilience des services de télécommunication pour le Canada, en réalisant ce qui suit :

- Une étude de marché des pratiques, de la stratégie et de l'approche actuelles en matière de résilience des services de télécommunication pour les gouvernements étrangers d'un maximum de 9 pays (y compris les États-Unis, le Royaume-Uni, l'Australie, la Corée du Sud, la France, l'Allemagne, l'Union européenne, la Nouvelle-Zélande et le Japon) afin de dresser un tableau général et de déterminer les tendances perceptibles.
- Une analyse des pratiques exemplaires en matière de résilience des services de télécommunication pour un sous-ensemble de pays sélectionnés à l'aide de la recherche de Gartner, de 14 consultations dans ces administrations et de données de référence. Les six gouvernements étrangers comprenaient les États-Unis, le Royaume-Uni, l'Australie, l'Union européenne, la Nouvelle-Zélande et le Japon.
- Une évaluation et la prise en compte de la technologie nécessaire afin de permettre l'analyse des tendances, la formulation d'hypothèses et l'analyse des technologies nouvelles et existantes relatives à la résilience des services de télécommunication.

2.0 Introduction

2.0 Introduction

En collaboration avec ISDE et le CRTC, Gartner s'est appuyée sur ses recherches approfondies, ses cadres, ses idées, ses professionnels chevronnés et ses experts mondiaux pour effectuer une comparaison des critères de référence avec les approches en matière de résilience des services de télécommunication d'autres gouvernements étrangers.

Gartner a procédé à des consultations et à une étude de marché à l'aide des bases de données et des recherches de Gartner, et a déterminé les documents de recherche pertinents sur lesquels reposent :

- l'analyse comparative des environnements de télécommunications à l'échelle mondiale en utilisant une approche tous risques (par exemple, catastrophes naturelles, cyberattaques et activités malveillantes, erreurs humaines, erreurs de procédure ou actions de tiers comme des pannes de fibres, d'électricité ou de systèmes).
- l'expérience mondiale fournie par Gartner dans les domaines suivants :
    - les cadres politiques et réglementaires en matière de télécommunications, y compris les cadres relatifs aux infrastructures essentielles, à la gestion des urgences et à la reprise après sinistre.
    - l'architecture et l'exploitation des réseaux de communication (par exemple, réseau filaire, sans fil ou satellitaire).
    - les services d'urgence et leurs architectures de réseau (9-1-1 ou équivalent local, réseaux d'alertes et réseaux nationaux spécialisés, par exemple FirstNet).

2.1 Résilience des services de télécommunication

La résilience des services de télécommunication concerne les pannes et la dégradation des méthodes de communication filaires, sans fil, satellitaires et sous-marines.

Selon la Cybersecurity and Infrastructure Security Agency (CISA) des États-Unis, la résilience des communications signifie qu'un réseau peut résister à des dommages, ce qui réduit la probabilité d'une interruption de service. La résilience est le résultat de trois éléments principaux : la diversité d'acheminement, la redondance et les mesures de protection ou de rétablissement.

Selon l'Union européenne, les réseaux résilients se caractérisent par la fourniture et le maintien d'un niveau de service acceptable face à des défaillances (involontaires, intentionnelles ou d'origine naturelle) qui ont une incidence sur leur fonctionnement habituel. L'objectif principal de la résilience est de rendre les défaillances invisibles pour les utilisateurs. Une liste largement acceptée de risques pour la résilience des réseaux comprend les événements de foule éclair, les cyberattaques, les pannes d'autres services de soutien, les catastrophes naturelles et les défaillances de systèmes.

L'Office of Communications (Ofcom), l'organisme de régulation des services de communication du Royaume-Uni, définit la résilience des communications comme la gestion du risque de perturbation des réseaux publics en matière de disponibilité, de rendement et de fonctionnalité.

Le gouvernement de l'Australie indique que la résilience des réseaux de télécommunications permet de prévenir, d'atténuer et de gérer les pannes en cas d'urgence grâce à l'innovation, au renforcement du réseau, aux connexions par satellite et aux capacités d'infrastructure temporaires.

Selon le Comité consultatif canadien pour la sécurité des télécommunications dans « Résilience des réseaux de télécommunications au Canada : Une voie à suivre » (mars 2023) :

- La résilience et la fiabilité des réseaux exigent que les fournisseurs canadiens de services de télécommunication (FCST) visent à assurer une disponibilité permanente des services, dans la plus large mesure possible, compte tenu des aspects économiques, opérationnels et techniques associés à l'exploitation de réseaux de télécommunications complexes dans le contexte canadien.
- La résilience des réseaux suppose que les FCST cherchent à disposer de mécanismes d'atténuation immédiate des anomalies et de rétablissement rapide pour réduire les répercussions d'un événement indésirable sur la prestation de services en cas de dégradation ou de défaillance de la connexion de première ligne. Ces mécanismes peuvent être passifs ou actifs.
- Les FCST devraient également s'efforcer d'assurer, lorsque cela est possible, le déploiement et la maintenance de réseaux de communication résilients pour le personnel de rétablissement d'urgence (p. ex., opérations d'urgence, centres d'exploitation du réseau et autres membres du personnel du FCST participant aux interventions d'urgence).
- Il s'agit notamment de tenter d'établir des partenariats fiables entre un FCST et tout fournisseur tiers qui pourrait participer à la prestation du service de communication d'un FCST.
- De plus, les FCST doivent se soutenir mutuellement, lorsque cela est possible, en cas de besoin, en vue de préserver la connectivité de l'ensemble des utilisateurs du système de télécommunications du Canada.

2.2 Analyse comparative des pratiques exemplaires

L'analyse comparative des pratiques exemplaires en matière de résilience des services de télécommunication comprend les éléments suivants :

- La détermination des pratiques exemplaires qui pourraient remplacer la réglementation en vue de prévenir ou réduire les pannes des réseaux de télécommunications; ainsi que les obligations réglementaires.

2.3 Buts et objectifs du rapport final

Le but du rapport final et l'objectif de l'évaluation étaient les suivants :

- Fournir un support en matière de critères de référence à ISDE et au CRTC dans le cadre de leur analyse des implications de la résilience des services de télécommunication pour le Canada.

2.4 Secteur des technologies de l'information et des communications

Pour les besoins de cette évaluation, il est important de comprendre le contexte et la définition du secteur des technologies de l'information et des communications (TIC). Gartner a évalué un type particulier de fournisseurs dans le domaine des TIC. Ils ne doivent pas être considérés comme les seuls organismes ou fournisseurs susceptibles d'influencer ou de soutenir la résilience des services de télécommunication, mais ils seraient considérés comme les principaux fournisseurs de services de télécommunication dans les administrations analysées.

Dans le cadre de ce rapport, le secteur des fournisseurs de services de télécommunication a été classé en quatre catégories en fonction du type d'infrastructure de communication :

- **Réseau sans fil :** réseaux de communication qui transfèrent des données entre des nœuds sans utiliser de fils, en s'appuyant généralement sur des radiofréquences.
- **Réseau filaire – terrestre :** réseaux de communication qui utilisent des câbles physiques et des fibres sur terre pour transférer des données entre les nœuds de communication.
- **Réseau filaire – sous-marin :** réseaux de communication qui utilisent des câbles physiques et des fibres sous la mer pour transférer des données entre les nœuds de communication.
- **Réseau satellitaire :** réseaux de communication qui utilisent des satellites en orbite autour de la Terre pour transférer des données entre les nœuds de communication.

3.0 Méthodologie

3.0 Méthodologie

Pour cette mission, Gartner a réalisé une évaluation comparative et une étude de marché des pratiques, de la stratégie et de l'approche actuelles en matière de résilience des services de télécommunication pour les gouvernements étrangers de neuf pays et administrations. Ces administrations comprenaient les États-Unis, le Royaume-Uni, l'Australie, la Corée du Sud, la France, l'Allemagne, l'Union européenne, la Nouvelle-Zélande et le Japon.

Plus loin dans le rapport, l'analyse se penchera plus en détail sur un sous-ensemble de la grande liste des administrations, en procédant à une évaluation comparative des règlements, de la législation et des autres méthodes nécessaires en vue de prévenir ou réduire les pannes des réseaux de télécommunications, des codes de conduite volontaires, des normes et des pratiques exemplaires.

3.1 Collecte de données

L'approche consistait à rassembler des données de haut niveau sur les neuf pays à partir de sources multiples afin de dresser un tableau général et de déterminer les tendances perceptibles. Les méthodes utilisées et les sources référencées pour cette étude comprennent :

- des entretiens directs avec les parties prenantes des organismes de réglementation des pays respectifs. Ces parties prenantes comprenaient des personnes actuellement « en fonction » qui sont employées activement par l'administration, les organismes de réglementation ou les organismes qui influencent les organismes de réglementation, ainsi que des personnes qui ont précédemment occupé des fonctions au sein de ces organismes.
- Des documents officiels publiés par les organismes de réglementation des pays cibles.
- Des rapports et articles de sources secondaires.

3.1.1 Profils des administrations

Les caractéristiques non liées aux télécommunications de chaque administration ont également été recueillies afin de fournir un contexte de référence pour les comparaisons analytiques. Ces caractéristiques comprennent la population, la superficie, la densité de population, le littoral, les caractéristiques géographiques, le nombre de fournisseurs de services de télécommunication (FST), et bien d'autres.

Tableau 1. Mission sur la priorité accordée aux TIC – Fournisseurs de services de télécommunication

								Union européenne	
	Canada	**Australie**	**États-Unis**	**Royaume-Uni**	**Nouvelle-Zélande**	**Japon**	**Corée du Sud**	**Allemagne**	**France**
Population (en millions [M])	39 M	26 M	340 M	68 M	5 M	123 M	52 M	83 M	65 M
Superficie (km^2)	**10,0 M**	**7,7 M**	**9,4 M**	0,24 M	0,27 M	0,38 M	0,10 M	0,36 M	0,55 M
Densité (/km^2)	**4**	**3**	37	280	20	338	531	238	118
Connexions sous-marines	**21**	23	90	59	8	32	11	8	29
Nombre de FST	4+	4+	3+	4+	3+	4+	3+	4+	4+

Sources : Population mondiale par pays en 2023 (en direct), The World Factbook

- La superficie du Canada n'est comparable qu'à celles des États-Unis et de l'Australie, où la couverture du réseau, et donc la redondance, devient plus préoccupante en raison de l'étendue du territoire à traverser.
- La densité relative du Canada correspond davantage à celles de l'Australie et de la Nouvelle-Zélande et se prête à des défis semblables en matière d'interruptions pour des facteurs environnementaux potentielles afin de promouvoir la résilience dans les zones à faible ou très faible densité.
- Le Canada dispose d'un nombre modéré de connexions sous-marines par rapport à d'autres pays, ce qui permet une redondance au cas où une ou plusieurs connexions seraient compromises en même temps.

À titre de référence, les caractéristiques du Canada sont les suivantes :

- **Population** : Avec 39 millions d'habitants, il est plus petit que la plupart des pays analysés.
- **Masse terrestre** : Avec 10,0 millions de km^2, il est plus grand que tous les pays analysés.
- **Densité** : Avec 4/km^2, il est moins dense que la plupart des pays analysés.
- **Littoral** : Avec 202 080 km, il est presque 10 fois plus grand que celui de tout autre pays analysé.
- **Caractéristiques géographiques** : La géographie diversifiée du Canada comprend presque toutes les caractéristiques géographiques des autres administrations analysées, ce qui en fait la plus complexe.
- Les plus grands fournisseurs de services de télécommunication (FST) au Canada :
    - Bell Canada, TELUS, Rogers-Shaw et Québecor, qui contrôlent plus de 90 % du secteur des télécommunications du pays.
    - Il existe quelques entreprises régionales, dont Vidéotron, SaskTel et Eastlink.
    - La plupart des administrations analysées ont de trois à cinq grands FST, ainsi que de nombreux sous-fournisseurs.

Remarque : L'Union européenne est actuellement composée de 27 États membres, dont l'Autriche, la Belgique, la Bulgarie, la Croatie, la République de Chypre, la République tchèque, le Danemark, l'Estonie, la Finlande, la France, l'Allemagne, la Grèce, la Hongrie, l'Irlande, l'Italie, la Lettonie, la Lituanie, le Luxembourg, Malte, les Pays-Bas, la Pologne, le Portugal, la Roumanie, la Slovaquie, la Slovénie, l'Espagne et la Suède.

3.1.2 Structure organisationnelle et gouvernance

Des informations relatives aux mandats et à la structure de gouvernance des organismes de réglementation ont été recueillies pour chaque administration afin de fournir un contexte de référence pour les comparaisons analytiques. La plupart des administrations disposent d'organismes de réglementation ou d'organes de surveillance qui rendent compte directement au gouvernement.

Tableau 2. Structures organisationnelles et gouvernance

Admin.	Organisme de réglementation	Mandat	Gouvernance
Canada	Innovation, Sciences et Développement économique Canada (ISDE)	Responsable de la *Loi sur les télécommunications*, et dans ce contexte, le ministère est chargé de réglementer le spectre, les équipements de télécommunications, les câbles sous-marins internationaux et les cadres de réglementation des satellites, ainsi que de collaborer avec des organismes des secteurs public et privé sur la résilience des infrastructures de télécommunications.	Ministère fédéral qui rend compte au Parlement du Canada.
	Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC)	Réglemente et surveille la radiodiffusion et les télécommunications dans l'intérêt du public. Le CRTC est résolu à veiller à ce que les Canadiens aient accès à un système de communication de classe mondiale qui encourage l'innovation et enrichit leur vie.	Organisme indépendant qui rend compte au Parlement du Canada.
	Centre canadien pour la cybersécurité (CCC)	Source unifiée d'avis, de conseils, de services et de soutien en matière de cybersécurité pour le gouvernement, le secteur privé, les Canadiens ainsi que les propriétaires et les exploitants d'infrastructures essentielles. Le Centre pour la cybersécurité fait partie du Centre de la sécurité des télécommunications (CST).	Ministère fédéral rend compte au Parlement du Canada.
États-Unis	Commission fédérale des communications (FCC)	Réglemente les communications interétatiques et internationales par radio, télévision, fil, satellite et câble dans les 50 États, dans le District de Columbia et dans les territoires des États-Unis. (À propos de la FCC)	Organisme indépendant, soumis au contrôle du Congrès.

Admin.	Organisme de réglementation	Mandat	Gouvernance
	Cybersecurity and Infrastructure Security Agency (CISA)	Responsable opérationnel de la cybersécurité à l'échelle du gouvernement fédéral et coordinateur national pour la sécurité et la résilience des infrastructures essentielles. Collabore avec des partenaires pour se défendre contre les menaces actuelles et pour mettre en place une infrastructure plus sûre et plus résistante pour l'avenir. (À propos de la CISA)	Composante opérationnelle du département de la Sécurité intérieure.
	National Telecommunications and Information Administration (NTIA)	Responsable en vertu de la loi de conseiller le président sur les questions de politique en matière de télécommunications et d'information, il se concentre sur l'accès à Internet haute vitesse et son adoption en Amérique, sur l'extension de l'utilisation du spectre par tous les utilisateurs et sur la garantie qu'Internet reste un moteur d'innovation continue et de croissance économique. (À propos de la NTIA)	Agence du pouvoir exécutif située au sein du département du Commerce.
Royaume-Uni	Office of Communications (Ofcom)	Responsable de la réglementation des secteurs de la télévision, de la radio et de la vidéo sur demande, des entreprises de services de télécommunications de lignes fixes, de la téléphonie mobile, des services postaux et du spectre. (Qui est l'Ofcom?)	Organisme indépendant qui rend compte au Parlement britannique.
	Ministère de la Science, de l'Innovation et de la Technologie (MSIT)	Responsable du positionnement du Royaume-Uni à l'avant-garde du progrès scientifique et technologique mondial, de la stimulation d'innovations qui changent des vies et soutiennent la croissance économique, de la mise en œuvre de programmes pour les talents, de l'infrastructure physique et numérique et de la réglementation pour soutenir l'économie, la sécurité et les services publics du Royaume-Uni. (MSIT)	Ministère fédéral qui rend compte au Parlement britannique.
	National Cyber Security Centre (NCSC)	Responsable de la fourniture de conseils et de soutien aux secteurs public et privé sur la manière d'éviter les menaces à la sécurité informatique. Il a été créé à partir	Son organisme mère est l'agence de renseignement et de sécurité du Royaume-Uni (Governement

Admin.	Organisme de réglementation	Mandat	Gouvernance
		d'un certain nombre d'organismes préexistants, notamment : Centre for Cyber Assessment (CSA), Computer Emergency Response Team UK (CERT UK), Cyber Security Information Sharing Partnership (CISP) et CovCertUK.	Communications Headquarters ou GCHQ).
Australie	Australian Competition and Consumer Commission (ACCC)	Responsable de l'application de la *Competition and Consumer Act 2010* et d'autres lois, de la promotion de la concurrence, du commerce équitable et de la régulation de l'infrastructure nationale dans l'intérêt de tous les Australiens. (À propos de l'ACCC)	Autorité statutaire indépendante du Commonwealth, sous la responsabilité du portefeuille du Trésor.
	Australian Communications and Media Authority (ACMA)	Responsable de la réglementation de la radiodiffusion, des radiocommunications, des télécommunications et du contenu en ligne. Sa gouvernance et ses fonctions sont prescrites par la *Australian Communications and Media Authority Act 2005*. (Déclaration d'intention de l'ACMA)	Autorité statutaire indépendante du Commonwealth qui rend compte au Parlement australien.
Nouvelle-Zélande	New Zealand Infrastructure Commission	Deux fonctions principales prévues par la *Telecommunications Act 2001* qui contribuent à garantir la concurrence des marchés de la large bande et de la téléphonie mobile. La première consiste à réglementer certains services de téléphonie fixe et mobile en fixant le prix ou les conditions d'accès à ces services. La seconde consiste à surveiller la concurrence, le rendement et l'évolution des marchés des télécommunications et à en rendre compte. (*NZIC/Te Waihanga Act* 2019)	Entité indépendante de la Couronne qui rend compte au Parlement de la Nouvelle-Zélande.
Japon	Ministère des Affaires intérieures et des Communications (MAIC)	Responsable de la gestion et de l'administration du système administratif de base du pays, de l'administration de l'autonomie locale, des services d'urgence et de l'application des stratégies de croissance des TIC.	Responsable devant le cabinet du premier ministre.
Corée du Sud	Ministère des Sciences et des Technologies de l'information et des communications (MSTIC)	Responsable de promouvoir une croissance économique inclusive au moyen d'une innovation et d'une transformation technologiques continues, en partenariat avec la société civile. (Informations sur le MSIT)	Il rend compte directement au président de la Corée du Sud.

Admin.	Organisme de réglementation	Mandat	Gouvernance
Allemagne	Bundesnetzagentur (BNetzA)	Responsable de l'établissement des conditions générales d'une concurrence loyale dans les secteurs de l'électricité, du gaz, des télécommunications et des infrastructures postales, et du rôle d'autorité de surveillance. (À propos de BNetzA)	Autorité fédérale indépendante, qui rend compte directement au ministère fédéral des Affaires économiques et de l'Énergie.
France	Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP)	Responsable de la régulation des communications électroniques, du secteur postal et de la distribution de la presse. Architecte et gardienne des réseaux Internet, fixes, mobiles et postaux en France, l'ARCEP veille à ce que ces réseaux se développent comme un « bien commun ». (ARCEP)	Autorité administrative indépendante (AAI), qui rend compte au Parlement français.
Union européenne	Agence de l'Union européenne pour la cybersécurité (ENISA)	Responsable du renforcement de la coopération opérationnelle au sein de l'Union européenne, de l'aide aux États membres de l'Union européenne qui le souhaitent pour gérer leurs incidents de cybersécurité et du soutien à la coordination de l'Union européenne en cas de cyberattaques et de crises transfrontalières de grande ampleur.	▪ Le conseil d'administration (CA) est composé de représentants des États membres et de la Commission européenne. ▪ Le conseil exécutif est composé de cinq membres du CA et est présidé par le président du CA. ▪ Le conseil exécutif élabore les décisions pour adoption par le CA sur les questions administratives et budgétaires et se réunit une fois tous les trois mois.
	Organe des régulateurs européens des communications électroniques (ORECE)	Responsable de la mise en œuvre cohérente du Cadre réglementaire de l'Union européenne pour les communications électroniques.	Organisme indépendant de l'Union européenne, qui rend compte à la Commission européenne.

3.1.3 Fournisseurs de services de communication des administrations

Les principaux fournisseurs de services de télécommunication dans chaque administration sont les suivants :

- Canada 4+

- Rogers
- Bell
- TELUS
- Québecor

- États-Unis 3+
  - AT&T
  - Verizon
  - T-Mobile (Sprint fait partie de T-Mobile)
- Royaume-Uni 4+
  - BT Group
  - Sky
  - Virgin Media
  - TalkTalk
- Australie 4+
  - Telstra Corporation Limited
  - Optus
  - Vodafone Hutchison Australia (VHA)
  - TPG Telecommunications Limited
- Nouvelle-Zélande 3+
  - Spark New Zealand
  - Vodafone New Zealand
  - 2degrees
- Japon 4+
  - NTT Group
  - KDDI Corporation
  - SoftBank Corp.
  - Rakuten Mobile
- Corée du Sud 3+
  - SK Télécommunications
  - KT Corporation (anciennement connu sous le nom de Korea Telecommunications)
  - LG Uplus
- Allemagne 4+
  - Deutsche Telekom AG
  - Vodafone Germany
  - Telefonica Germany (O2 – opérant sous la marque O2)
  - 1&1 Drillisch AG
- France 4+
  - Orange (anciennement France Télécom)
  - SFR (Société française du radiotéléphone)
  - Bouygues Telecom
  - Free

3.1.4 Couverture du réseau de l'administration

Contrairement aux réseaux sans fil, qui nécessitent une alimentation continue en électricité au moyen d'une infrastructure de transmission (contiguë), mais qui peuvent également exister en utilisant une infrastructure de transmission intermittente, les réseaux filaires nécessitent à la fois

une alimentation électrique et une infrastructure physique contiguë sous la forme de câbles afin de soutenir les capacités de transmission. Il est donc difficile pour les pays qui ont une grande superficie et une géographie variée ou des archipels de parvenir à une couverture universelle.

Les plus grands pays de cette liste – **Canada**, **États-Unis** et **Australie** – sont encore loin d'avoir atteint la couverture universelle. Aux États-Unis, de nombreuses régions du nord du Midwest, comme le Montana, le Dakota et le Wyoming, ne sont pas encore couvertes par la fibre à large bande. L'Alaska, avec son terrain difficile, ses conditions météorologiques et sa faible densité, est presque entièrement dépourvu de fibre et dépend des technologies satellitaires et sans fil.

De même, l'Australie possède de vastes zones intérieures arides où vivent de petites collectivités rurales agraires isolées qui n'ont pas de couverture à large bande. Malgré cela, les deux pays sont bien couverts, car une grande majorité de la population a accès à la large bande.

Le Canada présente des similitudes avec les États-Unis et l'Australie. De nombreuses régions du nord de plusieurs provinces, ainsi que du Yukon, des Territoires du Nord-Ouest et du Nunavut, ne sont pas couvertes par la fibre. Même dans certaines de ces régions, l'utilisation du satellite et du sans fil peut s'avérer difficile en raison du terrain et de l'environnement.

En revanche, au **Royaume-Uni**, plus de 90 % de la population est couverte par la fibre. Les 5 à 10 % restants de la population vivent dans des collectivités rurales et le gouvernement travaille à l'octroi de subventions et d'incitatifs aux opérateurs privés pour les couvrir, tout en envisageant la création d'un réseau public de fibres pour offrir une couverture universelle.

Ce sont 92 % de la masse continentale du Royaume-Uni qui sont couverts par un bon signal 4G en provenance d'au moins un opérateur de réseau mobile, tandis que 70 % du pays est couvert par les quatre opérateurs. La couverture 5G est désormais disponible auprès d'au moins un opérateur pour au moins 77 % des locaux.

La vitesse du réseau dans les zones couvertes est élevée. En janvier 2022, 64 % des locaux du Royaume-Uni disposaient d'une connexion à large bande avec une vitesse de téléchargement d'au moins un gigabit par seconde, selon l'Ofcom, l'organisme de régulation des entreprises de télécommunications.

En **Allemagne** et en **France** (à l'exclusion des territoires français d'outre-mer), avec une topographie généralement douce et une répartition relativement uniforme de la population dans les campagnes, se targue d'avoir la meilleure couverture de câbles à large bande, avec une distribution universelle dans l'ensemble du pays, malgré quelques zones montagneuses dans les Alpes.

Le **Japon** et la **Nouvelle-Zélande** ont la plus grande partie de leur population dans deux ou trois grandes îles (la Nouvelle-Zélande en a deux et le Japon trois). Il y a de grandes agglomérations autour des centres importants et des régions intérieures vallonnées avec une faible densité de population et des zones essentiellement rurales. Malgré cela, les deux pays ont réussi à atteindre un taux de pénétration élevé des services à large bande (le Japon a un taux de couverture de 99,1 % des ménages et seuls 530 000 ménages ne sont pas couverts, tandis que la Nouvelle-Zélande compte réduire le nombre de ménages non couverts à 10 000 au cours des deux prochaines années).

La **Corée du Sud** ressemble au Royaume-Uni, avec une petite masse continentale et une population essentiellement concentrée autour de la ville de Séoul. En raison de la forte concentration et de l'urbanisation de sa population, la Corée du Sud bénéficie de taux de pénétration très élevés dans tous les segments des télécommunications : téléphonie fixe (44 %

au début de 2022), large bande fixe (46 %), téléphonie et données mobiles (144 %) et large bande mobile (120 %). 1 2

Historiquement, la Corée du Sud s'est vantée d'avoir certaines des vitesses de téléchargement à haute vitesse les plus rapides au monde (deuxième en 2019 et quatrième en 2020). Cependant, selon le site de mesure de la vitesse Internet Speedtest, en novembre 2023, la vitesse moyenne de téléchargement à large bande de la Corée du Sud était de 171,12 mégabits par seconde (Mbps), au 34e rang mondial. Le recul de la Corée dans le classement des vitesses de téléchargement à large bande a été attribué au fait que l'infrastructure filaire du pays a été construite à l'aide de câbles hybrides de fibres optiques et de câbles coaxiaux de moins bonne qualité, alors que les pays qui ont commencé à construire leurs réseaux après la Corée du Sud ont bénéficié de la mise en place de câbles à fibres optiques plus rapides.

3.1.5 Catégories de pannes

Lors de la collecte des données, Gartner a rassemblé et validé les catégories de pannes suivantes :

- Facteurs environnementaux : catastrophes naturelles, conditions météorologiques, feux de forêt, inondations, etc.
- Erreurs opérationnelles : erreurs de configuration, erreurs de procédure, redondance insuffisante
- Cybersécurité : déni de service distribué (DDoS), rançongiciel, cyberattaques, autres activités malveillantes
- Facteurs tiers : dépendances du système
- Dommages involontaires ou intentionnels : coupures de fibres, dommages causés par des animaux, coupures de câbles sous-marins
- Autres menaces ou causes (non définies)

Il est évident que les administrations ont des objectifs et des champs d'action différents en matière de résilience, influencés par des différences géographiques, économiques, politiques et démographiques.

3.1.6 Pannes de réseau et défaillances

Analyse de la couverture médiatique

- Dans le cadre des recherches effectuées pour le présent rapport, une étude a été menée sur les événements récents de panne ou de dégradation survenus dans les différentes administrations.
- Portée de l'examen :
    - Événements survenus entre 2018 et 2023.

[1] Why Korea fell 27 spots in world internet speed rankings to 32nd place last year : National : News : The Hankyoreh (hani.co.kr)

[2] Korea's internet speed ranking falls to 34th: report - The Korea Times

    - Couverture dans les sources accessibles au public
        - Médias et rapports publiés par les organismes de réglementation.

- Les informations relatives à chaque événement comprennent plusieurs éléments :
    - Cause de l'événement (erreurs opérationnelles, facteurs environnementaux, cybersécurité, facteurs tiers, dommages involontaires ou intentionnels).
    - Type d'infrastructure touchée (sans fil, filaire – terrestre, filaire – sous-marine ou satellitaire).
    - Durée de la panne et mesures de rétablissement.
    - Résultats ou mesures réglementaires.

Résumé des conclusions relatives aux types de pannes :

- Les types d'infrastructures les plus touchés sont les infrastructures terrestres sans fil et filaires.
    - La raison principale est le plus souvent des erreurs opérationnelles, suivies par des dommages aux câbles ou intentionnels.
- Les événements relatifs aux infrastructures sous-marines et satellitaires ont été moins fréquents.

3.2 Analyse approfondie et évaluation comparative

Gartner a approfondi et élargi la collecte de données pour un sous-ensemble de la grande liste des administrations, en réalisant une évaluation comparative des réglementations, de la législation et des autres méthodes nécessaires en vue de prévenir ou réduire les pannes des réseaux de télécommunications, des codes de conduite volontaires, des normes et des pratiques exemplaires. Ce sous-ensemble comprenait les États-Unis, le Royaume-Uni, l'Australie, la Nouvelle-Zélande, le Japon et l'Union européenne.

3.2.1 Facteurs pour l'amélioration de la résilience du réseau

Gartner a évalué les pannes de réseau et les défaillances qui ont eu une incidence sur la vie et les activités des clients qui reçoivent des services de communication afin de déterminer les facteurs ou mesures qui ont influencé ou amélioré la résilience du réseau. Cette évaluation comprend les éléments suivants :

- Facteurs gouvernementaux (par exemple, le respect de la réglementation nationale en matière de télécommunications, l'encouragement aux investissements, la sécurité publique et les interventions d'urgence).
- Facteurs de l'industrie (par exemple, la concurrence, la qualité du service, la fiabilité).
- Autres facteurs (environnementaux ou sociétaux)

Ces facteurs seront présentés plus en détail dans les sections suivantes.

3.2.1.1 Facteurs gouvernementaux pour l'amélioration de la résilience

Facteurs gouvernementaux pour l'amélioration de la résilience des services de télécommunication

La plupart des administrations disposent d'une législation qui impose un cadre de déclaration obligatoire des incidents en cas de pannes ou de défaillance des services. Toutefois, certaines administrations cherchent à renforcer la législation et la réglementation afin de combler les lacunes de la prestation des fournisseurs de services dues à des pannes ou des incidents qui auraient pu être évités.

Tableau 3. Principaux enseignements des facteurs gouvernementaux pour l'amélioration de la résilience des services de télécommunication

Champ d'application défini pour les fournisseurs de services de communication visés	▪ Les critères de catégorisation pour déterminer quels fournisseurs sont inclus dans le champ d'application du cadre de déclaration obligatoire sont généralement basés sur le type de service fourni ou d'infrastructure utilisée (par exemple, satellite, voix sans fil, données sans fil, réseau fixe). ▪ Par exemple, le cadre de l'Allemagne prévoit des exigences en matière de déclaration pour les opérateurs des infrastructures essentielles qui sont définies par type de réseau ou système (par exemple, réseau d'accès, réseau fédérateur, station d'atterrissage de câbles sous-marins, centre de données).
Seuils des pannes ou d'incidents	▪ Les cadres établissent des seuils relatifs à la déclaration par type d'incident (par exemple, la cybersécurité, les appels d'urgence) ou l'impact global de l'incident, généralement calculé en multipliant le nombre de clients touchés par la durée totale de la panne.
Délais de déclaration définis	▪ Les délais de déclaration varient d'une administration à l'autre, d'un cadre à l'autre et d'un type d'incident à l'autre. Toutefois : o Un premier avis à l'organisme de régulation est généralement requis dans un délai d'une à trois heures. o Dans la plupart des cas, les délais sont calculés en multipliant le nombre de personnes touchées par la durée de la panne. o Un rapport initial est généralement requis dans un délai de deux à trois jours, et le rapport final doit être remis dans un délai d'un mois.
Mise en œuvre en cas de non-conformité	▪ La plupart des administrations disposent d'une réglementation qui sanctionne les FST par des sanctions administratives pécuniaires (SAP) ou des sanctions financières en cas de non-conformité des obligations de service ou des exigences en matière de déclaration. ▪ Les sanctions imposées aux fournisseurs sont généralement déterminées en fonction des répercussions sur les consommateurs (types de services touchés, nombre de clients concernés et durée de l'événement) et du niveau de négligence (y a-t-il eu violation des pratiques exemplaires).

Facteurs pour l'amélioration de la puissance et de la résilience du réseau

L'amélioration de la puissance et de la résilience du réseau est le plus souvent motivée par la réponse aux pannes causées par des catastrophes naturelles ou des pannes d'électricité.

Tableau 4. Principaux enseignements des facteurs pour l'amélioration de la puissance et de la résilience du réseau

Batteries de secours	▪ Dans le cadre du Programme de renforcement des réseaux mobiles (*Mobile Network Hardening Program*) et du Programme de renforcement des télécommunications contre les catastrophes naturelles (*Strengthening Telecommunications Against Natural Disasters Program*), l'Australie a investi dans l'amélioration de l'alimentation par batterie de secours de 467 stations de base du réseau. ▪ Le Japon a mis en place des systèmes d'alimentation de secours obligatoires (alimentation sans interruption et génératrices de secours) pour se protéger contre les pannes causées par les tremblements de terre et les tsunamis.
Infrastructure déployable	▪ Pour contrer les pannes relatives aux feux de brousse, l'Australie a investi dans des infrastructures déployables comme des cellules sur roues, des centraux mobiles sur roues et des camions Road Muster du Réseau national à large bande (*National Broadband Network*).
Renforcement du site physique	▪ Dans le cadre du Programme de renforcement des réseaux mobiles (*Mobile Network Hardening Program*) et du Programme de renforcement des télécommunications contre les catastrophes naturelles (*Strengthening Telecommunications Against Natural Disasters Program*), l'Australie a adopté une politique en vue de garantir que les bâtiments qui abritent des infrastructures essentielles soient construits avec des matériaux résistants au feu. ▪ Le réseau japonais repose en grande partie sur des lignes enfouies et sous-marines pour atténuer les répercussions des tremblements de terre et des tsunamis.
Redondance du réseau	▪ Les efforts en vue d'éliminer les points de défaillance uniques et de créer une redondance au sein des réseaux ont été observés dans toutes les administrations.

Facteurs pour l'amélioration de la cybersécurité et l'exploitation de l'intelligence artificielle

Historiquement, les efforts en matière de cybersécurité se sont concentrés sur la prévention de la perte de données et de la protection de la vie privée, sous l'impulsion du gouvernement. Toutefois, les fournisseurs ont récemment réorienté leurs efforts vers la lutte proactive contre les menaces et l'exploitation des technologies émergentes.

Tableau 5. Principaux enseignements des facteurs pour l'amélioration de la cybersécurité et d'exploitation de l'intelligence artificielle

Préoccupations relatives à la perte de données et à la protection de la vie privée	▪ La divulgation potentielle des données des clients, de la propriété intellectuelle, des renseignements financiers et des renseignements organisationnels de nature exclusive ou sensible incite les fournisseurs à investir dans la cybersécurité.
Répercussions sur les activités	▪ Les cyberattaques détournent les ressources internes des activités productives (pour la réponse à l'incident, l'enquête et la correction) et, dans certains cas, elles peuvent endommager l'infrastructure physique.
Répercussions financières ou atteintes à la réputation	▪ Les pannes et la dégradation des services peuvent entraîner des pertes financières, des risques juridiques et des atteintes à la réputation. ▪ La presse et la publicité relatives aux piratages, aux événements liés aux logiciels malveillants et à d'autres cyberactivités peuvent être des facteurs déterminants qui encourageant une plus grande proactivité dans ce domaine.
Réseaux autonomes et autorégulateurs	▪ L'intelligence artificielle (IA) dans les réseaux s'articule autour de l'analyse prédictive. Elle vise à résoudre un problème ou un enjeu avant qu'il ne survienne en comprenant l'objectif de conception du réseau et ses politiques, et en examinant des mesures prédéfinies, des flux de trafic, des tendances et des modèles, tout en les comparant aux bases de référence du réseau. ▪ Il en résulte une amélioration de la disponibilité (> 25 %) et une réduction générale des pannes opérationnelles et involontaires.

Facteurs pour l'amélioration de la couverture du réseau

La plupart des administrations ont adopté une approche hybride en vue d'étendre la couverture du réseau. Les mesures comprennent les obligations de service universel (OSU) et les obligations de service d'urgence. Il s'agit plus particulièrement de l'extension de la couverture du réseau, généralement au moyen de l'infrastructure, que de l'ajout ou de l'extension de la redondance des réseaux. Cependant, la redondance pourrait être une considération essentielle pour toutes les extensions de réseau afin de garantir que la résilience est intégrée dans le réseau dès le départ.

Tableau 6. Principaux enseignements des facteurs pour l'amélioration la couverture du réseau

Initiatives de l'industrie	▪ Permettre aux FST de déterminer le marché et de lancer des initiatives en vue d'améliorer la couverture dans les régions qui sont commercialement viables. ▪ Permettre aux bénéfices d'inciter les FST à répondre aux demandes des clients, à améliorer leurs offres de services et à stimuler la croissance des revenus grâce à une meilleure couverture du réseau.
Initiatives soutenues par le gouvernement	▪ Soutenir les investissements et intervenir dans les régions où il n'est pas commercialement possible pour le marché de fournir des services (c'est-à-dire les régions rurales dotées d'un relief accidenté et d'une faible population). ▪ Soutenir les nouveaux investissements dans les infrastructures comme les satellites en orbite basse (LEO), les tours cellulaires supplémentaires et les infrastructures filaires. o Le gouvernement britannique estime qu'environ 10 % des locaux du Royaume-Uni ne sont pas commercialement viables pour l'industrie; il a soutenu les zones non desservies au moyen du Programme de large bande extrêmement rapide (*Superfast Broadband Programme*) de Building Digital UK (BDUK), qui prévoit la mise en place d'un réseau entièrement en fibre dans ces zones. o Les États-Unis ont lancé des programmes comme le Programme d'équité, d'accès et de déploiement de la large bande (*Broadband Equity, Access, and Deployment Program*) et le Programme de subventions pour les infrastructures intermédiaires à large bande (*Enabling Middle Mile Broadband Infrastructure Grant Program*) afin d'améliorer l'accès à la large bande dans les collectivités non desservies ou mal desservies.

Canada

Aperçu de la législation et des cadres réglementaires sur la résilience (y compris en attente)

- Le Conseil de la radiodiffusion et des télécommunications canadiennes (Conseil) a pour mandat de réglementer et de surveiller les télécommunications dans l'intérêt du public et de veiller à ce que la population canadienne ait accès à un système de communication de classe mondiale qui encourage l'innovation et enrichit sa vie.
- Le mandat du CRTC est établi par la législation et vise à atteindre les objectifs en matière de politique établis dans la *Loi sur les télécommunications* et la Loi canadienne anti-pourriel (LCAP).
- L'alinéa 7b) de la *Loi sur les télécommunications* comprend un objectif en matière de politique relatif à la fiabilité, qui peut être pris en compte dans la prise de décision relative aux cadres réglementaires et législatifs existants.
- En conséquence, le Conseil a imposé ou exigé la mise en œuvre de la résilience et de la fiabilité des réseaux et services de télécommunication dans le cadre de diverses instances de politique qui ont donné lieu à des décisions ou ordonnances relatives à la résilience et à la fiabilité techniques et opérationnelles.

- Le Conseil a approuvé ou imposé la mise en œuvre de diverses recommandations concernant les exigences et les pratiques exemplaires en matière de résilience technique, opérationnelle et procédurale élaborées par le Comité directeur du CRTC sur l'interconnexion (CDCI) et ses divers groupes de travail, notamment le Groupe de travail Réseau (GTR), le Groupe de travail Services d'urgence (GTSU) et le Groupe de travail Plan de travail (GTPT).
- Les modifications proposées à la *Loi sur les télécommunications* en matière de sécurité dans le cadre de la Partie I du projet de loi C-26 qui, si elles sont adoptées, établiront de nouveaux pouvoirs qui permettront au gouvernement de prendre des mesures pour promouvoir la sécurité du système canadien de télécommunications, ce qui pourrait inclure des mesures liées à la résilience de manière plus générale.
- Un nouvel objectif de politique serait ajouté pour promouvoir la sécurité du système canadien de télécommunications, ce qui permettrait au ministre de l'Industrie et au Conseil de prendre en compte cet objectif lorsqu'ils exercent leurs pouvoirs respectifs en vertu de la *Loi sur les télécommunications.*
- Les nouveaux pouvoirs d'ordonnance du ministre de l'Industrie pourraient être utilisés pour ordonner aux FST de prendre un large éventail de mesures, sous réserve de consultation, en vue de protéger le système de télécommunications contre les risques d'interférence, de manipulation ou de perturbation.

Initiatives en vue d'améliorer la puissance et la résilience du réseau

- ISDE a créé le Comité consultatif canadien pour la sécurité des télécommunications (CCCST) et le Forum canadien pour la résilience des infrastructures numériques (FCRIN) afin de faire avancer les priorités communes, d'échanger des renseignements et de mettre au point les pratiques exemplaires.
- Le programme de fiabilité des réseaux de télécommunications a été publié en septembre 2022 afin de garantir la fiabilité et la résilience des réseaux, non seulement face aux cyberattaques, mais aussi face aux catastrophes naturelles et aux erreurs humaines susceptibles de provoquer des interruptions prolongées des réseaux. Ce programme a été lancé à la suite d'une panne survenue en juillet 2022 dans l'une des trois principales entreprises de télécommunications du Canada, qui a duré 15 heures ou plus pour des millions d'abonnés.
- Le Protocole d'entente sur la fiabilité des télécommunications est désormais pleinement opérationnel après la négociation d'ententes bilatérales d'itinérance d'urgence et l'élaboration de plans d'action internes pour les communications d'urgence.
- Les recommandations du CCCST en vue de renforcer la résilience du réseau ont été publiées en mars 2023. ISDE et ses partenaires gouvernementaux sont en train d'examiner ces recommandations.
- De même, les recommandations du FCRIN en vue d'améliorer la fiabilité et la résilience de l'infrastructure numérique du Canada ont été publiées le 1er mai 2023. ISDE et ses partenaires gouvernementaux sont en train d'examiner ces recommandations.

Initiatives en vue d'améliorer la cybersécurité

- Les initiatives actuelles s'inscrivent dans le cadre de la Stratégie nationale de cybersécurité du Canada et du Plan d'action national en matière de cybersécurité. Elles sont également soutenues par la Stratégie nationale sur les infrastructures essentielles du Canada et le Plan d'action sur les infrastructures essentielles.
- La Partie II du projet de loi C-26 propose d'adopter la *Loi sur la protection des cybersystèmes essentiels* (LPCSE), qui établirait un cadre réglementaire pour les secteurs des télécommunications, de la finance, des transports et de l'énergie.

- La LPCSE énumère les services et systèmes vitaux dans l'annexe 1, et les catégories d'exploitants de ces services et systèmes dans l'annexe 2. Les exploitants désignés auront des obligations en vertu de la LPCSE en ce qui concerne leurs cybersystèmes essentiels qui sous-tendent les services et systèmes qui sont d'une importance critique.
- Actuellement, l'annexe 1 énumère les services de télécommunication. Le ministre de l'Industrie fera office d'organisme de réglementation pour le secteur des télécommunications dans le cadre de la LPCSE.
- Les exploitants désignés devront réaliser ce qui suit :
  - établir des programmes de cybersécurité;
  - atténuer les risques associés aux chaînes d'approvisionnement et aux tiers;
  - déclarer les incidents de cybersécurité au Centre de la sécurité des télécommunications et informer l'organisme de réglementation du secteur;
  - se conformer à toute directive relative à la cybersécurité (pouvoir d'ordonnance).

Initiatives en vue d'améliorer la couverture

- ISDE a créé la Stratégie canadienne pour la connectivité en 2019 avec l'objectif que toute la population canadienne ait accès à la large bande à des vitesses de 50 mbps de téléchargement et de 10 mbps de téléversement d'ici 2030 et à une couverture mobile sans fil élargie. Les programmes de large bande d'ISDE, notamment le Fonds pour la large bande universelle (FLBU) et Brancher pour innover (BPI), contribuent à soutenir cette initiative.

États-Unis

Aperçu de la législation et des cadres réglementaires sur la résilience

- La Commission fédérale des communications (FCC) est le principal organisme de régulation des télécommunications aux États-Unis.
- Trois lois primaires et une ordonnance couvrent la réglementation (*Communications Act 1934*, *Telecommunications Act 1996*, l'ordonnance relative à l'Internet ouvert de 2015 de la FCC, et *Digital Equity Act 2021*).
- Les lois réglementent pratiquement tous les aspects de l'industrie des communications et de la radiodiffusion, y compris l'attribution des fréquences, les tarifs et les redevances, les normes, la concurrence, les conditions d'accès des abonnés, les messages publicitaires, la radiodiffusion dans l'intérêt public, l'utilisation des systèmes de communication par les pouvoirs publics.
- Les lois prévoient également une réglementation et une surveillance plus détaillées par l'intermédiaire de la FCC.
- Ces lois encouragent la concurrence et l'entrée dans l'industrie, tout en réglementant pratiquement tous les aspects de l'industrie des communications et de la radiodiffusion.

Initiatives en vue d'améliorer la puissance et la résilience du réseau

- La *Bipartisan Infrastructure Law* prévoit un financement de 65 milliards de dollars pour aider à atteindre l'objectif de connecter tous les Américains à un Internet haute vitesse abordable et fiable, sous la houlette de quatre agences : la National Telecommunications and Information Administration (NTIA), la Commission fédérale des

communications (FCC), le Department of the Treasury, et le United States Department of Agriculture (USDA).

- Le Programme de recherche et développement sur l'infrastructure des réseaux mobiles sécurisés et résilients et sur les communications d'urgence (*Secure and Resilient Mobile Network Infrastructure and Emergency Communications Research and Development Program*) de la Direction des sciences et technologies du département de la Sécurité intérieure apporte un soutien direct en matière de recherche et développement aux priorités de la Cybersecurity and Infrastructure Security Agency (CISA) en vue de sécuriser et de rendre résilientes l'infrastructure 5G ainsi que les capacités de communication d'urgence.
- Cela permettra de sécuriser l'infrastructure des réseaux mobiles pour les missions du gouvernement fédéral et d'utiliser les capacités des systèmes de communication des premiers intervenants.
- Le Plan national de communication d'urgence (*National Emergency Communications Plan*) est le plan stratégique des États-Unis en vue de renforcer et d'améliorer les capacités de communication d'urgence.
- Le titre XVIII de la *Homeland Security Act of 2002* exige que la CISA élabore le Plan afin de fournir des recommandations pour soutenir les interventions d'urgence en cas de catastrophe.
- Le Fonds d'innovation pour la chaîne d'approvisionnement des services publics sans fil (*Public Wireless Supply Chain Innovation Fund*) prévoit un investissement de 1,5 milliard de dollars dans le développement de réseaux ouverts et interopérables, la promotion de la concurrence, la réduction des coûts, le soutien à l'innovation et le renforcement de la chaîne d'approvisionnement de la 5G. L'un des objectifs de ce fonds est la promotion de l'adoption du réseau d'accès radio (RAN) ouvert. Bien que cela n'ait pas d'influence directe sur la résilience, le fait d'avoir de nouveaux entrants et une certaine souplesse de la part de plusieurs fabricants permet d'assurer la résilience grâce à la diversification et au développement de la redondance.

Initiatives en vue d'améliorer la cybersécurité

- Le décret 13800 de 2017, intitulé « Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure » (Renforcer la cybersécurité des réseaux fédéraux et des infrastructures essentielles), exige que les secrétaires au Commerce et à la Sécurité intérieure « mènent conjointement un processus ouvert et transparent pour déterminer et promouvoir les mesures prises par les parties prenantes appropriées afin d'améliorer la résilience d'Internet et de l'écosystème des communications et d'encourager la collaboration dans le but de réduire considérablement les menaces perpétrées par des attaques automatisées et distribuées (par exemple, les réseaux de zombies). »

Initiatives en vue d'améliorer la couverture

- La *Access Broadband Act of 2021* a été créée afin d'améliorer l'accès à Internet haute vitesse en étendant les réseaux à large bande aux collectivités qui en ont besoin.

Royaume-Uni

Aperçu de la législation et des cadres réglementaires sur la résilience

- L'Ofcom est l'organisme de réglementation et l'autorité en matière de concurrence pour les industries de la communication au Royaume-Uni. Il réglemente les secteurs de la télévision et de la radio, des télécommunications de lignes fixes, de la téléphonie mobile,

des services postaux, ainsi que les ondes sur lesquelles fonctionnent les appareils sans fil.
- La *Communications Act 2003* est la loi de base. La *Loi* réglemente les fournisseurs de services de communication au moyen d'autorisations générales qui doivent être respectées pour pouvoir opérer sur le marché.
- Elle nécessite un réseau téléphonique public efficace et, en cas de panne catastrophique du réseau, sa disponibilité et son accès ininterrompu pour les situations d'urgence.
- Elle permet également à l'Ofcom de mettre en œuvre des conditions qui exigent des fournisseurs qu'ils aident les administrations centrales et locales en cas d'urgence.

Initiatives en vue d'améliorer la puissance et la résilience du réseau

- Le Code de pratique sur la sécurité des télécommunications (*Telecommunications Security Code of Practice*) du Royaume-Uni est un cadre établi par la *Telecommunications (Security) Act 2021* qui comporte trois niveaux : des obligations de sécurité renforcées pour les fournisseurs de services de télécommunication publics, des mesures ou exigences particulières en matière de sécurité et des orientations techniques.
- Ce code de pratique fournit des lignes directrices détaillées aux fournisseurs de services de télécommunication publics de moyenne et grande taille sur l'approche à privilégier pour démontrer la conformité.
- En cas de non-conformité, l'Ofcom peut émettre un avis d'infraction, déterminer les mesures correctives à prendre et les mesures provisoires à prendre pour combler les lacunes en matière de sécurité.
- L'Ofcom peut également imposer des sanctions administratives pécuniaires (SAP) ou des sanctions financières. Les sanctions financières peuvent atteindre 10 % du chiffre d'affaires de l'entreprise si celle-ci ne déploie pas suffisamment d'efforts pour se mettre en conformité.
- Les FST peuvent se conformer aux obligations et aux exigences en adoptant des solutions ou des approches différentes de celles spécifiées dans le code de pratique, avec l'approbation de l'Ofcom.

Initiatives en vue d'améliorer la cybersécurité

- Le National Cyber Security Centre du gouvernement britannique fournit des conseils et du soutien aux secteurs public et privé sur la manière d'éviter les menaces à la sécurité informatique.

Initiatives en vue d'améliorer la couverture

- La grande priorité stratégique du gouvernement britannique est de promouvoir une concurrence efficace et l'investissement dans les réseaux numériques. La promotion de l'investissement est prioritaire par rapport aux interventions en vue de réduire davantage les prix de détail à court terme, compte tenu des avantages à plus long terme.
- Le gouvernement a défini une série de résultats pour atteindre cette priorité stratégique :
    - Une stabilité et une clarté réglementaires accrues, grâce à des périodes d'examen du marché plus longues (cinq ans) et à un cadre qui garantit des rendements équitables.
    - Une réglementation uniquement lorsque et dans la mesure où elle est nécessaire pour répondre aux préoccupations en matière de concurrence et pour garantir la protection des intérêts des consommateurs.

    - Le cas échéant, une approche géographique différenciée de la réglementation. Dans les régions où il y a de la concurrence, la nécessité d'une réglementation serait moindre.
- Le gouvernement britannique estime qu'au moins un tiers des locaux du Royaume-Uni pourraient accueillir au moins trois réseaux concurrents dotés d'une capacité d'un gigabit, que près de la moitié pourrait accueillir deux réseaux concurrents ou plus, et qu'il peut y avoir des zones du pays qui ne bénéficieront pas d'investissements bien que commercialement viables pour au moins un opérateur.
- Le nouveau Code des communications électroniques européen (CCEE) permet de désigner les zones dans lesquelles aucun opérateur n'a indiqué son intention de se déployer et d'indiquer qu'un financement supplémentaire sera nécessaire pour assurer une couverture nationale.
- Cette stratégie repose sur la réalisation de cinq objectifs :
    - Réduire autant que possible le coût du déploiement des réseaux de fibres en éliminant les obstacles au déploiement, qui augmentent les coûts et entraînent des retards;
    - Favoriser l'entrée sur le marché et l'expansion d'autres opérateurs de réseaux grâce à un accès facile aux conduits et aux poteaux d'Openreach, accompagné d'un accès à l'infrastructure d'autres services publics (par exemple, les égouts);
    - Une réglementation stable et à long terme qui incite à investir dans des réseaux concurrentiels;
    - Une approche « de l'extérieur vers l'intérieur » en matière de déploiement qui signifie que la connectivité dotée d'une capacité d'un gigabit est atteinte en même temps dans toutes les régions du Royaume-Uni grâce à des investissements soutenus par le gouvernement;
    - Un processus de transition pour augmenter la demande pour des services entièrement par fibre.
- La fourniture de services entièrement par fibre sera privilégiée dans le cadre du Programme de large bande extrêmement rapide (*Superfast Broadband Programme*) de BDUK, qui a déjà permis l'accès à plus de 200 000 locaux dans des zones essentiellement rurales.
- L'examen de la chaîne d'approvisionnement en télécommunications de 2019 a mis en évidence la nécessité de gérer et d'atténuer les risques relatifs aux fournisseurs à haut risque, d'introduire un nouveau cadre en matière de sécurité solide pour les télécommunications et de créer une base d'approvisionnement plus diversifiée et plus compétitive pour les réseaux de télécommunications (diversification de la 5G).
- Le gouvernement a pris des décisions importantes pour limiter et exclure les vendeurs à haut risque de l'infrastructure des télécommunications du Royaume-Uni et a proposé une législation pour donner à ces décisions un statut légal.
- Il s'agissait notamment de soutenir les fournisseurs titulaires, d'attirer de nouveaux fournisseurs et d'accélérer les solutions d'interface ouverte et leur déploiement afin que le Royaume-Uni ne soit pas tributaire d'un seul fournisseur.
- Le Royaume-Uni a élaboré des principes du RAN ouvert, Open RAN principles – GOV.UK (www.gov.uk) [en anglais seulement], qui renvoient directement à la stratégie de diversification, ainsi que des travaux de recherche et développement en cours soutenus par le gouvernement et les essais relatifs au RAN ouvert, tels que SmartRAN Open Network Interoperability Centre (SONIC) Labs – Case study – GOV.UK (www.gov.uk) [en anglais seulement].

Australie

Aperçu de la législation et des cadres réglementaires sur la résilience

- L'Australian Communications and Media Authority (ACMA) est le principal organisme de réglementation des télécommunications en Australie.
- L'Australian Competition and Consumer Commission (ACCC) est responsable de la réglementation de la concurrence.
- L'ACCC évalue et fait respecter les conditions d'accès au Réseau national à large bande (*National Broadband Network* [NBN]), fixe les prix de gros et les conditions d'accès de gros pour les services déclarés, assure le suivi des prix et de la concurrence et établit des rapports à ce sujet, et enquête sur les allégations de conduite anticoncurrentielle.
- La *Telecommunications Act 1997* est la principale loi qui régit les télécommunications en Australie et qui couvre les entreprises (c'est-à-dire les propriétaires et les opérateurs d'infrastructures) et les autres entités qui fournissent des services aux utilisateurs finals, appelés fournisseurs de services de distribution.
- La *Telecommunications (Consumer Protection and Service Standards) Act 1999* établit le service universel et d'autres services de télécommunication d'intérêt public.

Initiatives en vue d'améliorer la puissance et la résilience du réseau

- Le Programme de renforcement des réseaux mobiles (*Mobile Network Hardening Program*) est une initiative du gouvernement de l'Australie (avec financement) qui aide les opérateurs de réseaux mobiles, les fournisseurs d'infrastructures et les gestionnaires d'infrastructures à améliorer la résilience de l'infrastructure des télécommunications des réseaux mobiles régionaux à :
  - prévenir les pannes en cas de catastrophe naturelle;
  - renforcer la résilience des installations de télécommunications pour leur permettre de fonctionner plus longtemps pendant les feux de brousse et toute autre catastrophe naturelle;
  - permettre le rétablissement rapide des services après une panne.
- La première étape a permis d'augmenter l'autonomie des batteries de secours de 467 stations de base à au moins 12 heures.
- La deuxième étape a permis la réalisation de plus de 530 améliorations de la résilience sur des sites de stations de base de téléphonie mobile en ce qui concerne :
  - le déploiement de nouvelles génératrices portables et permanentes
  - la mise à niveau des systèmes de batteries, ajout de dispositifs d'extension des batteries;
  - l'amélioration de la résilience de la transmission au sein des groupes de réseaux mobiles régionaux afin de réduire les points de défaillance uniques du réseau;
  - le renforcement physique des sites contre les dommages causés par les feux de brousse.
- Le Programme de renforcement des télécommunications contre les catastrophes naturelles (*Strengthening Telecommunications Against Natural* Disasters *Programme*) est une subvention temporaire accordée en 2022. Son objectif était d'améliorer la résilience des collectivités qui ont été touchées par de graves feux de brousse ou qui risquent de subir des catastrophes naturelles, et d'améliorer le rétablissement des services en déployant rapidement des installations temporaires pour combler les lacunes causées par les pannes.
- Le Programme d'innovation en matière de résilience des télécommunications face aux catastrophes (*Telecommunications Disaster Resilience Innovation Program*) pour 2022-

2025 a encouragé le développement de nouvelles technologies pour la résilience, en particulier dans les collectivités régionales, éloignées et les communautés des Premières Nations.
    - La première série portait sur la résilience face aux conséquences des pannes d'électricité.
    - La deuxième série portait sur les technologies innovantes pour améliorer la résilience face aux catastrophes naturelles.
- Ces programmes étaient destinés à aider à faire face aux risques climatiques croissants, notamment à l'augmentation prévue de la fréquence et de la gravité des catastrophes naturelles.
- Le gouvernement de l'Australie a co-investi avec l'industrie des télécommunications pour acheter des installations de communication portables, notamment des cellules sur roues, des centraux mobiles sur roues, des camions Road Muster du NBN, et des trousses de satellites portables, pour les positionner dans les zones sinistrées afin de rétablir rapidement les services.
- Le gouvernement a également amélioré la connectivité des stations des services d'incendie en milieu rural et des centres d'évacuation grâce aux connexions par satellite Sky Muster.

Initiatives en vue d'améliorer la cybersécurité

- L'Australian Cyber Security Centre (ACSC) de l'Australian Signals Directorate (ASD) dirige les efforts du gouvernement australien afin d'améliorer la cybersécurité.
- L'ACSC est un centre de collaboration et d'échange de renseignements des secteurs privé et public qui a pour fonction de :
    - répondre aux menaces et aux incidents de cybersécurité en tant qu'équipe d'intervention en cas d'urgence informatique de l'Australie;
    - collaborer avec les secteurs privé et public pour échanger des renseignements sur les menaces et accroître la résilience;
    - sensibiliser les gouvernements, l'industrie et la collectivité à la cybersécurité;
    - fournir des renseignements, des conseils et de l'aide en matière de cybersécurité à tous les Australiens.
- En 2021, la *Security of Critical Infrastructure Act 2018* a été modifiée afin d'ajouter des obligations pour les entreprises et les fournisseurs de services de distribution, notamment :
    - aviser l'ACSC si un incident de cybersécurité a des répercussions importantes sur une infrastructure essentielle;
    - fournir au Cyber and Infrastructure Security Centre du ministère de l'Intérieur certains renseignements sur les infrastructures essentielles afin de les inclure dans un registre.

Initiatives en vue d'améliorer la couverture

- La politique australienne du NBN de 2009 visait à améliorer la disponibilité et le rendement de la large bande en Australie et à faciliter la séparation structurelle de Telstra en fournissant une option en fibre à son réseau en cuivre.
- Le Réseau est construit et géré par une entreprise publique, nbnTM.
- L'un des principes fondamentaux de la politique est que nbnTM ne fournit que des services de gros aux fournisseurs de services de détail et ne dessert pas les utilisateurs finals.
- Le plan initial du NBN prévoyait d'équiper 93 % des locaux d'une connexion en fibre optique. Les 7 % de locaux restants seraient desservis par un nouveau service par satellite ou par un service terrestre sans fil fixe.

- Le cadre réglementaire du NBN a été établi au moyen de deux lois :
  - *National Broadband Network Companies Act 2011*
  - *Telecommunications Legislation Amendment (National Broadband Network Measures—Access Arrangements) Act 2011*
- Récemment, le gouvernement de l'Australie s'est engagé à investir 2,4 milliards de dollars afin de permettre à 1,5 million de foyers et d'entreprises supplémentaires actuellement desservis par la fibre jusqu'au nœud (FTTN) de passer à la fibre jusqu'aux locaux de l'abonné (FTTP).
- La FTTP est estimée comme meilleure que la FTTN (plus grande vitesse et fiabilité), et les deux sont meilleures que le cuivre, car elles sont plus rapides, meilleures sur les longues distances, ont une plus grande largeur de bande, sont plus évolutives, et sont plus fiables et stables.
- Ces améliorations permettront d'offrir des vitesses de connexion à large bande plus rapides, une meilleure fiabilité, une plus grande efficacité énergétique et une capacité de données supplémentaire.

Nouvelle-Zélande

Aperçu de la législation et des cadres réglementaires sur la résilience

- Le ministère des EntreprisesMinistry of Business, Innovation and Employment (MBIE), la New Zealand Commerce Commission et le Telecommunications Forum (TCF) jouent un rôle clé dans la législation, la réglementation et la fourniture de services de télécommunication en Nouvelle-Zélande.
- La *Telecommunication Act 2001* sert de base à la réglementation et à la législation et permet au TCF de réglementer la prestation de services de télécommunication.

Initiatives en vue d'améliorer la puissance et la résilience du réseau

- Le Programme d'amélioration de la capacité rurale (*Rural Capacity Upgrade Programme*) permettra de moderniser les tours cellulaires existantes et d'en construire de nouvelles dans les zones rurales où le rendement est médiocre, ainsi que de déployer la fibre, une couverture de ligne d'abonné numérique à très haut débit (VDSL) supplémentaire et d'autres technologies sans fil dans les zones encombrées.
- Le programme pour les utilisateurs éloignés vise à équiper le plus grand nombre possible de foyers éloignés de l'infrastructure de connectivité nécessaire pour accéder aux services à large bande.
- Le Fonds pour les zones sans réseau mobile (*Mobile Black Spot Fund*) permet d'améliorer la couverture mobile sur environ 1 400 kilomètres de routes nationales et dans plus de 168 sites touristiques où aucune couverture n'existe actuellement.

Initiatives en vue d'améliorer la cybersécurité

- Le principal organisme gouvernemental chargé de définir la politique en matière de cybersécurité en Nouvelle-Zélande est le Département du Premier ministre et du Cabinet (DPMC).
- Le Plan d'intervention d'urgence en matière de cybersécurité (*Cyber Security Emergency Response Plan*) définit le cadre de la réponse du gouvernement à une situation d'urgence en matière de cybersécurité. Il définit les rôles, les responsabilités, l'approche du gouvernement ainsi que la coordination et veille à ce que les services et les opérations soient rétablis rapidement et à ce que les leçons appropriées sont tirées et mises en œuvre.

- Le Plan fait partie du Système de sécurité nationale (*National Security System*) de la Nouvelle-Zélande. Il est géré par le DPMC et est rédigé en collaboration avec d'autres agences qui jouent un rôle en cybersécurité.

Initiatives en vue d'améliorer la couverture

- Le Programme de la large bande ultrarapide (*Ultra-Fast Broadband Program*) a été mis en place pour permettre à environ 87 % des Néo-Zélandais, dans plus de 390 villes, d'accéder à la fibre d'ici la fin de 2022.
- Près de 1,8 milliard de dollars ont été investis dans l'infrastructure de la large bande ultrarapide.
- Crown Infrastructure Partners a été créée en tant que société d'État pour gérer l'investissement du gouvernement dans la large bande ultrarapide.
- La large bande ultrarapide utilise des câbles à fibre optique pour acheminer la fibre jusqu'à l'abonné. Elle est plus appropriée dans les zones urbaines à forte densité de population.
- Grâce au déploiement efficace de la fibre optique et de liaisons par câble sous-marin supplémentaires, la Nouvelle-Zélande se situe désormais bien au-dessus de la moyenne de l'Organisation de coopération et de développement économique (OCDE) et dans une position similaire à celle des États-Unis, avec des vitesses Internet moyennes de 33 mbps.

Japon

Aperçu de la législation et des cadres réglementaires sur la résilience

- Le ministère des Affaires intérieures et des Communications (MAIC) est l'organisme de régulation des télécommunications (plus précisément le Bureau des télécommunications).
- Son rôle consiste à formuler des politiques, à attribuer des licences, à gérer les radiofréquences, à promouvoir la concurrence, à protéger les droits des consommateurs et à assurer le bon déroulement des opérations.

Initiatives en vue d'améliorer la puissance et la résilience du réseau

- Le Japon dispose d'un solide système d'alerte précoce aux tremblements de terre qui permet d'alerter le public et de prévenir les perturbations des infrastructures de télécommunications.
- La communication sans fil à adresses multiples, les récepteurs domestiques et les radios sont utilisés pour transmettre des informations aux collectivités locales par l'intermédiaire de sirènes, de haut-parleurs et d'autres moyens.
- J-Alert est un système qui convertit les renseignements provenant d'organisations publiques en XHL, en courrier électronique et dans d'autres formats, et les transmet aux médias et aux entreprises de communication.
- Le Japon utilise des unités de ressources mobiles et déployables de TIC, qui comportent des dispositifs de communication, de traitement de l'information et de stockage montés sur un conteneur ou véhicule mobile.
- Les bureaux régionaux du gouvernement ont créé des stations fixes, dont beaucoup sont équipées de systèmes de communication par satellite portables.
- Au Japon, les FST sont tenus de mettre en place des systèmes d'alimentation de secours, notamment des systèmes d'alimentation sans interruption (ASI) et des génératrices d'urgence.

- Pour minimiser les risques de tremblements de terre et de catastrophes et s'en protéger, une grande partie de l'infrastructure de télécommunication, y compris les câbles à fibres, est installée sous terre.

Initiatives en vue d'améliorer la cybersécurité

- La Politique de cybersécurité pour la protection des infrastructures essentielles est un plan d'action commun entre le gouvernement, chargé de promouvoir les mesures indépendantes, et les opérateurs d'infrastructures essentielles qui mettent en œuvre de manière indépendante des mesures de protection pertinentes.
- La *Basic Act on Cybersecurity* du Japon stipule que les opérateurs d'infrastructures essentielles, et certaines entreprises de télécommunication, doivent s'efforcer de sécuriser la cybersécurité de manière volontaire et proactive et de coopérer avec les mesures de cybersécurité mises en œuvre par le gouvernement.
- En vertu de la *Telecommunications Business Act*, les opérateurs de services ont l'obligation de protéger le secret des télécommunications et de maintenir ou exploiter les installations conformément aux normes techniques établies par le MAIC.
- La Stratégie de sécurité nationale est à la base de la stratégie de sécurité nationale du Japon, en définissant les stratégies diplomatiques et de défense en réponse au nouvel environnement de sécurité.
- La Stratégie de défense nationale définit la stratégie de défense de la Force japonaise d'autodéfense (FJA), en fixant des objectifs pour la sécurité nationale et en décrivant les approches et les moyens pour les atteindre.
- Le Programme de renforcement de la défense désigne un plan de développement à moyen et long terme qui comprend le niveau de capacité de défense et le plan d'approvisionnement.

Initiatives en vue d'améliorer la couverture

- En 2020, le taux de couverture nationale pour la large bande par fibre dans les ménages était de 99,1 %.
- Le gouvernement actuel a pour objectif de porter la zone couverte par la fibre optique à plus de 99,9 % de la masse continentale du pays d'ici 2028.

Union européenne

Aperçu de la législation et des cadres réglementaires sur la résilience

- L'Organe des régulateurs européens des communications électroniques (ORECE) est l'organisme de réglementation de l'Union européenne. Il est composé de représentants des autorités réglementaires nationales (ARN) de chaque État membre de l'Union européenne.
- Son rôle principal est de promouvoir l'application cohérente du cadre réglementaire de l'Union européenne pour les communications électroniques, de garantir la concurrence et de préserver les intérêts des consommateurs et des utilisateurs finals.
- L'ORECE fournit des orientations et des conseils à la Commission européenne, contribue à l'élaboration d'approches communes en matière de réglementation et à l'harmonisation du secteur des télécommunications dans l'ensemble de l'Union européenne. Le règlement de l'ORECE définit les tâches, les pouvoirs et la composition de l'ORECE.
- Le Code des communications électroniques européen (CCEE) est un cadre réglementaire complet pour les communications électroniques dans l'Union européenne. Le CCEE établit des règles pour les réseaux et les services de communications

électroniques, la gestion du spectre, l'accès aux réseaux, la protection des consommateurs et la concurrence. Il oblige les fournisseurs à garantir la sécurité et l'intégrité de leurs réseaux, à mettre en œuvre des mesures de sécurité appropriées et à mettre en place des capacités de réponse aux incidents.

Initiatives en vue d'améliorer la puissance et la résilience du réseau

- Les fournisseurs de services de communications électroniques de l'Union européenne sont tenus de déclarer les incidents qui ont des répercussions importantes sur la continuité des services de communications électroniques aux ARN des télécommunications de chaque État membre de l'Union européenne.
- Chaque année, les ARN transmettent à l'Agence de l'Union européenne pour la cybersécurité un résumé d'une sélection de ces incidents (les plus importants, en fonction d'un ensemble de seuils convenus à l'échelle de l'Union européenne).
- L'obligation de déclarer les incidents visait surtout les incidents de sécurité qui ont des répercussions importantes sur le fonctionnement de chaque catégorie de services de télécommunication.
- Au fil des ans, les organismes de régulation ont convenu de se concentrer principalement sur les pannes de réseau ou de service (incidents de type A – panne de service, par exemple, continuité, disponibilité – une panne due à une coupure de câble causée par une erreur de l'opérateur d'une machine d'excavation utilisée lors de la construction d'une route serait classée dans la catégorie des incidents de type A).
- Cela exclurait de la portée de ces rapports les attaques ciblées, telles que celles qui impliquent l'utilisation des vulnérabilités du protocole du système de signalisation no 7 (SS7), les fraudes par usurpation de carte SIM, ou même des attaques plus étendues qui ne provoquent cependant pas de pannes.
- La déclaration des incidents en matière de sécurité des télécommunications aux autorités nationales ne concerne que les incidents majeurs, c'est-à-dire ceux qui ont des répercussions importantes. Les incidents de moindre importance, qui ne touchent que de petits pourcentages de la population, comme les attaques d'usurpation de carte SIM, ne sont pas déclarés.
- En outre, le champ d'application du CCEE s'étend à un plus grand nombre de services, y compris les opérateurs de services de télécommunication traditionnels, mais aussi, par exemple, les fournisseurs de services de communication par contournement (tels que les services de messagerie comme Viber et WhatsApp).
- Les lignes directrices relatives aux rapports annuels combinent des paramètres quantitatifs et qualitatifs ainsi que la déclaration des incidents de sécurité qui touchent non seulement les services de téléphonie et Internet fixes et mobiles, mais aussi les services de communication interpersonnelle par numéro ou les services de communication interpersonnelle sans numéro (services de communication par contournement).

Initiatives en vue d'améliorer la cybersécurité

- L'Union européenne s'est concentrée sur la réglementation de la cyber-résilience des fournisseurs de services de communications électroniques dans le cadre réglementaire des télécommunications de l'Union européenne.
- Elle s'est étendue, au moyen de la Directive sur la sécurité des réseaux et des systèmes d'information (Directive SRI), aux opérateurs de services essentiels et aux fournisseurs de services numériques, qui comprennent notamment les fournisseurs d'infrastructures numériques et les services d'informatique en nuage.
- L'Agence de l'Union européenne pour la cybersécurité (ENISA) est une agence indépendante et essentielle de l'Union européenne, dont la mission principale est de

renforcer la cybersécurité en Europe et d'aider les États membres et les institutions de l'Union européenne dans leurs efforts pour améliorer leur résilience face aux cybermenaces.

- La Directive SRI est une législation européenne en matière de cybersécurité, dont l'objectif est d'atteindre un niveau élevé commun de cybersécurité pour tous les États membres. L'un des trois piliers de la Directive SRI est la mise en œuvre de la gestion des risques et des exigences en matière de déclaration des incidents.
- L'ENISA évalue et mesure chaque année l'incidence de la Directive SRI sur la cybersécurité.
- La Directive SRI2 est entrée en vigueur en 2023 et améliore le niveau actuel de cybersécurité par :
    - la création du réseau d'organisations de liaison en cas de cyber-crises (*Cyber Crises Liaison Organisation Network* [CyCLONe]);
    - l'amélioration du niveau d'harmonisation des exigences en matière de sécurité et de déclaration;
    - la promotion de l'introduction de la chaîne d'approvisionnement, de la gestion des vulnérabilités, de l'Internet de base et de la cyberhygiène dans les stratégies nationales de cybersécurité des États membres;
    - l'introduction de l'évaluation par les pairs afin d'améliorer la collaboration et le partage des connaissances;
    - l'inclusion d'un plus grand nombre de secteurs, ce qui signifie qu'un plus grand nombre d'entités sont obligées de prendre des mesures afin d'améliorer leur niveau de cybersécurité.
- La *Loi sur la cyberrésilience* de l'Union européenne met en place des exigences minimales en matière de cybersécurité pour les produits et les logiciels qui sont mis sur le marché unique, quel que soit leur lieu de production.
- Alors qu'il sera possible de faire des autodéclarations de conformité pour 90 % des produits, pour une trentaine de produits, l'examen de conformité devra être effectué par un tiers. La Commission européenne pourra demander le retrait du marché d'un produit qui présente un cyberrisque.
- L'Union européenne continue de veiller à la mise en œuvre de la boîte à outils de la cybersécurité de la 5G afin de déployer des réseaux sécurisés. Tous les États membres ont décidé à l'unanimité d'exclure les fournisseurs dits à haut risque de leurs réseaux (centraux et RAN).

Initiatives en vue d'améliorer la couverture

- Le Mécanisme pour l'interconnexion en Europe (*Connecting Europe Facility*) est un programme en vue de promouvoir le développement d'infrastructures numériques performantes, durables et interconnectées dans les États membres. Il apporte un soutien financier aux projets relatifs au déploiement de la large bande, aux réseaux 5G, au Wi-Fi public et à d'autres services numériques, dans le but d'améliorer la couverture et la connectivité.
- L'Europe à large bande (*Broadband Europe*) fait la promotion de la connexion des citoyens et des entreprises européens avec des réseaux à très haute capacité, y compris la connectivité dotée d'une capacité d'un gigabit pour tous les principaux moteurs socio-économiques, la couverture 5G ininterrompue pour toutes les zones urbaines et les principales voies de transport terrestre, et l'accès à une connectivité d'au moins 100 mbps pour tous les ménages européens.

- L'ambition de la décennie numérique de l'Europe est que, d'ici 2030, tous les foyers européens soient couverts par un réseau doté d'une capacité d'au moins un gigabit par seconde et que toutes les zones peuplées soient couvertes par la 5G.

3.2.1.2 Facteurs de l'industrie pour l'amélioration de la résilience

La concurrence, les consommateurs, les tendances du marché et la technologie déterminent les investissements de l'industrie dans la résilience des services de télécommunication. Dans l'ensemble des administrations, les efforts tendent à être réactifs, avec des signes de proactivité lorsque l'accès au réseau a été entravé ou perturbé ou que les répercussions sont ressenties sur le plan commercial ou en matière de réputation.

Tableau 7. Principaux enseignements des facteurs de l'industrie pour l'amélioration de la résilience des services de télécommunication

Concurrence	▪ La résilience peut constituer un avantage concurrentiel dans le secteur des télécommunications. Les fournisseurs qui peuvent offrir des solutions de connectivité fiables et robustes sont plus susceptibles d'attirer et de conserver des clients. En améliorant la résilience, les FST se différencient.
Dépendance croissante à la connectivité et à la technologie	▪ Les entreprises et les particuliers dépendent fortement d'une connectivité continue et fiable pour communiquer, transférer des données et accéder aux services essentiels. Cette dépendance rend nécessaire la résilience des télécommunications pour garantir une connectivité ininterrompue, même en cas de perturbations.
Attentes des clients	▪ Les entreprises et les consommateurs s'attendent à de la connectivité. Les pannes de réseau et les interruptions de service peuvent avoir des conséquences sur le plan financier et en termes de réputation pour les fournisseurs de services, et pousser les clients à se tourner vers la concurrence.
Télétravail et transformation numérique	▪ La pandémie de COVID-19 a accéléré l'adoption du télétravail la transformation numérique dans les entreprises, les organismes et les gouvernements. Alors que de plus en plus d'entreprises continuent à travailler à distance et s'appuient davantage sur des services infonuagiques, le besoin de résilience des services de télécommunication est d'autant plus important.
Technologies futures	▪ Le déploiement de technologies émergentes comme la 5G, l'Internet des objets et l'IA imposera des exigences supplémentaires aux services de télécommunication. L'industrie continuera à investir dans ces technologies et à soutenir ces sources de revenus.

Collaboration avec l'industrie et pression des pairs	▪ L'élaboration de normes et de pratiques exemplaires par des groupes de l'industrie, tant au sein d'une administration qu'entre différentes administrations (par exemple, l'ENISA dans l'Union européenne), continuera à favoriser les progrès et les améliorations en matière de résilience.

Les plus grands fournisseurs de services de télécommunication et fournisseurs de services Internet :

Comme indiqué à la section 3.1.3 Fournisseurs de services de communication des administrations, toutes les administrations évaluées possèdent au moins trois principaux fournisseurs ou entreprises de services qui fournissent des services de télécommunication.

Les facteurs de l'industrie se situent dans l'ensemble des éléments de motivation. Dans l'ensemble, les facteurs qui poussent le secteur des télécommunications à améliorer sa résilience sont les suivants : répondre aux attentes des clients, se différencier de la concurrence, se conformer aux réglementations, se prémunir contre les menaces de cybersécurité, assurer la continuité des activités et tirer parti des potentiels du marché.

Les fournisseurs de services sont plus motivés à s'améliorer lorsqu'ils en retirent un avantage financier, à court et à long terme.

3.2.1.3 Autres facteurs pour l'amélioration de la résilience

Les autres facteurs comprennent des éléments tels que l'environnement et les changements climatiques, l'impact de la COVID-19 et du télétravail ainsi que la transformation numérique. L'environnement et les changements climatiques sont généralement plus inattendus et ont une incidence sur la disponibilité et le rendement.

Les facteurs liés à l'environnement et aux changements climatiques ont tendance à être plus inattendus et ont des conséquences plus importantes. Les catastrophes naturelles peuvent avoir des effets dévastateurs sur les pays et leurs citoyens, accentués par les perturbations et la perte des télécommunications.

Tableau 8. Principaux enseignements pour les autres facteurs liés à l'environnement et aux changements sociétaux

Fréquence et intensité accrues	▪ L'élévation du niveau de la mer, les tempêtes et l'érosion côtière peuvent menacer les infrastructures de télécommunications côtières. En outre, les vagues de chaleur, les sécheresses prolongées et les incendies de forêt peuvent endommager les équipements de réseau. ▪ Les pays connaissent ces conditions avec une fréquence et une gravité accrues. ▪ L'Australie, par exemple, continue de souffrir d'interruptions de réseau plus fréquentes et plus graves en raison de phénomènes météorologiques et d'incendies de forêt.
Adaptation aux conditions changeantes	▪ Les facteurs environnementaux nécessitent également une adaptation aux conditions changeantes. Les FST peuvent être amenés à modifier l'infrastructure de leur réseau ou à déployer

	des ressources supplémentaires dans des zones exposées à des risques environnementaux précis. ▪ Par exemple, la Nouvelle-Zélande a été plus proactive dans sa réponse à la gestion des répercussions des catastrophes naturelles, comme en témoigne le récent cyclone Gabrielle, en constatant une pénétration accrue des dispositifs satellitaires dans les communautés rurales et isolées.
Systèmes de surveillance et d'alerte précoce	▪ La capacité des organisations à surveiller et à prévoir les changements environnementaux avec une plus grande précision permettra une plus grande proactivité pour traiter les vulnérabilités et planifier de futures mesures de résilience pour les réseaux de télécommunications. ▪ Le Japon, par exemple, est témoin de tremblements de terre puissants et fréquents, accompagnés de tsunamis, d'éruptions volcaniques, d'ouragans et de typhons violents. Le Japon a mis au point des systèmes et des cadres d'échange de renseignements sur les catastrophes, des communications par satellite pour la redondance, des tours mobiles et des équipes d'intervention rapide.
Télétravail transformation numérique	▪ La pandémie de COVID-19 a accéléré l'adoption du télétravail et de la transformation numérique dans les entreprises, les organismes et les gouvernements. Alors que de plus en plus d'entreprises continuent à travailler à distance et s'appuient davantage sur des services infonuagique, le besoin de résilience des services de télécommunication est d'autant plus important.

Les **États-Unis**, avec leur diversité géographique, sont confrontés à un large éventail de catastrophes naturelles : ouragans, incendies de forêt, tornades, inondations, tempêtes hivernales et tremblements de terre. À ce titre, les États-Unis ont mis au point plusieurs cadres et initiatives, notamment le *Système d'information sur les catastrophes (Disaster Information Reporting System)*, un système de déclaration volontaire, le Plan national de protection des infrastructures (*National Infrastructure Protection Plan*) pour renforcer les infrastructures essentielles, le Cadre coopératif pour la résilience des réseaux sans fil (*Wireless Resiliency Cooperative Framework*) qui encourage les fournisseurs de services sans fil à se coordonner en cas d'urgence et d'autres initiatives locales et étatiques (par exemple, des groupes de travail, des réglementations ou des lignes directrices). Les États-Unis ont également mis en place des initiatives précises pour faire face à des risques tels que les ouragans et les incendies de forêt (par exemple, les alertes d'urgence sans fil [*Wireless Emergency Alerts*], les subventions d'aide à la gestion des incendies [*Fire Management Assistance Grants*]).

Le **Royaume-Uni** a connu, ces dernières années, de violentes tempêtes et inondations qui ont causé des dégâts et des perturbations considérables. Au cours des mois d'hiver, le Royaume-Uni a connu des vagues de froid extrême accompagnées d'importantes chutes de neige, des températures inférieures à zéro et des vents violents, ce qui a posé des problèmes aux infrastructures et aux services publics. Le Royaume-Uni n'est généralement pas sujet à des catastrophes naturelles de grande ampleur comme les tremblements de terre ou les tsunamis.

Comme la plupart des pays, le Royaume-Uni dispose de plusieurs systèmes d'alerte précoce pour atténuer les effets des phénomènes météorologiques violents.

L'**Australie** a subi des interruptions de réseau dues à des phénomènes météorologiques et à des incendies de forêt et a toujours été à la traîne des autres pays étudiés en termes de résilience du réseau face aux catastrophes naturelles. Il y a moins d'infrastructures pour répondre aux besoins des zones rurales et peu d'initiatives gouvernementales pour y remédier. Cette situation a toutefois évolué au cours des dernières années, car le gouvernement a augmenté les dépenses consacrées à des programmes tels que le Programme d'innovation pour la résilience des télécommunications face aux catastrophes (*Telecommunications Disaster Resilience Innovation Program*) et à la création de l'infrastructure à large bande. En outre, les campagnes australiennes présentent une forte pénétration de dispositifs et d'infrastructures de communication par satellite, ce qui renforce la résilience du réseau.

Comme l'Australie, la **Nouvelle-Zélande** est restée la traîne des autres pays de cette liste jusqu'à récemment, mais le gouvernement néo-zélandais a pris les devants et incite les entreprises privées à créer des infrastructures résilientes. En outre, le gouvernement est également proactif dans sa réponse à la gestion des répercussions des catastrophes naturelles, comme en témoigne le récent cyclone Gabrielle. Comme l'Australie, la Nouvelle-Zélande connaît également une forte pénétration des dispositifs satellitaires dans les communautés rurales et isolées.

Le **Japon** est le pays le plus exposé aux catastrophes de cette liste. Situé sur la ceinture de feu du Pacifique, le Japon est le témoin de tremblements de terre puissants et fréquents dus à l'activité tectonique, accompagnés de tsunamis et d'éruptions volcaniques. Le Japon connaît également une saison des ouragans et de puissants typhons. C'est pourquoi le Japon dispose d'une infrastructure très solide pour relever ces défis : des systèmes d'alerte précoce et de détection omniprésents dans tout le pays, des systèmes et cadres d'échange de renseignements sur les catastrophes, des réseaux de communication par satellite pour la redondance, des tours de transmission mobiles et des équipes d'intervention rapide toujours en attente avec les exploitants privés de télécommunications. En outre, les câbles sous-marins du Japon sont situés dans des baies relativement moins exposées aux catastrophes naturelles. La résilience du réseau japonais face à la menace spécifique que représentent les catastrophes naturelles est exemplaire.

L'**Union européenne**, avec sa diversité au travers de ses 27 pays membres, présente un large éventail d'enjeux environnementaux et climatiques. Plusieurs pays d'Europe ont été confrontés à de graves tempêtes et inondations au cours des dernières années, notamment le Royaume-Uni, l'Allemagne, la Pologne, la France et d'autres pays. Les incendies de forêt ont également été plus fréquents, notamment en Grèce, au Portugal, en Espagne, en Italie et en Suède. Les tempêtes hivernales et les vagues de froid ont également touché plusieurs régions d'Europe, avec une plus grande fréquence. Chaque pays dispose de ses propres mécanismes et ressources pour répondre aux catastrophes naturelles, souvent en coordination avec le Mécanisme de protection civile et le Centre de coordination de la réaction d'urgence de l'Union européenne, qui facilitent la coopération entre les États membres en cas d'urgence. L'Union européenne a également élaboré la Stratégie d'adaptation de l'Union européenne, qui définit la manière dont l'Union européenne peut s'adapter aux impacts inévitables des changements climatiques et devenir résiliente aux changements climatiques d'ici 2050. La stratégie s'est fixé des objectifs principaux : rendre l'adaptation plus intelligente, plus rapide et plus systémique, et intensifier l'action internationale en matière d'adaptation aux changements climatiques.

Gartner a effectué des recherches pour les entreprises qui cherchent à atténuer les risques liés aux changements climatiques. L'adaptation au climat crée une résilience organisationnelle en

réponse aux changements climatiques. Les organismes, y compris les FST, doivent utiliser des modèles de scénarios et des évaluations de risques pour cerner les menaces climatiques et y répondre tout en protégeant les revenus et la réputation de l'entreprise.

L'impact de la pandémie de COVID-19 ainsi que l'accélération de l'adoption du télétravail et de la transformation numérique dans les entreprises, les organisations et les gouvernements constituent un autre facteur qui touche toutes les administrations. Alors que de plus en plus d'entreprises continuent à travailler à distance et s'appuient davantage sur des services infonuagiques, le besoin de résilience des services de télécommunication est d'autant plus important. Cette augmentation de la demande et du trafic, en particulier de la connectivité Internet haute vitesse, peut mettre à rude épreuve la capacité du réseau. L'évolution des habitudes d'utilisation peut entraîner des changements dans les heures de pointe et des besoins accrus en bande passante à certains moments de la journée, ce qui réduit les fenêtres de maintenance pour les fournisseurs de services. La décentralisation de la main-d'œuvre a accru les exigences en matière de fiabilité, de redondance et de résilience des infrastructures étendues, alors qu'auparavant l'accent était mis sur les centres urbains et les centres-villes.

3.2.2 Obligations réglementaires

Les fournisseurs de services de télécommunications (FST) sont soumis à diverses obligations réglementaires généralement établies dans la législation de chaque compétence au moyen de règles et de réglementations juridiquement contraignantes. Ces obligations peuvent prendre la forme de lois, de règlements, de règles, de permis, de licences, d'exigences de déclaration ou d'autres formes de mandats légaux. Ils comprennent souvent des dispositions relatives au contrôle, à l'application et aux sanctions en cas de non-conformité.

Des mesures de conformité peuvent être imposées si un FST ne fournit pas de service pendant une panne ou si les objectifs de service ne sont pas atteints lors de la reprise. Elles sont aussi généralement imposées si un FST ne respecte pas les obligations réglementaires en matière de fourniture de services d'urgence. Toutes ces mesures visent à prévenir, à réduire et à faciliter le rétablissement après une panne de réseau.

Tableau 9. Principaux enseignements pour les obligations réglementaires

Des services de communication essentiels accessibles à tous les citoyens	▪ Toutes les administrations ont adopté, sous une forme ou une autre, une obligation de service universel ou de service d'urgence. ▪ Certains FST sont chargés de fournir des services de base (généralement la téléphonie, l'accès à Internet et les services d'urgence) à tous les citoyens. ▪ Ces coûts sont généralement financés en partie par l'imposition d'une taxe aux FST qui ne sont pas facturés dans le cadre de l'obligation de service. ▪ La plupart des obligations de service universel concernent le service vocal, mais certains commencent à introduire le service à large bande comme service de base.

Systèmes de notification en cas de pannes et contrôles des rapports d'incidents	▪ La plupart des administrations disposent d'un cadre de déclaration obligatoire des incidents, avec des variantes, mais avec trois (3) éléments communs. 1. Définition du champ d'application des fournisseurs de communications couverts – typiquement classés en fonction du type de service fourni ou de l'infrastructure. 2. Seuils de panne ou d'incident – classés par type d'incident et/ou répercussions de l'incident (nombre de clients touchés multiplié par la durée totale de la panne). 3. Délais de déclaration définis – le délai pour le premier avis est généralement de 1 à 3 heures en fonction de la gravité de l'incident.
Sanctions	▪ De nombreuses administrations disposent d'une réglementation qui sanctionne les FST par des SAP ou des sanctions financières en cas de non-conformité. • Les sanctions imposées sont déterminées en fonction des répercussions de la violation sur les consommateurs (types de services touchés, nombre de clients concernés et durée de l'événement) et du niveau de négligence (y a-t-il eu violation des pratiques exemplaires). ▪ Cependant, aucune des administrations interrogées n'avait défini de cadre pour déterminer la valeur des amendes potentielles.

Canada

Obligation de service universel

L'Obligation de service universel (OSU) au Canada vise à garantir que tous les Canadiens ont accès à des services de télécommunications abordables et fiables, y compris les services vocaux et l'Internet à large bande. Le CRTC a fixé des objectifs précis pour que ces services soient accessibles à toute la population canadienne, quelle que soit sa situation géographique.

En ce qui concerne les services vocaux, le CRTC a établi un OSU qui exige que toute la population canadienne doive disposer d'un accès Internet fiable et abordable et à des services vocaux locaux, y compris l'accès aux services d'urgence.

Appels d'urgence

Le Canada a élaboré des politiques réglementaires de télécom précises qui établissent le plan d'action concernant les services 9-1-1 du Conseil pour la fiabilité et la résilience des réseaux 9-1-1, y compris les avis aux centres d'appel 9-1-1 lorsque des pannes de réseau sont susceptibles de les toucher.

Toutes les entreprises qui fournissent des réseaux 9-1-1 doivent prendre toutes les mesures raisonnables pour s'assurer que leurs réseaux 9-1-1 sont fiables et résilients dans toute la mesure du possible. Il doit comporter une combinaison adéquate des pratiques exemplaires de l'industrie, qui doivent généralement inclure :

- les principes de conception du réseau 9-1-1;
- les pratiques d'exploitation et de maintenance du 9-1-1;
- les plans d'urgence pour le rétablissement des réseaux 9-1-1 après une catastrophe ou une panne;

- la surveillance des réseaux 9-1-1 en tout temps.

Le Conseil a également établi un cadre pour le processus d'avis afin de garantir que (i) les parties qui sont directement tenues de prendre des mesures pour rétablir le service puissent le faire rapidement, et que (ii) les parties puissent informer le public des mesures de rechange pour accéder aux services d'urgence si le délai de réparation de la panne est long.

En ce qui concerne les services 9-1-1 de prochaine génération (9-1-1 PG), cela comprend la capacité de i) réacheminer le trafic vers d'autres centres d'appels de la sécurité publique (CASP) dans le cas où un CASP ne serait pas en mesure de répondre aux appels 9-1-1; ii) maintenir la fiabilité et la performance du réseau même lorsque les points de démarcation, les systèmes de traitement des appels et les téléphones sont séparés par une grande distance géographique; et iii) se procurer de l'équipement et des services interopérables auprès de différents revendeurs qui adhèrent tous à la norme i3 pour les services 9-1-1 PG (norme i3) de la National Emergency Number Association (NENA) approuvée par le Conseil.

Le Conseil a également ordonné aux fournisseurs de réseaux 9-1-1 PG d'inclure dans leurs ententes de service 9-1-1 PG des exigences obligatoires particulières pour l'interconnexion des CASP aux réseaux 9-1-1 PG afin d'assurer la compatibilité entre les réseaux 9-1-1 PG et les réseaux des CASP, ainsi que la fiabilité, la résilience et les mesures de sécurité pour les services 9-1-1 PG et les réseaux interconnectés.

Avis en cas de pannes et rapports d'incidents

Le Conseil a lancé un processus visant l'élaboration d'un cadre pour améliorer la fiabilité et la résilience des réseaux de télécommunications. Dans la première phase de ce processus, le Conseil a lancé une instance d'avis de consultation afin de recueillir des observations sur une proposition en vue d'exiger toutes les entreprises canadiennes à transmettre un avis au Conseil, à ISDE et à d'autres autorités compétentes au sujet des interruptions de service majeures, et à soumettre au Conseil un rapport complet après l'interruption de service.

Dans l'attente du dénouement de l'avis de consultation 2023-39, le Conseil a ordonné à toutes les entreprises canadiennes, à titre provisoire, de fournir les renseignements suivants au Conseil, à compter du 8 mars 2023 :

- Les entreprises doivent aviser le Conseil dans les deux heures suivant le moment où elles prennent connaissance d'une « interruption de service majeure », définie aux fins de cette mesure provisoire comme toute panne touchant (i) plus de 100 000 abonnés ou une partie importante des abonnés de l'entreprise pendant plus d'une heure; (ii) les abonnés qui se trouvent dans une zone géographique desservie uniquement par l'entreprise concernée; (iii) les infrastructures essentielles; (iv) de grandes installations de transport; ou (v) un réseau 9-1-1.
- Les entreprises doivent fournir au Conseil, dans les 14 jours suivant la date à laquelle le Conseil a été informé d'une interruption de service majeure (comme exigé par le paragraphe 22a ci-dessus), un rapport complet détaillant : i) les causes de l'interruption de service; ii) les mesures prises pour résoudre l'interruption; iii) la façon dont les services d'urgence et d'accessibilité (y compris ceux adaptés aux personnes sourdes, malentendantes ou malvoyantes) ont été particulièrement touchés par l'interruption; et iv) les plans mis en place pour éviter des interruptions semblables à l'avenir.

Le Conseil a également indiqué qu'il lancerait d'autres instances publiques pour aborder la résilience des réseaux en termes plus généraux (par exemple, les principes de résilience des réseaux, les services d'urgence [9-1-1], les alertes au public, la communication avec les consommateurs, l'indemnisation des consommateurs, l'accessibilité, les mesures techniques et l'imposition de sanctions administratives pécuniaires).

Les renseignements sur les pannes de service au Canada sont affichés dans le domaine public sur la page Web suivante du CRTC : CRTC : Information générale – Pannes de service : 8000-C12-201909780.

Plans de remise en état

Comme d'autres administrations, le CRTC peut appliquer divers plans de remise en état pour résoudre les problèmes et assurer la conformité des FST. Bien que les plans particuliers puissent varier en fonction de la nature du problème, les mesures et les actions comprennent des exigences en vue de respecter les obligations de couverture, d'améliorer les niveaux de service ou d'investir dans les infrastructures afin d'améliorer la qualité du service. La plupart des plans de remise en état prévoient un suivi et des rapports obligatoires pour s'assurer que les plans sont respectés et que les résultats sont obtenus dans les délais prévus. Dans certains cas, des vérifications supplémentaires peuvent être prévues.

En outre, une proposition de loi a été déposée dans le cadre du projet de loi C-26. Les parties 1 et 2 comprennent les politiques pécuniaires administratives (PPA) et les régimes d'infraction en cas de non-conformité (les dispositions sont soumises à un examen parlementaire).

Sanctions administratives pécuniaires, amendes et sanctions

Le CRTC a la possibilité d'appliquer des SAP aux FST. Comme indiqué ci-dessus, une proposition de loi a été déposée dans le cadre du projet de loi C-26. Les parties 1 et 2 comprennent les SAP et les régimes d'infraction en cas de non-conformité (les dispositions sont soumises à un examen parlementaire).

Indemnisation des utilisateurs

Au Canada, les FST ne sont pas tenus d'indemniser les clients en cas de panne de service. Le droit à l'indemnisation est dicté par les circonstances propres à la panne et par l'accord contractuel entre les fournisseurs de services et leurs clients.

États-Unis

Obligation de service universel

Le service universel est une pierre angulaire de la loi qui a créé la Commission fédérale des communications (FCC), la *Communications Act of 1934*. Depuis lors, les politiques de service universel ont contribué à rendre le service téléphonique omniprésent, même dans les zones rurales éloignées. Aujourd'hui, la FCC reconnaît Internet haute vitesse comme la technologie de communication essentielle du XXIe siècle et s'efforce de rendre la large bande aussi omniprésente que les communications vocales, tout en continuant à soutenir le service vocal.

La *Loi* a établi des principes pour le service universel qui se concentrent spécifiquement sur l'amélioration de l'accès aux services évolutifs pour les consommateurs qui vivent dans les zones rurales et insulaires, ainsi que pour les consommateurs à faibles revenus.

Appels d'urgence

La *Wireless Communications and Public Safety Act of 1999* (*911 Act*) est entrée en vigueur en octobre 1999 dans le but d'améliorer la sécurité publique en encourageant et en facilitant le déploiement rapide d'une infrastructure de communication sans faille à l'échelle nationale pour les services d'urgence. L'une des dispositions de la *911 Act* demande à la FCC de faire du 911 le numéro d'urgence universel pour tous les services téléphoniques.

La FCC a pris plusieurs mesures pour renforcer la sécurité publique en encourageant et en coordonnant le développement d'un système de communication homogène à l'échelle nationale

pour les services d'urgence. La FCC a conçu et établi des périodes de transition pour rendre les infrastructures de communication du pays conformes.

Afin de fournir une aide d'urgence plus rapidement et plus efficacement, les entreprises et les organismes de sécurité publique améliorent régulièrement le réseau 9-1-1. Par exemple, la plupart des systèmes 9-1-1 transmettent désormais automatiquement le numéro de téléphone et la localisation des appels 9-1-1 effectués à partir de téléphones filaires, une fonctionnalité appelée service 9-1-1 évolué, ou E9-1-1.

La FCC exige également des entreprises de téléphonie sans fil qu'elles fournissent des services 9-1-1 et E9-1-1 lorsqu'un centre d'appels de la sécurité publique (CASP) en fait la demande. Lorsqu'il sera pleinement mis en œuvre, le service E9-1-1 sans fil fournira une localisation précise pour les appels 9-1-1 effectués à partir de téléphones sans fil.

D'autres règles de la FCC régissent le service 9-1-1 pour la voix par protocole Internet (VoIP), les services mobiles par satellite, la télématique et les appareils de télécommunication pour personnes sourdes (ATS). Les exigences relatives au service 9-1-1 constituent une partie importante des programmes de la FCC en vue d'appliquer les technologies de communication modernes à la sécurité publique.

Avis en cas de pannes et rapports d'incidents

Dans le cadre du mandat de la FCC, l'organisation est responsable de l'administration de deux bases de données et systèmes distincts pour les avis en cas de pannes et les rapports d'incidents relatifs aux services de télécommunication, à savoir le Système d'information sur les pannes de réseau (*Network Outage Reporting System* [NORS]) et le Système d'information sur les catastrophes (*Disaster Information Reporting System* [DIRS]).

Le NORS est un système de déclaration obligatoire qui permet à la FCC de recueillir des renseignements sur les perturbations importantes des services de communication susceptibles de compromettre la sécurité intérieure, la santé ou la sécurité publique ainsi que le bien-être économique du pays. Les fournisseurs de services de communication couverts par le mandat du Système comprennent les fournisseurs de services par ligne terrestre, par câble, par satellite, sans fil, par VoIP interconnectée et par système de signalisation no 7. Le cadre du système comprend des seuils et des directives qui déterminent si le fournisseur est tenu de répondre à un incident ou non. Ces lignes directrices comprennent, sans s'y limiter, les incidents qui perturbent 900 000 minutes d'utilisation ou les incidents qui touchent les services E9-1-1. Dans le cadre de l'Initiative d'intervention obligatoire en cas de catastrophe (*Mandatory Disaster Response Initiative*), les fournisseurs sont tenus de déclarer les pannes et les activités de rétablissement par l'intermédiaire des portails de la FCC (c'est-à-dire le NORS).

Les lignes directrices en matière de déclaration à l'intention des fournisseurs de services de communication sont les suivantes :

- Fournisseurs de services par ligne terrestre, par câble, par satellite, sans fil et par système de signalisation no 7 :
  - Envoyer un avis du NORS dans les 120 minutes suivant la réception des renseignements préliminaires sur la panne;
  - Soumettre un rapport de panne initial dans les trois (3) jours civils suivant la panne;
  - Soumettre un rapport final au plus tard 30 jours après la découverte de la panne.
- Fournisseurs de services par VoIP :
  - Envoyer un avis du NORS dans les 240 minutes suivant la découverte d'une panne susceptible de toucher une installation du service 9-1-1 ou dans les 24 heures suivant la découverte d'une panne susceptible de toucher

900 000 minutes d'utilisation et d'entraîner une perte totale de service ou susceptible de toucher des bureaux et installations spéciaux (qui comprennent toutes les installations inscrites au Programme de priorité des services de télécommunication avec une priorité de niveaux 1 et 2).
    - Soumettre un rapport final dans les 30 jours suivant la découverte de la panne.
- Les fournisseurs de services 9-1-1 couverts, ou les fournisseurs qui regroupent le trafic des appels 9-1-1 d'un fournisseur de services d'origine et le transmettent à un centre d'appel du service 9-1-1 :
    - Obligation d'aviser le responsable désigné du centre d'appel 9-1-1 au plus tard 30 minutes après la découverte d'une panne qui touche un centre d'appel 9-1-1.
    - Obligation de communiquer les renseignements importants supplémentaires au centre d'appel 911 concerné dès qu'ils sont disponibles, mais au plus tard deux heures après le premier contact.

Les renseignements et les données recueillis par le NORS sont utilisés par la Division de la cybersécurité et de la fiabilité des communications (*Cybersecurity and Communications Reliability Division*) du Bureau de la sécurité publique et de la sécurité intérieure (*Public Safety and Homeland Security Bureau*) pour évaluer l'impact des pannes majeures, cerner les tendances et créer les pratiques exemplaires susceptibles de prévenir ou d'atténuer les pannes à l'avenir.

Le DIRS est un système de déclaration volontaire en ligne que la FCC a mis en place à la suite de la catastrophe naturelle de l'ouragan Katrina. L'objectif du DIRS est de permettre la collecte de renseignements sur l'état opérationnel et le rétablissement des fournisseurs de communications (y compris les fournisseurs de services par ligne terrestre, sans fil, de radiodiffusion, par câble, par VoIP interconnectée et à large bande) lors de catastrophes majeures et des efforts de rétablissement qui s'ensuivent. En outre, les fournisseurs de services de communication du DIRS disposent d'un moyen pour demander de l'aide lors de ces événements.

La FCC compile les données et fournit des renseignements sur l'état du réseau aux responsables fédéraux de la gestion des urgences, et publie des rapports publics contqui regroupent les renseignements sur le rétablissement. L'analyse des données du DIRS par la FCC permet de guider les efforts de rétablissement menés par les partenaires fédéraux et les évaluations de l'agence sur la fiabilité des communications pendant les catastrophes.

Le DIRS n'est activé par la FCC qu'en cas d'urgence majeure anticipée, comme un gros ouragan, ou à la suite d'une catastrophe imprévisible. La FCC annonce les activations du DIRS par des avis publics et des courriels adressés aux participants du DIRS.

Plans de remise en état

Outre son rôle d'administrateur des systèmes de déclaration NORS et DIRS, la Division de la cybersécurité et de la fiabilité des communications est également chargée de favoriser l'amélioration du réseau par des enquêtes sur les incidents, des processus menés par les parties prenantes et l'élaboration de règles. À la suite de l'enquête sur l'incident, la Division peut émettre un plan de conformité à l'intention des FST impliqués dans l'incident.

La structure et le contenu d'un plan de conformité diffèrent en fonction des circonstances de l'incident, mais l'objectif de tous les plans de conformité est de s'assurer que le personnel des plus grands FST comprend les causes de l'incident et est conscient des facteurs atténuants. En règle générale, les plans de conformité abordent des sujets tels que les procédures opérationnelles, l'élaboration de manuels et de listes de contrôle de conformité, un plan d'amélioration continue (formation et examen du matériel de conformité), une vue d'ensemble

des pratiques exemplaires et une feuille de route de remise en état (le délai est généralement compris entre 30 et 90 jours ouvrables).

Sanctions administratives pécuniaires, amendes et sanctions

- Amendes liées à des pannes de réseau qui ont bloqué les appels au 9-1-1 : La FCC a imposé des amendes d'un montant de 6 millions de dollars à AT&T, CenturyLink (aujourd'hui Lumen Technologies), Intrado et Verizon. Les amendes portent généralement sur la capacité des fournisseurs à prendre en charge les appels au 9-1-1 et à alerter la FCC et les opérateurs du 9-1-1 en temps utile en cas de panne.
- Amendes pour non-utilisation des fréquences attribuées : Verizon Communications Inc. VZ.N et son unité Straight Path Communications Inc. ont payé une amende civile de 614 millions de dollars à la FCC. L'organisme de réglementation des télécommunications a déclaré que ce règlement mettait fin à une enquête sur des allégations selon lesquelles Straight Path n'aurait pas utilisé les fréquences qui lui avaient été attribuées et, ce faisant, aurait enfreint les règles de la FCC en rapport avec environ 1 000 licences.

Indemnisation des utilisateurs

La législation américaine ne prévoit pas d'obligation générale pour FST d'indemniser les clients en cas de panne de service. La FCC n'impose pas d'indemnisation automatique, mais le droit à l'indemnisation est dicté par les circonstances propres à la panne et par l'accord contractuel entre les fournisseurs de services et leurs clients.

Royaume-Uni

Obligation de service universel

La *Communications Act 2003* prévoit également des dispositions en vue de garantir la qualité du service aux clients, sous la forme de la législation sur le service universel en téléphonie (*Telephony Universal Service Legislation*), et définit un ensemble minimum de services qui doivent être fournis à chaque personne, sur demande, à un prix abordable.
En mars 2018, le gouvernement a introduit une législation, *The Electronic Communications (Universal Service) (Broadband) Order 2018*, pour une obligation de service universel à large bande, afin de donner aux foyers et aux entreprises le droit de demander une connexion à large bande décente et abordable.

Appels d'urgence

L'Ofcom a également mis en place un programme de contrôle pour vérifier si les FST respectent leurs obligations en matière d'appels d'urgence, alors que le Royaume-Uni passe d'un système téléphonique analogique à un système numérique.
Les services vocaux numériques utilisent les mêmes câbles à fibre optique que les services à large bande, ce qui améliore la qualité de la voix pour les clients et réduit les coûts, la complexité et la consommation d'énergie pour les FST.

Le seul changement auquel les utilisateurs finals doivent s'attendre est qu'ils branchent leur combiné sur leur routeur plutôt que sur une prise murale spécifique.
Étant donné que les appels numériques dépendent de l'électricité, les FST devront également rendre leurs systèmes d'alimentation plus fiables.

Avis en cas de pannes et rapports d'incidents

L'article 105K de la *Telecommunications (Security) Act 2021* impose aux fournisseurs d'informer l'Ofcom de toute atteinte à la sécurité, qui est définie comme « tout ce qui compromet la disponibilité, la performance ou la fonctionnalité du réseau ou du service » [*Traduction*].

Il est à noter que cette évaluation concerne les FST et non les exploitants de services essentiels (EES). Il convient de noter que les EES peuvent avoir une incidence et une influence significatives sur la résilience des services de télécommunications et qu'ils doivent être pris en compte dans le cadre d'une stratégie de résilience plus large (par exemple, l'Ofcom dispose d'orientations pour les EES dans le cadre de leur sous-secteur numérique pour les systèmes de noms de domaine [DNS], les domaines supérieurs et les points d'échange Internet [IXP]; l'Union européenne et l'Allemagne prévoient des seuils pour des domaines tels que les DNS, les domaines supérieurs et les IXP).

En vertu de l'article 105A de la *Telecommunications (Security) Act 2021*, le champ d'application des atteintes à la sécurité comprend plusieurs situations, notamment les pannes de réseau ou de service et les incidents de cybersécurité. Les atteintes à la sécurité à déclarer à l'Ofcom sont définies comme suit :

- Toute atteinte à la sécurité qui entraîne des répercussions sur la disponibilité des services, qui atteint les seuils indiqués dans le tableau ci-dessous.
- Toute atteinte à la sécurité qui touche les réseaux ou les services impliqués dans la connexion des appels d'urgence (par exemple, les plateformes des agents de traitement des appels, l'acheminement des appels d'urgence) et qui entraîne une réduction de la capacité habituelle à répondre aux appels ou à les acheminer correctement.
- Toute atteinte à la sécurité qui pourrait, à la connaissance du fournisseur, entraîner des pertes de vies humaines.
- Toute atteinte à la sécurité qui implique des infractions importantes de la cybersécurité.
- Toute atteinte à la sécurité qui a été déclarée à d'autres agences ou services du gouvernement.
- Toute atteinte à la sécurité qui a été annoncée aux médias (sources d'information locales, nationales ou commerciales) à la connaissance du fournisseur.

Tableau 10. Seuils numériques des réseaux fixes

Type de réseau ou service	Nombre minimum de clients finals concernés	Durée minimale de la perte de service ou de la perturbation majeure
Réseau fixe d'accès aux services d'urgence	1 000	1 heure
Réseau fixe d'accès aux services d'urgence	100 000	N'importe quelle durée
Service ou réseau fixe de voix ou de données offert aux clients de détail	10 000 ou 25 % (voir la remarque 2 ci-dessous)	8 heures
Service ou réseau fixe de voix ou de données offert aux clients de détail	100 000	1 heure

Remarques concernant le tableau ci-dessus :

1. Un client est touché si les fonctions principales d'un réseau ou d'un service ne lui sont pas accessibles en raison de l'atteinte à la sécurité.

2. Ce seuil doit être interprété comme étant soit 10 000 clients finals, soit 25 % du nombre total de clients finals du fournisseur pour le service concerné, le chiffre le plus bas étant retenu.

Tableau 11. Seuils numériques des réseaux mobiles

Type de réseau/service	Nombre minimum de clients finals concernés	Durée minimale de la perte de service ou de la perturbation majeure
Réseau mobile d'accès aux services d'urgence	1 000	1 heure
Réseau mobile d'accès aux services d'urgence[2]	100 000	N'importe quelle durée
Service ou réseau de voix ou de données des exploitants de réseaux mobiles virtuels offert aux clients de détail[3]	25 % (voir la remarque 3 ci-dessous)	8 heures
Service ou réseau de voix ou de données d'exploitant de réseau mobile offert aux clients de détail	Voir les remarques[4]	

Remarques sur ce qui précède :

1. Un client est touché si les fonctions principales d'un réseau ou d'un service ne lui sont pas accessibles en raison de l'atteinte à la sécurité.
2. Les exploitants de réseaux mobiles virtuels (ERMV) doivent déclarer les atteintes à la sécurité de leurs clients finals, même si elles résultent d'une défaillance du réseau de l'exploitant de réseau mobile (ERM) qui les héberge. Dans ce cas, les coordonnées du tiers doivent être fournies.
3. Ce seuil doit être interprété comme représentant 25 % du nombre total de clients finals du fournisseur pour le service concerné.
4. En raison de la difficulté inhérente à la détermination du nombre exact de clients finals touchés par une atteinte à la sécurité des réseaux mobiles, l'Ofcom a convenu d'un processus de déclaration avec chacun des quatre exploitants de téléphonie mobile britanniques, en fonction de leur définition individuelle d'une interruption majeure de service (IMS). Les IMS du réseau sont des atteintes à la sécurité qui ont un impact significatif sur le réseau et sont portées à la connaissance de la direction de l'ERM. L'objectif ultime est de garantir la déclaration des atteintes à la sécurité des réseaux mobiles qui entraînent des perturbations similaires à celles qui doivent être déclarées sur les réseaux fixes. Les accords visent à garantir la cohérence entre les ERM en ce qui concerne la déclaration et le calcul de l'impact sur les clients. L'Ofcom réexaminera périodiquement les critères de déclaration avec les ERM afin de maintenir cette cohérence entre les ERM et entre les réseaux mobiles et fixes.

La *Telecommunications (Security) Act 2021* répartit les atteintes à la sécurité en deux catégories : les atteintes urgentes et les atteintes non urgentes. Les atteintes à la sécurité doivent être considérées comme « urgentes » si elles répondent à l'un des critères suivants :

- Toutes les atteintes à la sécurité qui impliquent des violations importantes de la cybersécurité qui doivent être déclarées en vertu des critères ci-dessus relatifs aux

« atteintes à la sécurité à déclarer » et qui nécessitent des mesures correctives urgentes.

- Les atteintes à la sécurité qui touchent des services offerts à au moins 10 millions d'utilisateurs finals.
- Les atteintes à la sécurité qui touchent des services aux utilisateurs finals et qui dépassent 3 millions d'heures d'utilisation. Ce chiffre doit être calculé en fonction de la durée de la perte ou de l'interruption du service et du nombre de clients finals concernés.
- Les atteintes à la sécurité qui font l'objet d'une couverture médiatique nationale, qu'elles atteignent ou non les seuils quantitatifs des tableaux 1, 2 et 3
- Les atteintes à la sécurité qui touchent des services essentiels du gouvernement ou du secteur public (par exemple, impact généralisé sur le 999, les numéros non urgents à 3 chiffres, les communications des services d'urgence).
- Toute atteinte à la sécurité susceptible de toucher la fourniture de services de gros aux fournisseurs de communications fixes et mobiles dans une zone géographique donnée.

Les exigences en matière de déclaration des atteintes à la sécurité urgentes sont les suivantes :

- Fournir un avis initial à l'Ofcom dans les 3 heures suivant le moment où le fournisseur a pris connaissance de l'atteinte à la sécurité.
- Fournir un rapport complet dans les 72 heures suivant l'avis initial.

Les atteintes à la sécurité doivent être considérées comme « non urgentes » lorsque la durée de la perte ou de l'interruption du service et le nombre de clients finals concernés est supérieure à 250 000 heures d'utilisation. Les exigences en matière de déclaration des atteintes à la sécurité non urgentes prévoient la présentation d'un rapport dans les 72 heures suivant la prise de connaissance de l'atteinte à la sécurité.

Toutes les atteintes à la sécurité inférieures au seuil de 250 000 heures d'utilisation perdues sont considérées comme « non majeures » et ne sont pas soumises à l'obligation de déclaration dans les 72 heures. Les atteintes à la sécurité non majeures pour un mois civil peuvent être déclarées par lots avant le deuxième lundi du mois suivant l'incident ou l'atteinte.

Plans de remise en état

Comme d'autres administrations, l'Ofcom pourra appliquer divers plans de remise en état pour résoudre les problèmes et assurer la conformité des fournisseurs de services de télécommunications. Bien que les plans particuliers puissent varier en fonction de la nature du problème, les mesures et les actions comprennent des exigences en vue de respecter les obligations de couverture, d'améliorer les niveaux de service ou d'investir dans les infrastructures afin d'améliorer la qualité du service. La plupart des plans de remise en état prévoient un suivi et des rapports obligatoires pour s'assurer que les plans sont respectés et que les résultats sont obtenus dans les délais prévus. Dans certains cas, des vérifications supplémentaires peuvent être prévues.

Sanctions administratives pécuniaires, amendes et sanctions

L'Ofcom tire ses pouvoirs en matière d'application de la *Communications Act 2003* et d'autres dispositions législatives. Lorsqu'il évalue les amendes ou les sanctions, l'Ofcom prend en compte des facteurs tels que la gravité de l'infraction, l'étendue du préjudice causé, la durée et l'impact de la panne, ainsi que les antécédents du fournisseur en matière de conformité. L'Ofcom vise des sanctions proportionnées et dissuasives qui reflètent la gravité de la non-

conformité ou de l'infraction. Il existe des limites légales aux amendes ou aux sanctions que l'Ofcom peut imposer. Ces limites varient en fonction du cadre réglementaire spécifique et de la nature de l'infraction. Par exemple, dans le cadre des Conditions générales de participation (*General Conditions of Entitlement*), qui définissent les obligations des fournisseurs de services de communication, la sanction maximale par infraction est fixée à 10 % du chiffre d'affaires du fournisseur. Avant d'imposer des amendes ou des sanctions, l'Ofcom entame généralement un processus de consultation avec le fournisseur, ce qui lui permet de répondre aux allégations et de présenter ses arguments.

Indemnisation des utilisateurs

L'Ofcom a mis en place un système d'indemnisation automatique qui permet aux clients de la large bande et de la ligne terrestre de se faire rembourser par leur fournisseur dans certaines conditions, sans avoir à en faire la demande. Une dizaine de fournisseurs ont adhéré au programme. Ce programme prévoit une indemnisation pour les réparations retardées à la suite d'une perte de service, pour les rendez-vous de réparation ou de mise au point manqués, et pour les retards dans la mise en place d'un nouveau service.

Australie

Obligation de service universel

L'obligation de service universel (OSU) est une protection de longue date des consommateurs qui garantit à chaque personne l'accès aux téléphones fixes et aux cabines téléphoniques, quel que soit son lieu de résidence ou de travail.

Telstra est responsable de l'exécution de l'OSU et doit fournir des services téléphoniques normalisés sur demande à tous les locaux en Australie dans des délais raisonnables. Il s'agit d'une obligation à la fois législative et contractuelle. Le ministère des Infrastructures, des Transports, du Développement régional, des Communications et des Arts contrôle la manière dont Telstra respecte l'OSU. L'OSU est régi par la *Telecommunications (Consumer Protection and Service Standards) Act 1999*. En décembre 2018, le gouvernement a annoncé que l'OSU serait intégrée dans une nouvelle Garantie de service universel (*Universal Service Guarantee* [USG]) plus vaste, qui comprend à la fois la large bande et les services vocaux.

Appels d'urgence

L'Australian Communications and Media Authority (ACMA) impose également aux FST de fournir un service d'appel d'urgence aux clients (*Telecommunications [Emergency Call Service] Determination 2019* et le Emergency Call Service Requirements Industry Code C526:2011), dont le non-respect est sanctionné par de lourdes amendes (comme l'amende de 400 000 dollars payée par le FST TPG en 2014 après une enquête de l'ACMA concernant une plainte déposée par un client qui avait essayé de composer le 0-0-0 en 2011 lorsque son partenaire avait été victime d'une crise cardiaque).

Les FST sont également tenus d'informer leurs clients au moins cinq jours ouvrables avant toute interruption de service, conformément au Code de protection des consommateurs des services de télécommunication (*Telecommunications Consumer Protections Code*) de l'Australie, et les opérateurs de télécommunications et les fournisseurs de services Internet (FSI) ont été condamnés à des amendes (nominales) ou ont reçu un avertissement formel de la part de l'ACMA dans le cadre de la réponse clémente de l'organisme de réglementation.

Avis en cas de pannes et rapports d'incidents

Les organismes australiens de réglementation des télécommunications ne disposent pas d'un mécanisme d'avis en cas de pannes des services de télécommunication ou de rapports d'incidents. L'Australian Cyber Security Centre (ACSC) impose aux propriétaires et exploitants d'infrastructures essentielles de déclarer les incidents de cybersécurité.

Plans de remise en état

Comme d'autres administrations, l'ACMA pourra appliquer divers plans de remise en état pour résoudre les problèmes et assurer la conformité des FST. Bien que les plans particuliers puissent varier en fonction de la nature du problème, les mesures et les actions comprennent des exigences en vue de respecter les obligations de couverture, d'améliorer les niveaux de service ou d'investir dans les infrastructures afin d'améliorer la qualité du service. La plupart des plans de remise en état prévoient un suivi et des rapports obligatoires pour s'assurer que les plans sont respectés et que les résultats sont obtenus dans les délais prévus. Dans certains cas, des vérifications supplémentaires peuvent être prévues.

Sanctions administratives pécuniaires, amendes et sanctions

Les critiques ont allégué que les organismes de réglementation australiens ont limité à la fois l'imposition d'amendes et le montant des amendes imposées. Cette situation a toutefois évolué récemment. Outre l'obligation de fournir des services, les FST et les FSI ont également été condamnés à des amendes par l'Australian Competition and Consumer Commission (ACCC) lorsqu'il s'est avéré qu'ils fournissaient des services de qualité inférieure aux clients. Dans un passé récent, l'ACCC a pénalisé le National Broadcasting Network (NBN) pour des services encombrés ou lents.

Indemnisation des utilisateurs

La Norme de garantie du service à la clientèle (*Customer Service Guarantee Standard*) de l'Australie protège les clients contre un service de mauvaise qualité. La Norme indique aux entreprises de télécommunications les délais dans lesquels elles doivent connecter ou réparer les lignes terrestres. Elle fixe également les indemnités qu'elles doivent verser si elles ne respectent pas ces délais. La Norme couvre les services téléphoniques et les rendez-vous sur le lieu de résidence de l'utilisateur, y compris la connexion d'un service et la réparation d'une panne ou d'un problème de service (c'est-à-dire que le client ne peut pas passer ou recevoir d'appels, qu'il est coupé à plusieurs reprises, qu'il subit de graves interférences qui ont une incidence sur le service ou qu'il est incapable d'utiliser le service). La norme ne couvre pas les services Internet et de téléphonie mobile. Cette garantie est assortie de nombreuses conditions et dépendances. Notamment, la Norme ne s'applique pas si une panne ou une perturbation du réseau résulte d'une catastrophe naturelle ou de conditions météorologiques extrêmes, de travaux de maintenance ou de mises à niveau planifiées, ou de dommages causés à leurs installations ou à leur réseau par un tiers. En cas d'interruption majeure des services, l'entreprise de télécommunications doit suivre les règles énoncées dans la Norme. Dans les 10 jours suivant le début de la perturbation, elles doivent écrire à toutes les personnes concernées ou publier un avis sur leur site Web et dans le journal local, et informer l'ACMA et le médiateur de l'industrie des télécommunications de la perturbation.

Nouvelle-Zélande

Obligation de service universel

Le cadre réglementaire des obligations de services de télécommunications (OST) [*telecommunications service obligations]* établi en vertu de la *Telecommunications Act 2001* permet à des services de télécommunication précis d'être disponibles et abordables.

Une OST est établie au moyen d'une entente en vertu de la *Telecommunications Act 2001* entre la Couronne et un fournisseur au titre de l'OST.

Il existe actuellement deux fournisseurs au titre de l'OST :

- Spark (soutenu par Chorus) est le fournisseur de l'OST pour le service téléphonique résidentiel local, qui comprend les appels locaux gratuits.
- Concentrix est le fournisseur du service de relais de télécommunication de la Nouvelle-Zélande pour les sourds, les malentendants et les personnes qui ont un trouble de la parole.

Les coûts de la subvention des services de télécommunication fournis dans le cadre des OST sont financés par la taxe de développement des télécommunications (*Telecommunications Development Levy*). Cette taxe est perçue auprès de l'industrie des télécommunications. La New Zealand Commerce Commission calcule les redevances des OST à verser à un fournisseur au titre de l'OST et la part de la taxe sur le développement des télécommunications qui incombe à chaque fournisseur.

Appels d'urgence

En Nouvelle-Zélande, les appels d'urgence sont passés en composant le 1-1-1. L'un des principaux éléments du système d'appel d'urgence est la Plateforme de prise d'appels initiale (*Initial Call Answering Platform*) pour la première réponse aux appels 1-1-1.

Spark gère la Plateforme de sorte que les appels d'urgence sont d'abord traités par un centre d'appel de Spark. Les appels d'urgence authentiques sont ensuite transmis au fournisseur de services d'urgence approprié (services de police, des pompiers, d'ambulance). Bien que les FST ne soient pas obligés de fournir des services d'appel d'urgence, ils sont encouragés à informer leurs clients sur l'accès aux appels d'urgence et sur la manière de les effectuer.

Le Telecommunications Forum fixe des normes minimales pour les services d'appel d'urgence au moyen de son code de pratique, le Code d'appel d'urgence (*Emergency Calling Code*).

Avis en cas de pannes et rapports d'incidents

Les organismes néo-zélandais de réglementation ne disposent pas d'un mécanisme d'avis en cas de pannes des services de télécommunications ou rapports d'incidents.

Plans de remise en état

Comme d'autres administrations, la New Zealand Commerce Commission pourra appliquer divers plans de remise en état pour résoudre les problèmes et assurer la conformité des FST. Bien que les plans particuliers puissent varier en fonction de la nature du problème, les mesures et les actions comprennent des exigences en vue de respecter les obligations de couverture, d'améliorer les niveaux de service ou d'investir dans les infrastructures afin d'améliorer la qualité du service. La plupart des plans de remise en état prévoient un suivi et des rapports obligatoires pour s'assurer que les plans sont respectés et que les résultats sont obtenus dans les délais prévus. Dans certains cas, des vérifications supplémentaires peuvent être prévues.

Sanctions administratives pécuniaires, amendes et sanctions

La New Zealand Commerce Commission n'impose pas d'amendes ou de pénalités spécifiques pour les pannes, mais elle a le pouvoir de faire respecter diverses exigences réglementaires.

Indemnisation des utilisateurs

Aucun cadre d'indemnisation automatique propre aux pannes des services de télécommunications n'a été recensé en Nouvelle-Zélande.

Japon

Obligation de service universel

La *Telecommunications Business Act (TBA)* définit les services de télécommunication universels comme des services essentiels à la vie des Japonais. En vertu d'une ordonnance de la *TBA*, les services pour les appels téléphoniques, publics et privés, les appels urgents aux services de police et des pompiers sont inclus dans les services universels.

Pour répartir une partie des coûts des services universels, des contributions appelées redevances de service universel sont perçues auprès des sociétés de téléphonie mobile, des sociétés de téléphonie fixe et des sociétés de téléphonie par VoIP, et les contributions sont distribuées aux fournisseurs de services universels NTT EAST et NTT WEST. Le montant des contributions se situe entre 2 ¥ et 3 ¥ par mois et par numéro de téléphone, et les contributions sont refilées aux utilisateurs finals dans la plupart des cas.

La large bande n'est pas estimée comme un service universel à l'heure actuelle, mais le ministère de l'Intérieur et des Communications envisage d'en faire un service universel.

Appels d'urgence

Au Japon, le numéro d'urgence principal à composer pour rapporter un délit ou demander de l'aide à la police est le 1-1-0. Pour les urgences médicales ou pour demander une ambulance, le numéro à composer est le 1-1-9. Ces numéros d'urgence sont largement reconnus et accessibles dans tout le pays.

En vertu de la *Disaster Countermeasures Basic Act*, le gouvernement est responsable de la mise en place et du maintien d'un système d'intervention d'urgence solide. Il doit notamment veiller à ce que les services d'appel d'urgence soient accessibles au public. Cette loi fixe des lignes directrices pour la création et le fonctionnement des centres d'appel d'urgence, en veillant à ce qu'ils disposent d'un personnel suffisant, qu'ils soient équipés de la technologie nécessaire et qu'ils soient en mesure de coordonner les interventions d'urgence.

Avis en cas de pannes et rapports d'incidents

La *TBA* du Japon donne au ministère des Affaires intérieures et des Communications (MAIC) le mandat de recueillir des renseignements sur les pannes, les accidents et les incidents liés aux télécommunications. La *TBA* définit deux catégories d'accidents et d'incidents pour lesquels les FST sont tenus de transmettre un avis au MAIC : 1) les accidents graves et 2) les accidents et incidents qui nécessitent un rapport trimestriel.

La *TBA* définit les accidents graves comme :

- des accidents dans lesquels une défaillance des installations de télécommunications (c'est-à-dire des machines, des équipements, des fils et des câbles ou toute autre installation électrique nécessaire aux télécommunications) se produit et entraîne l'interruption des services ou la détérioration de la qualité des services, à condition que le nombre d'utilisateurs touchés et la durée correspondent aux critères spécifiés dans la classification des services de télécommunication énumérés dans le tableau ci-dessous.

Tableau 12. Critères de la définition d'un accident grave en vertu de la *TBA*

Classification des services de télécommunication	Heures	Nombre d'utilisateurs concernés
1. Services de transmission de la voix avec appels d'urgence	1 heure	30 000
2. Services de transmission de la voix sans appel d'urgence	2 heures 1 heure	30 000 100 000
3. Téléphonie mobile (à l'exclusion des services de télécommunication énumérés aux points 1 et 2 ci-dessus) avec des services cellulaires étendus à basse consommation (installations radio qui répondent aux conditions spécifiées à l'article 49-6-9, paragraphes 1 et 5 ou paragraphes 1 et 6 de l'ordonnance du MAIC no 18 de 1950 : Règlements des installations radio) et les services étendus à basse consommation sans licence stipulés à l'article 1, paragraphe 2, point 18 des Règles de déclaration	12 heures 2 heures	30 000 100 000
4. Services liés à Internet qui ne reçoivent pas de paiement de la part des utilisateurs en compensation de la fourniture de services de télécommunication (à l'exclusion des services de télécommunication énumérés aux points 1 à 3 ci-dessus)	24 heures 12 heures	100 000 100 000
5. Les services de télécommunication autres que ceux énumérés aux points 1 à 4 ci-dessus	2 heures 1 heure	30 000 100 000

Les accidents dans lesquels une défaillance des installations de télécommunications importantes (par exemple, les satellites, les câbles sous-marins ou d'autres installations de télécommunications importantes semblables) entraîne l'interruption de toutes les communications pendant deux heures ou plus.

La *TBA* définit les accidents et les incidents qui nécessitent un rapport trimestriel comme :

- des accidents dans lesquels une défaillance des installations de télécommunications et de la fourniture de l'ensemble ou d'une partie des services de télécommunication entraîne l'interruption des services ou la détérioration de la qualité des services, à condition que le nombre d'utilisateurs touchés soit supérieur ou égal à 30 000 ou que la durée de l'accident soit supérieure ou égale à deux heures.
- des accidents dans lesquels une défaillance des installations autres que les installations de télécommunications se produit, la fourniture de services de télécommunication est perturbée, et le nombre d'utilisateurs touchés par l'accident est supérieur ou égal à 30 000 ou la durée est d'au moins deux heures.
- Les incidents au cours desquels des fuites de renseignements sur les installations de télécommunication peuvent perturber la fourniture des services de télécommunication.
- Les accidents et incidents causés par une défaillance des installations de lignes de transmission du système terminal (limitées à celles interconnectées aux installations de terminaux mobiles à une extrémité) interconnectées par voie hertzienne aux installations de télécommunications des utilisateurs à une extrémité.

- Les accidents causés par une défaillance des dispositifs d'hébergement à distance installés dans les stations ou des dispositifs d'hébergement à distance des lignes d'alimentation ou des points de contact, et dont l'étendue des répercussions est limitée à une partie de ceux qui utilisent la ligne hébergée par le dispositif.
- Les accidents causés par une défaillance d'un multiplexeur d'accès de ligne d'abonné numérique (MALAN), et dont l'étendue des répercussions est limitée à certains des utilisateurs de la ligne hébergée par le dispositif.

Plans de remise en état

Comme d'autres administrations, le MAIC pourra appliquer divers plans de remise en état pour résoudre les problèmes et assurer la conformité des FST. Bien que les plans particuliers puissent varier en fonction de la nature du problème, les mesures et les actions comprennent des exigences en vue de respecter les obligations de couverture, d'améliorer les niveaux de service ou d'investir dans les infrastructures afin d'améliorer la qualité du service. La plupart des plans de remise en état prévoient un suivi et des rapports obligatoires pour s'assurer que les plans sont respectés et que les résultats sont obtenus dans les délais prévus. Dans certains cas, des vérifications supplémentaires peuvent être prévues.

Sanctions administratives pécuniaires, amendes et sanctions

Aucun cadre propre aux sanctions administratives pécuniaires, aux amendes et aux sanctions appliquées par le MAIC n'a été recensé.

Indemnisation des utilisateurs

Aucun cadre d'indemnisation automatique propre aux pannes des services de télécommunications n'a été recensé au Japon.

Union européenne

Obligation de service universel

Dans le contexte de l'Union européenne, l'obligation de service universel fait référence à la Directive de service universel (DSU). La DSU est une directive européenne qui vise à garantir la disponibilité des services de communication de base à tous les citoyens de l'Union européenne, indépendamment de leur situation géographique ou de leur situation personnelle.

L'USD définit certaines obligations pour les États membres de l'Union européenne et les FST, notamment en ce qui concerne l'accès aux services de communication de base : les États membres doivent veiller à ce que des services abordables et de qualité, tels que la téléphonie classique, Internet haute vitesse et l'assistance-annuaire, soient disponibles pour tous les utilisateurs.

Appels d'urgence

Le 1-1-2 est devenu le numéro d'appel d'urgence unique à composer en Europe en 1991. Le Code des communications électroniques européen garantit que les Européens peuvent composer le numéro d'urgence européen 1-1-2 où qu'ils se trouvent en Europe. Le règlement sur l'itinérance oblige les fournisseurs de services d'itinérance à envoyer un message texte aux personnes qui se rendent dans un autre pays de l'Union européenne pour les informer du numéro d'urgence européen 1-1-2. Le 1-1-2 fonctionne parallèlement aux numéros d'urgence nationaux existants. Le Danemark, l'Estonie, la Finlande, Malte, les Pays-Bas, le Portugal, la Roumanie et la Suède ont opté pour le 1-1-2 comme seul numéro d'urgence national.

Avis en cas de pannes et rapports d'incidents

L'obligation de déclaration des FST dans l'Union européenne est régie par le cadre réglementaire de l'Union européenne pour les communications électroniques. Ce cadre comprend plusieurs directives et règlements qui décrivent les obligations et les exigences en matière de déclaration. Cela comprend les éléments suivants :

- Rapports d'incident ou de panne – y compris la nature, la portée et les répercussions de la panne ou de l'incident (par exemple, la durée, la zone géographique, le nombre d'utilisateurs touchés). Ce rapport doit également inclure les mesures prises ou les plans de rétablissement du ou des services.
- Rapports de suivi d'incident ou de panne – qui fournit des mises à jour sur l'avancement des efforts de rétablissement du service et sur toute mesure prise afin de prévenir des incidents futurs.
- Rapports annuels sur la transparence – y compris la couverture du réseau, la qualité du service, les tarifs et la part de marché.
- Rapports sur la qualité de service – qui comprend des indicateurs comme les taux d'interruption d'appels, les temps d'établissement d'une communication, les vitesses et les mesures de rendement du service.
- Rapports d'incidents de sécurité – incidents de sécurité et atteintes à la sécurité déclarés aux autorités réglementaires nationales (ARN) et, dans certains cas, aux équipes d'intervention en cas d'incident de sécurité informatique ou à d'autres organismes compétents.

Les exigences et procédures propres à la déclaration varient d'un État membre à l'autre : ils ont la possibilité de transposer le cadre réglementaire de l'Union européenne dans leur législation nationale. Par exemple, l'Allemagne a des exigences de déclaration obligatoire en cas d'atteinte à la sécurité et de pannes.

Afin de renforcer la cybersécurité à l'échelle européenne, la Directive sur la sécurité des réseaux et des systèmes d'information (Directive SRI) de l'Union européenne a été publiée en juin 2017. La Directive SRI2 actualisée est entrée en vigueur en 2023.

Par exemple, en Allemagne

L'organisme de réglementation ou de surveillance compétent dans ces cas est l'Agence fédérale des réseaux (*Bundesnetzagentur*). Elle exige de tous les FST qu'ils déclarent les incidents de sécurité.
En outre, les grands opérateurs qui sont considérés comme des opérateurs d'infrastructures essentielles doivent également rendre compte à l'Office fédéral allemand de la sécurité de l'information. La définition des infrastructures essentielles est concrétisée par les points 1 à 7 du *Règlement sur la désignation des infrastructures essentielles conformément à la* Loi de l'Office fédéral de la sécurité de l'information. Des seuils précis déterminent quand un opérateur d'infrastructure essentielle est soumis à la réglementation.
Les entreprises de télécommunications seront plus fortement réglementées à l'avenir (*Loi sur la sécurité des technologies de l'information*). Ils seront tenus d'avertir leurs clients s'ils détectent une utilisation abusive d'une connexion client. En outre, dans la mesure du possible, elles sont tenues de divulguer les solutions possibles aux personnes concernées.

Tableau 13. Seuils pour les opérateurs d'infrastructure essentielle en Allemagne

Type de réseau ou système	Seuil
Réseau d'accès	100 000 utilisateurs
Réseau de base	100 000
Station d'atterrissage de câbles sous-marins	1 câble de mer
Point d'échange Internet (IXP)	100 serveurs d'application connectés
Résolveur du système de noms de domaine (DNS)	100 000 participants au réseau d'accès
Serveur DNS autoritaire	250 000 domaines
Registre des domaines supérieurs	250 000 domaines
Centre de données	Puissance de 3,5 MW
Ferme de serveurs	10 000 à 15 000 occurrences
Réseau de diffusion de contenu	75 To de données par an

Remarque : Ces seuils ont été obtenus par l'analyse des administrations. Toutefois, des renseignements plus détaillés concernant les seuils peuvent être offerts.

Par exemple, en France

En France, le cadre des avis en cas de pannes des services de télécommunication et des rapports d'incidents relève de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP). Le Code des postes et des communications électroniques de la France comprend des exigences pour les opérateurs de télécommunications relatives aux conditions de continuité, de qualité, de disponibilité, de sécurité et d'intégrité du réseau et du service, aux normes et spécifications du réseau et du service, ainsi qu'au transfert gratuit des appels d'urgence et au transfert des communications des autorités publiques concernant des dangers imminents.

La France dispose de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Dans le cadre du dispositif du Secteur d'activité d'importance vitale (SAIV), l'ANSSI est informée par les opérateurs des incidents qui surviennent sur leurs systèmes d'information essentiels. Les types d'incidents à déclarer ont été précisés par des arrêtés sectoriels.

Plans de remise en état

Comme d'autres administrations, l'Union européenne peut appliquer divers plans de remise en état pour résoudre les problèmes et assurer la conformité des fournisseurs de services de télécommunication. La plupart des plans de remise en état sont laissés à l'appréciation des États membres. Bien que les plans particuliers puissent varier en fonction de la nature du problème, les mesures et les actions comprennent des exigences en vue de respecter les obligations de couverture, d'améliorer les niveaux de service ou d'investir dans les infrastructures afin d'améliorer la qualité du service. La plupart des plans de remise en état prévoient un suivi et des rapports obligatoires pour s'assurer que les plans sont respectés et que les résultats sont obtenus dans les délais prévus. Dans certains cas, des vérifications supplémentaires peuvent être prévues.

Sanctions administratives pécuniaires, amendes et sanctions

Si l'Union européenne peut infliger des amendes aux entreprises qui enfreignent la réglementation en matière de télécommunications et en cas de non-conformité persistante, la plupart des sanctions administratives pécuniaires, des amendes et des sanctions relèvent de la responsabilité des États membres.

Indemnisation des utilisateurs

Aucun cadre d'indemnisation automatique propre aux pannes des services de télécommunication pour l'ensemble de l'Union européenne n'a été recensé.

3.2.3 Mesures volontaires de l'industrie

Les organismes de réglementation et les groupes industriels de la quasi-totalité des administrations où l'on a effectué des recherches approfondies ont également élaboré des orientations volontaires à l'intention des fournisseurs de services. Elles comprennent des procédures opérationnelles normalisées, des lignes directrices, de pratiques exemplaires et des recommandations relatives à la fiabilité des réseaux et des services de télécommunication. Toutes ces mesures visent à prévenir, à réduire et à faciliter le rétablissement après une panne de réseau.

Tableau 14. Principaux enseignements des mesures volontaires de l'industrie

Collaboration	▪ Dans la plupart des cas, les organismes de réglementation collaborent avec des groupes de travail composés d'intervenants de l'industrie ou avec des comités directeurs sur la résilience pour élaborer les lignes directrices et les recommandations qu'ils publient. Le partage des enseignements tirés et des renseignements sur les nouvelles menaces et vulnérabilités facilite l'échange de connaissances et la mise en œuvre de stratégies de résilience efficaces. ▪ Les déclarations publiques faites par les gouvernements ou les organismes de réglementation et les codes de conduite volontaires élaborés conjointement aident à guider les fournisseurs de services vers une meilleure résilience.
Lignes directrices et recommandations de l'industrie	▪ Les types de lignes directrices et de recommandations publiées par les organismes de réglementation et les groupes industriels varient considérablement. ▪ Toutefois, les sujets les plus fréquemment abordés dans ces lignes directrices et ces recommandations sont les suivants : plans de reprise après sinistre, sécurité et résilience du réseau, alimentation de secours et redondance du réseau.

Élaboration et adoption de pratiques exemplaires	▪ Bien que les organismes de réglementation de la plupart des administrations publient des lignes directrices, des recommandations ou des pratiques exemplaires, l'approche traditionnelle est légère. ▪ Dans la plupart des administrations, l'industrie a été laissée libre de déterminer et de mettre en œuvre les pratiques exemplaires au sein de leurs réseaux de télécommunications. ▪ Toutefois, en raison du rythme rapide des innovations technologiques, certains organismes de réglementation ont estimé nécessaire d'introduire des orientations plus normatives et de procéder à des évaluations de la conformité.
Système de déclaration volontaire des pannes et des incidents	▪ Sur les six administrations, les États-Unis sont le seul organisme de réglementation à avoir mis en place un système de déclaration volontaire des incidents et des pannes. ▪ Le système de déclaration volontaire est activé lors de catastrophes majeures et permet aux FST de déclarer rapidement les dégradations de service et de demander de l'aide.

États-Unis

Procédures opérationnelles normalisées, lignes directrices et recommandations

La Commission fédérale des communications (FCC) a mis en place un comité appelé le Conseil pour la sécurité, la fiabilité et l'interopérabilité (*Communications Security, Reliability, and Interoperability Council* [CSRIC]) en vue de formuler des recommandations à la FCC sur la manière dont elle peut contribuer à garantir la sécurité, la fiabilité et l'interopérabilité des systèmes de communication.

Les recommandations du CSRIC portent sur une série de questions relatives aux communications relatives à la sécurité publique et à la sécurité intérieure, notamment : 1) la fiabilité des systèmes et de l'infrastructure de communication; 2) le service 9-1-1, le service 9-1-1 évolué (E9-1-1) et le service 9-1-1 de prochaine génération (9-1-1 PG); 3) les alertes d'urgence; et 4) les communications relatives à la sécurité nationale et à la préparation aux situations d'urgence, y compris l'accès des forces de l'ordre à ces communications.

Les recommandations portent sur la prévention et la correction des événements préjudiciables à la cybersécurité, l'élaboration de pratiques exemplaires afin d'améliorer la fiabilité globale des communications, la disponibilité et le rendement des services de communication et des alertes d'urgence lors de catastrophes naturelles, d'attaques terroristes, d'attaques de cybersécurité ou d'autres événements qui exercent une pression exceptionnelle sur l'infrastructure de communication, le rétablissement rapide des services de communication en cas de perturbations étendues ou majeures, et les mesures que les fournisseurs de services de communication peuvent prendre pour aider à assurer la sécurité des utilisateurs finals et des serveurs.

Tous les deux ans, depuis 2009, le CSRIC a été remanié pour traiter de nouvelles questions qui lui ont été confiées par le président de la FCC. En réponse à ces tâches, le CSRIC produit des rapports qui traitent de divers aspects des questions posées, y compris des recommandations et des pratiques exemplaires. (Rapports du CSRIC)

Les États-Unis ont également développé le Système d'information sur les catastrophes (*Disaster Information Reporting System* [DIRS]), un système de déclaration volontaire.

Royaume-Uni

Procédures opérationnelles normalisées, lignes directrices et recommandations

En ce qui concerne la résilience des réseaux, le Royaume-Uni n'a pas élaboré de normes ou d'exigences contraignantes particulières, mais il suit une approche communautaire pour élaborer des recommandations et des lignes directrices. Il est recommandé aux fournisseurs de mettre en œuvre les lignes directrices sur la résilience des infrastructures de télécommunications publiées par le Groupe de résilience et de réponse des communications électroniques (*Electronic Communications Resilience and Response Group*). Le Groupe est composé des principaux opérateurs de réseaux, des gouvernements britanniques et décentralisés et de l'Ofcom en tant qu'organisme de régulation. L'Ofcom a mis au point un programme d'essais de pénétration qui est basé sur les renseignements sur les menaces et qui simule une cyberattaque menée par un État-nation ou de grands groupes criminels organisés disposant de ressources considérables, et peut exercer ses pouvoirs prévus par la loi pour exiger d'un fournisseur qu'il se soumette à des tests afin de déterminer et de corriger toute vulnérabilité en matière de sécurité ou toute autre faiblesse dans les fonctions, les processus, les politiques, les systèmes ou les réseaux d'un fournisseur.

En outre, tous les opérateurs de services essentiels qui relèvent du *Security of Network & Information Systems Regulations 2018* (*Règlement SRI*) doivent se conformer à diverses exigences en matière de déclaration qui sont toujours basées sur la Directive sur la sécurité des réseaux et des systèmes d'information (Directive SRI) de l'Union européenne de 2018. Il s'agit principalement des exigences suivantes :

- exigences de sécurité (de haut niveau) pour les opérateurs de services essentiels;
- obligations de déclaration des incidents pour les opérateurs de services essentiels.

À la suite d'une consultation en 2022, le gouvernement a annoncé son intention de mettre à jour ces réglementations afin d'améliorer la cyber-résilience du Royaume-Uni. Les changements comprenaient l'ajout des fournisseurs de services gérés dans le champ d'application des règlements pour :

- améliorer la déclaration des cyberincidents aux organismes de réglementation;
- mettre en place un système de recouvrement des frais pour l'application du Règlement SRI;
- donner au gouvernement le pouvoir de modifier le Règlement SRI à l'avenir afin de garantir son efficacité;
- permettre au commissaire à l'information d'adopter une approche plus axée sur les risques pour réglementer les services numériques.

En 2018, l'Ofcom a imposé aux fournisseurs de services de communication d'offrir au moins une solution pour garantir une alimentation de secours d'au moins une heure pour l'infrastructure des télécommunications en cas de panne de courant.

Australie

Procédures opérationnelles normalisées, lignes directrices et recommandations

Les organismes de réglementation de l'Australie ne publient généralement pas de procédures opérationnelles normalisées, de lignes directrices de l'industrie ou de recommandations

relatives à la fiabilité et à la résilience des réseaux de télécommunications. L'approche actuelle consiste à s'appuyer sur la concurrence au sein du marché pour déterminer les pratiques exemplaires et améliorer la résilience des réseaux.

Cependant, dans le passé, des organismes de réglementation comme l'Australian Communications and Media Authority (ACMA) ont mené des enquêtes et publié des rapports sur la fiabilité et la résilience des réseaux de télécommunications du pays. Les enquêtes et les rapports sont généralement réalisés sur une base ponctuelle et en réponse à un incident majeur. Un exemple récent serait le rapport de l'ACMA (en collaboration avec la Communications Alliance et l'Australian Mobile Telecommunications Association [AMTA]) sur les répercussions des feux de brousse de 2019-2020 sur le réseau de télécommunications. Ce rapport fournit une analyse détaillée des renseignements obtenus auprès des entreprises sur les pannes et les événements de dégradation causés par les feux de brousse de 2019-2020 et propose des observations sur la résilience du réseau et l'utilisation de mesures de remise en état pour rétablir les services. Le rapport n'a pas formulé de recommandations ni déterminé de pratiques exemplaires en matière de résilience.

Nouvelle-Zélande

Procédures opérationnelles normalisées, lignes directrices et recommandations

Le Telecommunications Forum (TCF) de Nouvelle-Zélande et l'Internet Service Providers Association of New Zealand (ISPANZ) fournissent des ressources, des conseils et des forums de collaboration pour les FST. Ces organismes font la promotion de pratiques exemplaires, partagent les connaissances et défendent les intérêts de leurs membres.

Le Cadre de conformité aux codes (*Code Compliance Framework* [CCF]) du TCF est essentiel pour assurer la protection des consommateurs et maintenir la validité de l'autorégulation de l'industrie des télécommunications. Le CCF définit les processus, les rôles et les responsabilités du TCF et des signataires des codes en matière de surveillance et de déclaration de la conformité aux codes du TCF. L'administration du CCF est assurée par le responsable de la conformité aux codes du TCF, conformément aux procédures définies dans le manuel d'exploitation du CCF.

Le TCF comprend trois types de codes : les codes réglementés, les codes obligatoires et les codes volontaires. Un code réglementé est un code de pratique qui relève de la *Telecommunications Act 2001*, tel que déterminé par le ministre ou la New Zealand Commerce Commission de temps à autre. Un code obligatoire est un code autorégulé qui, selon le conseil d'administration du TCF, doit obligatoire être signé par tous les membres du TCF, dans le cadre de leur adhésion au TCF. Un code volontaire est un code autorégulé que les membres du TCF et d'autres parties peuvent choisir de signer.

Les lignes directrices de l'industrie n'exigent pas de signataires ni de conformité, mais elles constituent souvent le document de base d'ententes contraignantes entre les FST.

Japon

Procédures opérationnelles normalisées, lignes directrices et recommandations

L'Association des entreprises de télécommunications (*Telecommunications Carriers Association*) au Japon est une association industrielle qui représente les principales entreprises de télécommunications. Elle élabore et fait la promotion des lignes directrices et des pratiques exemplaires à l'échelle de l'industrie, notamment en ce qui concerne la sécurité des réseaux, la qualité des services, la préparation aux catastrophes et la protection des consommateurs. Le

comité du Conseil pour la sécurité et la fiabilité (Council for Safety and Reliability) encourage la coordination des activités des entreprises, y compris le partage de divers renseignements entre les entreprises, dans le but d'assurer la sécurité et la fiabilité des systèmes de télécommunications.
Le ministère des Affaires intérieures et des Communications (MAIC) prépare et publie des rapports qui déterminent les causes des incidents ou des événements. Les conclusions de ces rapports sont considérées comme des lignes directrices, mais elles ne sont pas assorties d'une application légale.

Union européenne

Procédures opérationnelles normalisées, lignes directrices et recommandations

L'Institut européen des normes de télécommunications (ETSI) est un organisme de normalisation indépendant et sans but lucratif dans le domaine de l'information et des communications. L'ETSI soutient le développement et la vérification de normes techniques mondiales pour les systèmes, applications et services qui reposent sur les technologies de l'information et des communications (TIC), y compris les technologies fixes, mobiles, radio, convergentes, de radiodiffusion et Internet.

L'ETSI a été créé par la Conférence européenne des administrations des postes et des télécommunications (CEPT). L'ETSI est l'organisme officiellement reconnu comme responsable de la normalisation des TIC. Il est l'un des trois organismes, les autres étant le Comité européen de normalisation (CEN) et le Comité européen de normalisation électrotechnique (CENELEC), officiellement reconnus par l'Union européenne en tant qu'organismes européens de normalisation (OEN). Le rôle des OEN est de soutenir la réglementation et les politiques de l'Union européenne en produisant des normes européennes harmonisées et d'autres produits. Les normes élaborées par les OEN sont les seules à pouvoir être reconnues comme normes européennes.

Une publication clé est le « Rapport sur les communications d'urgence : Aperçu de la préparation et de la résilience des réseaux de communication d'urgence (« *Emergency Communications [EMTEL]: Overview of Emergency Communications Network Resilience and Preparedness* »). Le rapport fournit des lignes directrices et des recommandations pour maximiser le niveau de préparation et de résilience des services de communication d'urgence en fonction des risques déterminés pour les technologies concernées. Les lignes directrices comprennent des concepts comme la résilience au niveau des composants, la diversité et la séparation des chemins et des routes, la tolérance aux pannes, la reprise après sinistre, la diversité des services, la segmentation du réseau et les opérations isolées.

Par exemple, en Allemagne

L'Agence fédérale des réseaux (*Bundesnetzagentur*), conformément à l'Office fédéral de la sécurité de l'information et le Commissaire fédéral à la protection des données et à la liberté d'information, a élaboré un Catalogue des exigences de sécurité pour l'exploitation des systèmes de télécommunication et de traitement des données et pour le traitement des données personnelles, qui sert de base au concept de sécurité. Le catalogue classe les opérateurs de réseaux publics de télécommunications dans la catégorie des opérateurs qui présentent un potentiel de risque accru et il définit les exigences de sécurité particulières qui doivent être mises en œuvre.

Une liste de fonctions essentielles pour les réseaux et services publics de télécommunications détermine les fonctions essentielles dont les composants sont couverts par le règlement. La directive technique TR-03163, « Sécurité de l'infrastructure de télécommunications », contient

les mécanismes de certification pertinents pour les composants essentiels des réseaux de télécommunications publics qui présentent un potentiel de risque accru.

Outre les services de télécommunications publics, il existe des réglementations propres aux fournisseurs de services numériques et les fournisseurs de services Internet.

Des recommandations propres aux fournisseurs de services Internet ont été élaborées par l'Office fédéral de la sécurité de l'information de l'Allemagne. Elles reflètent l'état de l'art (pratiques exemplaires actuelles) qui est mentionné dans des documents de niveau supérieur.

3.2.4 Autres initiatives et technologies en vue d'améliorer la résilience

Il existe également d'autres initiatives et technologies qui contribuent à améliorer la résilience et qui ne sont pas directement associées aux efforts de résilience des services de télécommunication ou qui offrent des avantages primaires dans un cadre adjacent ou extérieur des télécommunications commerciales ou de multiples secteurs. Ces éléments pourraient être pris en compte dans le cadre d'une approche générale et exhaustive en matière de résilience.

Tableau 15. Principaux enseignements des autres initiatives et technologies

Satellites en orbite basse (LEO)	▪ Les réseaux de télécommunications traditionnels reposent sur des infrastructures terrestres qui sont plus susceptibles d'être endommagées par des actes de sabotage intentionnels ou par des événements liés au changement climatique. Les satellites LEO sont moins sensibles aux problèmes localisés ou terrestres. ▪ En cas de panne ou de perturbation de l'infrastructure terrestre, les satellites LEO peuvent être utilisés pour rétablir rapidement la connectivité et assurer la continuité des communications, ce qui confère aux réseaux de télécommunications une résilience supplémentaire.
Réseaux à large bande pour la sécurité publique (RLBSP)	▪ Bien qu'il soit spécifiquement destiné aux agences de sécurité publique et aux premiers intervenants, ce réseau a parfois pour effet indirect d'améliorer la résilience des réseaux commerciaux. ▪ Le renforcement et la redondance de l'infrastructure qui sont exigés des entreprises de services sans fil participantes ou les opérateurs pour les réseaux à large bande de la sécurité publique sont parfois utilisés par les réseaux et l'infrastructure qui fournissent des services aux utilisateurs commerciaux.
Résilience électrique	▪ Dans les zones où les coupures de courant sont fréquentes, les FST peuvent mettre en place des solutions d'alimentation localisées, y compris des systèmes de secours dédiés avec des génératrices, des batteries de plus longue durée ou des installations d'énergie solaire sur les sites des tours cellulaires ou des équipements de réseau. ▪ En outre, de multiples nœuds de réseau interconnectés et des voies redondantes sont mis en place pour réacheminer le trafic en cas de pannes de courant à des endroits précis.

Hôte neutre ou adoption d'un réseau d'accès radioélectrique (RAN) ouvert	▪ Parmi les autres approches de l'architecture des réseaux de télécommunications, il y a l'adoption de solutions plus ouvertes et interopérables. ▪ Cette approche vise à introduire plus de flexibilité, d'interopérabilité et d'innovation en découplant le matériel, les logiciels et les vendeurs ou fournisseurs spécifiques.

Solution de rechange : Satellites en orbite basse

Les satellites en orbite basse (LEO) tournent autour de la Terre à une altitude inférieure à 2 000 km, ce qui leur permet d'offrir un meilleur rendement et une latence plus faible que les anciennes générations de satellites géostationnaires.

Les réseaux de télécommunications traditionnels s'appuient sur des infrastructures terrestres (comme des tours de téléphonie cellulaire ou des câbles terrestres et sous-marins) pour transmettre les signaux nécessaires aux communications, ce qui les rend vulnérables aux dommages causés par des actes de sabotage intentionnels ou par des événements liés au changement climatique. Les satellites LEO, quant à eux, opèrent principalement dans l'espace et sont donc moins sensibles à ces problèmes localisés. En cas de panne ou d'interruption de l'infrastructure terrestre, les satellites LEO peuvent être utilisés pour rétablir rapidement la connectivité et assurer la continuité des communications, ce qui confère aux réseaux de télécommunications une résilience supplémentaire. Outre l'avantage d'une résilience accrue, les satellites LEO présentent d'autres avantages :

- Couverture étendue : La proximité des satellites LEO par rapport à la Terre leur permet d'assurer une couverture plus large et d'atteindre même les zones éloignées ou mal desservies où l'infrastructure de télécommunications traditionnelle est limitée ou inexistante.
- Flexibilité et évolutivité : Les réseaux de satellites LEO peuvent être rapidement déployés et étendus pour répondre à une demande accrue ou pour fournir une couverture temporaire en cas d'urgence. Cette flexibilité les rend idéales pour répondre à des besoins de communication soudains, comme lors de catastrophes naturelles ou d'événements majeurs.

Bien que les administrations puissent utiliser des satellites LEO pour les services des FST afin de profiter des avantages potentiels, la mise en place d'une grande constellation est une entreprise complexe et coûteuse. La plupart des FST préfèrent s'associer à des fournisseurs existants d'accès Internet à large bande par satellite LEO afin d'éviter les frais généraux et les coûts d'une construction à partir de zéro.

Solution de rechange : Réseau à large bande pour la sécurité publique

- Un réseau à large bande pour la sécurité publique (RLBSP) offre une résilience et une robustesse supplémentaires aux premiers intervenants d'un pays.
- Ce réseau peut parfois améliorer la résilience des réseaux commerciaux (et des utilisateurs commerciaux), lorsque le renforcement de l'infrastructure et la redondance sont exigés des entreprises de services sans fil participantes ou des opérateurs.
- Les coûts sont généralement très importants.
- La plupart des administrations restent confrontées à des problèmes de couverture et de résilience sur le RLBSP.

Un RLBSP est un réseau de communication conçu spécifiquement pour être utilisé par les organismes de sécurité publique, comme les forces de l'ordre, les pompiers, les services médicaux d'urgence et les autres premiers intervenants.

Traditionnellement, les organismes de sécurité publique s'appuyaient sur des communications séparées et fragmentées qui n'étaient pas toujours interopérables. Ces systèmes comprenaient des systèmes radioélectriques mobiles terrestres (SRMT) et d'autres technologies anciennes. Toutefois, plusieurs administrations ont récemment mis en place leurs propres RLBSP, en utilisant généralement la technologie d'évolution à long terme (LTE) ou des réseaux sans fil semblables. Certains de ces RLBSP s'efforcent également de tirer parti des progrès récents dans le domaine des communications par satellite LEO. Les RLBSP fournissent généralement des capacités de transmission de données, de voix et de vidéo à haute vitesse. L'absence de services à large bande, le manque d'interopérabilité entre les agences et le coût élevé des services sont autant de facteurs qui incitent à lancer des initiatives de RLBSP à l'échelle nationale.

Les RLBSP offrent résilience et robustesse à la sécurité publique, afin d'améliorer l'efficacité et l'efficience des interventions d'urgence en fournissant des capacités de communication spécialisées et avancées aux premiers intervenants.

Les projets européens examinés utilisent généralement un modèle de réseau partagé par plusieurs entreprises qui sont chargées de fournir des services de sécurité publique et le réseau est partagé entre les utilisateurs de la sécurité publique et les clients habituels des opérateurs de réseaux mobiles (ORM).

Dans l'ensemble, il existe différents modèles commerciaux pour les ORM dans les projets existants, et aucun de ces modèles n'a atteint une position clairement dominante. La part des utilisateurs de la sécurité publique sur le RLBSP est généralement comprise entre 0,4 % et 0,8 %.

Le tableau suivant donne un aperçu de quelques exemples de RLBSP à l'échelle internationale.

Tableau 16. Exemples de réseaux à large bande pour la sécurité publique à l'échelle internationale

	États-Unis	Royaume-Uni	Australie	France	Belgique	Corée du Sud
Type	Entreprise unique	Réseau partagé par plusieurs entreprises	Réseau partagé par plusieurs entreprises	Réseau hybride ou plusieurs entreprises	Réseau partagé par plusieurs entreprises	Réseau dédié à la sécurité publique
Spectre	Spectre pour une entreprise unique	Pas de spectre dédié	Spectre pour plusieurs entreprises	Spectre pour plusieurs entreprises	Spectre pour plusieurs entreprises	Spectre limité
Réseau d'accès radioélectrique (RAN)	RAN pour une entreprise unique	RAN pour plusieurs entreprises	RAN pour plusieurs entreprises	RAN pour plusieurs entreprises	RAN pour plusieurs entreprises	RAN privés
Infrastructure	Qualité commerciale	Qualité commerciale	Qualité commerciale	Réseau central de qualité pour la sécurité publique	Qualité commerciale	Réseau central de qualité pour la sécurité publique

	États-Unis	Royaume-Uni	Australie	France	Belgique	Corée du Sud
Interopérabilité	Quelques défis	-	Haut niveau	Haut niveau		Haut niveau

Les réseaux centraux de qualité commerciale sont principalement conçus pour répondre aux besoins de communication des consommateurs et des entreprises. Les réseaux centraux de qualité pour la sécurité publique sont spécialement conçus pour prendre en charge la fourniture de services indispensables, une haute disponibilité et des fonctions de sécurité robustes.

L'interopérabilité des RLBSP désigne la capacité des différents réseaux à communiquer et à échanger des renseignements de manière transparente, plus que les réseaux normalisés. La priorité et la préemption des utilisateurs de la sécurité publique sur les réseaux sont appliquées pour assurer une fourniture de services robuste et résiliente.

États-Unis

AT&T FirstNet

Le réseau américain FirstNet est un réseau partagé avec accès prioritaire et préemption. Ce réseau a été mis en place par une loi fédérale américaine en 2012 grâce à l'attribution de 10 MHz de spectre (actuellement 20 MHz, 10 MHz jumelés) dans la bande des 700 MHz (bande 14) et à la création d'un organisme de surveillance gouvernemental appelé FirstNet.

Une fois FirstNet créée, elle a pris des mesures pour répondre aux exigences d'interopérabilité à l'échelle nationale, solliciter l'industrie au moyen d'un vaste processus de demande de renseignements, consulter les 56 États et territoires des États-Unis, compiler les données recueillies et publier une demande de propositions axée sur les objectifs.

Le déploiement des données à large bande sur le réseau LTE est actuellement positionné comme un système superposé aux SRMT vocaux existants, avec un financement séparé alloué aux deux agences.

Royaume-Uni

Réseaux des services d'urgence

Comme les États-Unis, le Royaume-Uni a commencé à déployer un RLBSP national, le Réseau des services d'urgence (*Emergency Services Network*), afin de remplacer le système par ondes Airwave des services de police, d'incendie et d'ambulance en Grande-Bretagne (Angleterre, Pays de Galles et Écosse) et de transformer leur mode de fonctionnement.

Le Réseau permettra une transmission rapide, sûre et sécurisée de la voix, de la vidéo et des données sur le réseau 4G et donnera aux premiers intervenants un accès immédiat à des données, des images et des renseignements vitaux dans les situations d'urgence et de première ligne.

L'investissement dans le Réseau permettra également d'améliorer la couverture du réseau 4G, ce qui permettra de composer le 9-9-9 à partir de n'importe quel téléphone mobile compatible 4G dans certaines des régions les plus reculées et les plus rurales de Grande-Bretagne, où cela n'était pas possible auparavant.

Grâce à la technologie mobile essentielle du Réseau, la communication entre les services d'urgence aura la priorité sur le reste du trafic sur le réseau, même aux heures de pointe dans les zones urbaines très fréquentées. Les services d'urgence et les autres premiers intervenants

pourront ainsi partager rapidement et en toute sécurité des données, des renseignements et des compétences indispensables depuis la ligne de front, au moment où le besoin s'en fait le plus sentir.

Toutefois, le Réseau diffère de FirstNet en ce sens qu'il remplacera le réseau de radiocommunication bidirectionnelle de type « presser pour transmettre » essentiel du Royaume-Uni, ce qui permettra à tous les services d'urgence d'avoir accès non seulement à des données, mais aussi à la voix indispensable. Le réseau commercial et le spectre existants d'EE seront utilisés pour fournir des services au Réseau, étant donné qu'aucun nouveau spectre n'a été attribué.

Bien qu'annoncé en 2015, le projet de Réseau a connu des retards et des coûts importants (2 milliards de livres pour le Réseau et 2,9 milliards de livres pour maintenir Airwave). Le ministère de l'Intérieur (*Home* Office) a mis fin prématurément à son contrat avec Motorola (contestations auprès de l'autorité de la concurrence et des marchés).

Australie

Réseau LTE avancé pour les services d'urgence de Telstra

L'Australie exploite son offre de Réseau LTE avancé pour les services d'urgence (LANES) avec un accès prioritaire à son réseau LTE commercial depuis 2016, et a ajouté en 2017 un système de type « presser pour transmettre » essentiel qui a été rendu possible par ses capacités de diffusion LTE existantes pour la transmission d'appels de type « presser pour transmettre » à des groupes.

Le gouvernement a réservé le spectre de 800 MHz et de 4,9 GHz du service mobile à large bande de la sécurité publique. LANES offre un service d'accès prioritaire de base ainsi qu'un service qui permet aux organismes qui ont besoin de communications d'urgence d'utiliser leur propre spectre LTE combiné à « une option d'extension sur le spectre LTE de Telstra » [*Traduction*].

L'Australie a réalisé une étude détaillée portant sur un modèle entièrement commercial, un modèle dédié à la sécurité publique et deux variantes hybrides. L'étude a conclu qu'un modèle commercial était la meilleure approche en raison de son coût et de sa complexité moindres. En outre, elle a conclu qu'il serait préférable de s'aligner sur les normes internationales telles que la LTE et sur les attributions des bandes de fréquences des autres membres de la communauté des télécommunications de l'Asie-Pacifique.

Le Réseau à large bande pour la sécurité publique (RLBSP) de l'Australie comporte encore de nombreuses zones où la connectivité est médiocre ou inexistante. Environ 15 % des grands axes routiers n'ont pas de couverture mobile et environ 30 % du réseau ferroviaire a une couverture médiocre ou inexistante. Il y a 4 000 zones sans réseau mobile qui ont été déclarées. La stratégie de connectivité de la Nouvelle-Galles-du-Sud vise à combler ces lacunes.

Enseignements tirés du déploiement des capacités en dehors de la zone de couverture commerciale :

- Certaines régions de l'Australie n'ont pas de couverture mobile commerciale à l'heure actuelle, mais elles sont couvertes par des réseaux radio mobiles terrestres. Les possibilités de réutilisation des infrastructures existantes sont limitées dans ces zones, car le coût du déploiement d'un réseau mobile permanent à large bande est jugé très élevé.

- Le coût de la construction d'une nouvelle station de base a été estimé trois fois supérieur à celui du déploiement d'un nouvel équipement sur une station de base existante, ce qui nécessite une approche ciblée. Des options moins coûteuses ont été envisagées : équipement de station de base transportable et large bande par satellite.
- Il est prévu d'accorder un financement de 40 millions de dollars pour étendre ou améliorer la couverture de la téléphonie mobile et la concurrence dans les régions et les zones reculées d'Australie, en cofinançant des infrastructures de télécommunications nouvelles ou modernisées dans 54 localités ciblées.

France

Réseau Radio du Futur

La France a commencé à lancer des appels d'offres pour certains aspects du développement du réseau. Dans le spectre de 700 MHz, 19 MHz ont été réservés à la protection publique et aux secours en cas de catastrophe (licences prises en 2019).

Avec le Réseau Radio du Futur (RRF), la France souhaite se doter d'un réseau de communication à haute vitesse (4G/5G) commun à toutes les entreprises de sécurité et de secours, ce qui leur permettra de communiquer instantanément entre elles tout en bénéficiant de nouvelles fonctionnalités telles que les appels vidéo, le partage de la position en direct, l'envoi d'électrocardiogrammes et l'interopérabilité.
Le RRF est la réponse de l'État à la modernisation des communications pour la sécurité et les premiers intervenants en cas d'urgence. Aujourd'hui, la plupart utilise des équipements radio conçus au début des années 1990, spécifiques à chaque force, et qui ne permettent pas la transmission de grandes quantités de données ou d'images en temps réel depuis le terrain.

La France prévoit un investissement de plus de 700 millions d'euros du ministère de l'Intérieur pour le RRF. Le ministère de l'Intérieur a commencé la construction du futur réseau en septembre 2022. La construction puis les essais d'une première version du RRF devraient s'étendre sur une période de 19 mois.

Belgique

ASTRID

La mission d'ASTRID est d'établir, d'exploiter, de maintenir et de mettre en œuvre l'élargissement d'un réseau de communications radio pour les transmissions de voix et de données pour les services d'urgence et de sécurité belges (Blue Light Mobile : une seule carte SIM donne accès à trois opérateurs belges et à des opérateurs dans quatre pays voisins dans un environnement prioritaire et sécurisé, commutation automatique, compatible avec les tablettes, les téléavertisseurs, les drones et les caméras).

Dans le cadre d'ASTRID, STI Engineering a fourni un total de 189 émetteurs de radiomessagerie à très haute fréquence et de grande puissance à la Belgique. La première phase du renouvellement du système a débuté en 2015, et 89 sites supplémentaires seront mis à niveau en 2021.

De nombreuses ententes ont dû être conclues avec des opérateurs commerciaux (ententes de niveau de service [ENS] et garanties pour la couverture, l'accès prioritaire et le service de communication) et la mise aux enchères de fréquences de la gamme de 700 MHz est prévue.

Le contrat initial, conclu en 2015, prévoyait que STI Engineering modifie ses processus de développement et de fabrication afin de se conformer à toutes les directives européennes, y compris le marquage « CE » et la directive relative à la limitation de l'utilisation de certaines

substances dangereuses dans les équipements électriques et électroniques. Les émetteurs ont été livrés pour la première phase en 2015, et la deuxième phase a été livrée au premier trimestre de 2021.

En tant qu'organisme consultatif officiel, le comité consultatif des utilisateurs représente les utilisateurs d'ASTRID et il est chargé de formuler des recommandations. ASTRID respecte la protection des données personnelles et a mis en place un système de surveillance pour garantir la conformité avec le *Règlement général sur la protection des données* (RGPD).

Corée du Sud

SAFENET

SafeNet permet aux policiers, aux pompiers et à d'autres groupes de fonctionnaires de communiquer à l'aide de terminaux spécialisés. Il fournit un réseau de communication unique à l'échelle nationale qui soutient un canal unique de commandement et de contrôle, ainsi qu'une réponse intégrée sur les lieux de catastrophe.

La Corée du Sud, par l'intermédiaire de son ministère de la Sécurité publique, a également choisi un opérateur de réseau mobile commercial existant pour fournir des services d'urgence à tous les utilisateurs de la sécurité publique en Corée du Sud.

Un appel d'offres a été lancé pour le déploiement de SafeNet. Samsung a remporté un contrat pour fournir des appareils aux utilisateurs. Le gouvernement national a réservé 20 MHz de la bande de 700 MHz. Une version d'essai de SafeNet a été menée pendant les Jeux olympiques d'hiver de 2018.

Les utilisateurs passeront d'une variété de systèmes de radiocommunication bidirectionnels au nouveau système, qui fournira des services de voix et de données essentiels comme le Réseau des services d'urgence du Royaume-Uni (fréquences dédiées dans les canaux de 700 MHz). Le système utilisera le réseau commercial existant (tours, liaison de retour), ainsi que l'équipement et le spectre de radiofréquence dédiés à la sécurité publique. Il n'est donc pas nécessaire d'accorder la priorité à la sécurité publique par rapport aux utilisateurs commerciaux.

L'opérateur choisi est payé par le ministère de la Sécurité publique pour fournir le service. Le gouvernement s'est engagé à consacrer 1,5 milliard de dollars à la construction du réseau. La Corée du Sud prévoit également de lancer un réseau LTE de sécurité publique maritime.

Solution de rechange : Réseau d'accès radioélectrique ouvert ou hôte neutre

L'adoption d'un réseau d'accès radioélectrique (RAN) ouvert fait référence à la mise en œuvre et au déploiement de réseaux de télécommunications qui adhèrent aux principes et aux spécifications d'une architecture de RAN ouverte et interopérable. Traditionnellement, le RAN désigne l'équipement et la technologie qui relient les appareils au réseau central d'un fournisseur de services sans fil.

L'adoption d'un RAN ouvert représente un changement par rapport aux solutions de RAN traditionnelles, fermées et propriétaires, proposées par des fournisseurs particuliers, en faveur d'une approche plus ouverte et désagrégée. Il vise à accroître la flexibilité, l'interopérabilité et l'innovation dans le domaine des RAN en découplant les composants matériels et logiciels.

4.0 Annexe 4.0

4.0 Annexe

4.1 Facteurs gouvernementaux pour l'amélioration de la résilience des réseaux – Détails

Canada

Aperçu de la législation et des cadres réglementaires sur la résilience

Exemples de règlements du CRTC en vue d'améliorer la résilience et la fiabilité des réseaux et des services de télécommunication

Section – A

Décisions et politiques réglementaires du CRTC

Le Conseil de la radiodiffusion et des télécommunications canadiennes (Conseil) a pour mandat de réglementer et de surveiller les télécommunications dans l'intérêt du public et de veiller à ce que la population canadienne ait accès à un système de communication de classe mondiale qui encourage l'innovation et enrichit sa vie. Le mandat du CRTC est établi par la loi et vise à atteindre les objectifs en matière de politique établis dans la *Loi sur les télécommunications* et la *Loi canadienne anti-pourriel* (*LCAP*).

La *Loi sur les télécommunications* stipule les objectifs en matière de politique suivants :

a. 7 b) permettre l'accès aux Canadiens dans toutes les régions – rurales ou urbaines – du Canada à des services de télécommunication sûrs, abordables et de qualité;

b. 7 c) accroître l'efficacité et la concurrence, sur les plans national et international, des télécommunications canadiennes.

En conséquence, le Conseil a imposé ou exigé la mise en œuvre de la résilience et de la fiabilité des réseaux et services de télécommunication dans le cadre de diverses instances de politique qui ont donné lieu à des décisions ou ordonnances relatives aux exigences techniques et opérationnelles en matière de résilience et de fiabilité pour la mise en œuvre de certains services de télécommunication de gros ou de détail réglementés.

En voici quelques exemples :

1. *Norouestel Inc. – Examen du cadre de réglementation*, Politique réglementaire de télécom CRTC 2011-771, 14 décembre 2011, qui comprenait la fiabilité des services offerts par Norouestel.
2. *Norouestel Inc. – Cadre de réglementation, plan de modernisation et questions connexes*, Politique réglementaire de télécom CRTC 2013-711, 18 décembre 2013, qui se penche sur la redondance et la fiabilité du réseau de Norouestel.
3. Dans la politique réglementaire de télécom 2018-123, le Conseil a exigé l'élaboration de règles opérationnelles et des cibles minimales pour les indicateurs de la qualité du service des concurrents relatifs aux rendez-vous d'installation et de réparation de l'accès haute vitesse (AHV) respectés, ainsi que des délais moyens pour les rendez-vous d'installation et de réparation de l'AHV.

4. *Élaboration du Fonds pour la large bande du Conseil*, Politique réglementaire de télécom CRTC 2018-377, 27 septembre 2018, en vue d'améliorer l'accessibilité et la fiabilité des services de télécommunication.
5. Dans le cadre des projets du Fonds pour la large bande, le Conseil examine les projets qui améliorent la fiabilité des réseaux de télécommunications. Par exemple : *Fonds pour la large bande – Acceptation de l'énoncé des travaux pour le projet d'accès et de services mobiles de TELUS Mobilité dans le nord de l'Alberta*, Ordonnance de télécom CRTC 2022-188, 19 juillet 2022.
6. *Norouestel Inc. – Demande de modification du processus d'approbation des tarifs pour les services Internet de détail de l'entreprise*, Décision de télécom CRTC 2022-343, 20 décembre 2022.
   Paragraphe 114 : « simplifier le processus d'approbation des tarifs des services Internet de résidence de détail par voie terrestre de Norouestel de façon ciblée, afin de promouvoir la disponibilité rapide dans toutes les régions du Grand Nord de services de télécommunication fiables et abordables de grande qualité qui répondent aux besoins économiques et sociaux des utilisateurs. »
7. *Norouestel Inc. – Service de raccordement de gros – Tarifs définitifs*, Ordonnance de télécom CRTC 2018-338, 31 août 2018, qui est l'approbation des Tarifs des services d'accès des entreprises (CRTC 21480). Voir les exigences de l'entente sur le niveau de service (ENS) à la page 31, 6b) :

(b) Cibles de l'ENS

Mesure	Cibles en matière de conditions de service de base	Cibles en matière de conditions de service moyennes	Cibles en matière de conditions de service élevées	Cibles en matière de conditions de service les plus élevées
Disponibilité du service	99,9 %	99,9 %	99,9 %	99,9 %
Perte de paquets	S. O.	<2 %	<1 %	<1 %
Latence	S. O.	<200 ms	<150 ms	<80 ms
Gigue	S. O.	<50 ms	<25 ms	<25 ms

Section – B

Rapports et décisions du Comité directeur du CRTC sur l'interxonnexion

Le Conseil a approuvé ou imposé la mise en œuvre de diverses recommandations concernant les exigences et les pratiques exemplaires en matière de résilience technique, opérationnelle et procédurale élaborées par le Comité directeur du CRTC sur l'interconnexion (CDCI) et ses divers groupes de travail, notamment le Groupe de travail Réseau (GTR), le Groupe de travail Services d'urgence (GTSU) et le Groupe de travail Plan de travail (GTPT).

En voici quelques exemples :

1. Dans la décision de télécom 2022-264, « le Conseil **approuve** le rapport de consensus BPRE096b concernant le formulaire d'identification de la tâche du Groupe de travail Plan de travail et les Lignes directrices canadiennes relatives à l'échange de données mises à jour, et **ordonne** aux fournisseurs de services de télécommunication

de passer à l'utilisation du protocole Transport Layer Security 1.3 pour l'échange de données sur des liaisons Application Statement 2 au plus tard le 30 juin 2023 ».

2. – *Groupe de travail Plan de travail du CDCI – Rapports et lignes directrices concernant la mise en œuvre d'un nouveau régime de qualité du service aux concurrents*, Décision de télécom CRTC 2021-340, 14 octobre 2021.
3. *Mise en œuvre d'un nouveau régime de qualité du service aux concurrents*, Décision de télécom CRTC 2020-408, 22 décembre 2020.
4. *Groupe de travail Services d'urgence du CDCI – Rapport de consensus sur les questions liées à la compatibilité, à la fiabilité, à la résilience et à la sécurité des services 9-1-1 de prochaine génération*, Décision de télécom CRTC 2019-353, 22 octobre 2019.
5. *Groupe de travail Réseau du CDCI – Rapport de non-consensus concernant les paramètres de la qualité du service pour définir le service d'accès Internet à large bande fixe de grande qualité*, Décision de télécom CRTC 2018-241, 13 juillet 2018.
6. *Groupe de travail Services d'urgence du Comité directeur du CRTC sur l'interconnexion – Rapport de consensus ESRE0077 concernant les pratiques exemplaires en matière de cybersécurité des centres d'appels de la sécurité publique dans un écosystème canadien du 9-1-1*, Décision de télécom CRTC 2018-79, 23 février 2018.
7. *Groupe de travail Services d'urgence du CDCI – Rapport de consensus concernant une norme d'architecture des réseaux 9-1-1 de prochaine génération pour le Canada*, Décision de télécom CRTC 2015-531, 30 novembre 2015.
8. *Groupe de travail Réseau du CDCI – Rapport de consensus sur les recommandations en vue de régler la question des attaques par déni de service en téléphonie contre les centres d'appels de la sécurité publique*, Décision de télécom CRTC 2015-432, 21 septembre 2015.
9. **NTRE076.docx** (en anglais seulement) : Formulaire d'identification de tâche 41 – Rapport final sur les risques d'attaques par déni de service téléphonique et par déni de service distribué provenant des réseaux 5G et IP) [*Traduction*]
10. **NTRE043.doc** (en anglais seulement) **:** Rapport de consensus, Recommandations sur l'atténuation de l'encombrement du réseau concernant la mise en œuvre du service d'avis de communication (SAC) [*Traduction*]
11. **NTRE061.pdf** (en anglais seulement) **:** Élaborer des recommandations sur les paramètres et les rapports appropriés pour définir un service d'accès à Internet fixe à large bande de haute qualité [*Traduction*]
12. **NTRE054.docx** (en anglais seulement) **:** Rapport de consensus, Attaques par déni de service téléphonique contre les centres d'appel de la sécurité publique (CASP) [*Traduction*]
13. **NTRE046.doc** (en anglais seulement) : Lignes directrices pour l'interconnexion IP à IP [*Traduction*]
14. **NTRE055.docx** (en anglais seulement) : Spécifications techniques - Spécifications du service d'alerte publique sans fil [*Traduction*]

Section – C

Résilience et fiabilité des réseaux 9-1-1

1. *Plan d'action concernant les services 9-1-1*, Politique réglementaire de télécom CRTC 2014-342, 25 juin 2014, où le Conseil a indiqué qu'il examinerait la fiabilité et la

résilience des réseaux 9-1-1, dont l'émission d'avis aux centres d'appel des services 9-1-1 lorsque des pannes sur les réseaux sont susceptibles de les affecter.

2. *Questions ayant trait à la fiabilité et à la résilience des réseaux 9-1-1*, Politique réglementaire de télécom CRTC 2016-165, 2 mai 2016, paragraphes 30 à 33 :

   30. Par conséquent, le Conseil **impose** l'obligation suivante comme condition en vertu de l'article 24 de la *Loi sur les télécommunications* (*Loi*) à toutes les entreprises qui constituent des fournisseurs de réseaux 9-1-1 :

   > *Les fournisseurs de réseaux 9-1-1 doivent prendre toutes les mesures raisonnables pour s'assurer que leurs réseaux 9-1-1 (tels que définis à la note de bas de page 12) sont fiables et résilients dans toute la mesure du possible.*

   31. Pour aider les parties à déterminer en quoi consisteraient des mesures raisonnables pour chacun de leurs réseaux, les fournisseurs de réseaux 9-1-1 devraient utiliser une combinaison adéquate des pratiques exemplaires de l'industrie qui devraient normalement comprendre ce qui suit :

   - les principes de conception de réseaux 9-1-1 (note de bas de page 13), p. ex. des solutions de secours aux composantes essentielles configurées de façon géoredondante, des interconnexions variées des réseaux d'origine vers les réseaux 9-1-1 (y compris les solutions de secours), la diversité de l'emplacement (ou du site), la diversité du réseau de transport (c.-à-d. divers itinéraires ne comportant aucun point de défaillance unique), un réseau disponible 99,999 % du temps, des circuits de fréquences vocales d'une catégorie de service d'au moins p 0,01 (note de bas de page 14) et la fourniture d'alimentation de secours d'une durée d'au moins 24 heures dans le cas des commutateurs du bureau central et de 72 heures pour les commutateurs de transit;
   - les pratiques en matière d'exploitation et d'entretien liées au 9-1-1 (p. ex. la vérification de la diversité de l'itinéraire ou un processus de gestion du changement en vue de protéger cette diversité);
   - les plans d'urgence en cas de sinistre ou de panne des réseaux 9-1-1 en vue de limiter autant que possible la probabilité et la durée de pannes imprévues des réseaux 9-1-1 qui touchent les services (c.-à-d. les pannes des réseaux 9-1-1 qui feraient en sorte que des appels au 9-1-1 ne soient pas transmis au CASP approprié);
   - la surveillance en tout temps des réseaux 9-1-1, de sorte que les problèmes de performance des réseaux 9-1-1, notamment les pannes, sont détectés et réglés rapidement.

   32. Le Conseil traitera, au cas par cas, toute plainte ou tout problème soulevé quant à la fiabilité et à la résilience d'un réseau 9-1-1 donné, et prendra des mesures d'application de la *Loi*, s'il y a lieu.

   33. Le Conseil encourage les CASP à mettre en œuvre leurs propres stratégies d'atténuation afin d'améliorer la fiabilité et la résilience de leur infrastructure et leurs procédures, comme offrir aux fournisseurs de réseaux 9-1-1 des entrées physiquement variées aux installations de transmission vers l'immeuble du CASP, posséder un emplacement de secours (ou d'évacuation)

doté de diverses entrées, et établir une entente de traitement des appels avec un CASP partenaire afin de traiter des appels pour le compte de l'autre pendant les pannes.

3. Au paragraphe 51 de la politique réglementaire de télécom 2016-165, le Conseil a défini l'objectif de la procédure de l'envoi d'un avis :

   51. L'objectif global visé par l'envoi d'un avis de panne du service 9-1-1 est de garantir i) que les parties devant intervenir directement pour rétablir le service peuvent le faire rapidement; ii) que les parties peuvent informer le public des autres moyens à utiliser pour communiquer avec les services d'urgence si le temps de réparation de la panne se prolonge.

Au paragraphe 65, le Conseil demande que le GTSU prenne les mesures suivantes :

- élabore, à l'intention des fournisseurs de réseaux 9-1-1 et des entreprises FST, les procédures et les mécanismes en matière d'avis de panne du service 9-1-1 en se fondant sur les principes et les scénarios susmentionnés;
- présente ses recommandations au Conseil dans les **six mois** suivant la date de la présente décision.

En réponse, le GTSU a soumis le rapport ESRE0076 qui a été approuvé dans la décision de télécom 2017-389.

Le GTSU a mis à jour le processus d'envoi d'avis pour les services 9-1-1 de prochaine génération dans son rapport ESRE0098.

4. *9-1-1 de prochaine génération – Modernisation des réseaux 9-1-1 afin de satisfaire aux besoins des Canadiens en matière de sécurité publique*, Politique réglementaire de télécom CRTC 2017-182, 1 juin 2017, qui énonce des obligations en matière de fiabilité et de résilience, de sécurité et de souveraineté des composantes et des données.
5. *Groupe de travail Services d'urgence du Comité directeur du CRTC sur l'interconnexion – Rapport de consensus ESRE0077 concernant les pratiques exemplaires en matière de cybersécurité des centres d'appels de la sécurité publique dans un écosystème canadien du 9-1-1*, Décision de télécom CRTC 2018-79, 1 juin 2018.
6. *Groupe de travail Services d'urgence du CDCI – Rapport de consensus sur les questions liées à la compatibilité, à la fiabilité, à la résilience et à la sécurité des services 9-1-1 de prochaine génération*, Décision de télécom CRTC 2019-353, 22 octobre 2019.
7. *Modification du cadre des services 9-1-1 de prochaine génération afin d'intégrer des solutions de traitement des appels hébergées pour les centres d'appels de la sécurité publique*, Décision de télécom CRTC 2022-284, 17 octobre 2022, paragraphe 22 :

   22. Les interventions relatives à la souplesse supplémentaire offerte par le réseau 9-1-1 PG sur IP reflètent l'objectif du Conseil d'utiliser des solutions basées sur des normes qui permettent la souplesse. En ce qui concerne les services 9-1-1 PG, cela comprend la capacité de i) réacheminer le trafic vers d'autres CASP dans le cas où un CASP ne serait pas en mesure de répondre aux appels 9-1-1; ii) maintenir la fiabilité et la performance du réseau même lorsque les points de démarcation, les systèmes de traitement des appels et les téléphones sont séparés par une grande distance géographique; et iii) se procurer de l'équipement et des services interopérables auprès de différents revendeurs qui adhèrent tous à la norme i3 pour les services 9-1-1 PG (norme i3) de la National Emergency Number Association (NENA) approuvée par le Conseil.

8. Dans la décision de télécom CRTC 2019-353, le Conseil a ordonné aux fournisseurs de réseaux 9-1-1 PG d'inclure dans leurs ententes de service 9-1-1 PG des exigences obligatoires particulières pour l'interconnexion des CASP aux réseaux 9-1-1 PG afin d'assurer la compatibilité entre les réseaux 9-1-1 PG et les réseaux des CASP, ainsi que la fiabilité, la résilience et la sécurité des services 9-1-1 PG et les réseaux d'interconnexion.

Section – D

Exigences de production de rapports au sujet des interruptions de service du CRTC

Dans *Appel aux observations – Élaboration d'un cadre réglementaire pour améliorer la fiabilité et la résilience des réseaux – Obligations en matière de transmission d'avis et de production de rapports lors d'interruptions de services de télécommunication majeures*, Avis de consultation de télécom CRTC 2023-39, 22 février 2023, le Conseil a lancé un processus d'élaboration d'un cadre en vue d'améliorer la fiabilité et la résilience des réseaux de télécommunication. Comme première étape du processus, le Conseil a lancé l'instance d'avis de consultation afin de solliciter des observations concernant une proposition en vue d'exiger que toutes les entreprises canadiennes, à l'avenir et comme condition de service imposée en vertu de l'article 24 de la *Loi sur les télécommunications,* :

- de transmettre un avis au Conseil, à ISDE et aux autres autorités compétentes au sujet des interruptions de service majeures;
- de soumettre au Conseil un rapport complet après l'interruption de service.

En attendant le dénouement de cette instance, le Conseil a ordonné à toutes les entreprises canadiennes (telles que définies dans la *Loi sur les télécommunications*), à titre provisoire, de fournir les renseignements suivants au Conseil, à compter du 8 mars 2023 :

- Les entreprises doivent aviser le Conseil dans les deux heures suivant le moment où elles prennent connaissance d'une « interruption de service majeure », définie aux fins de cette mesure provisoire comme toute panne touchant (i) plus de 100 000 abonnés ou une partie importante des abonnés de l'entreprise pendant plus d'une heure; (ii) les abonnés qui se trouvent dans une zone géographique desservie uniquement par l'entreprise visée; (iii) les infrastructures essentielles; (iv) de grandes installations de transport; ou (v) un réseau 9-1-1.
- Les entreprises doivent fournir au Conseil, dans les 14 jours suivant la date à laquelle le Conseil a été informé d'une interruption de service majeure (comme exigé par le paragraphe 22a ci-dessus), un rapport complet détaillant : i) les causes de l'interruption de service; ii) les mesures prises pour résoudre l'interruption; iii) la façon dont les services d'urgence et d'accessibilité (y compris ceux adaptés aux personnes sourdes, malentendantes ou malvoyantes) ont été particulièrement touchés par l'interruption; et iv) les plans mis en place pour éviter des interruptions semblables à l'avenir.

Le Conseil a également indiqué qu'il amorcera d'autres instances publiques pour aborder la résilience des réseaux en termes plus généraux. Ces instances peuvent porter sur des questions telles que les principes de résilience des réseaux, les services d'urgence (9-1-1), les alertes au public, la communication avec les consommateurs, l'indemnisation des consommateurs, l'accessibilité, les mesures techniques et l'imposition de sanctions administratives pécuniaires.

Renseignements concernant les causes des récentes pannes au Canada :

Les renseignements sur les pannes de service au Canada sont affichés dans le domaine public sur la page Web suivante du CRTC : CRTC : Information générale – Pannes de service : 8000-C12-201909780.

Depuis mars 2023, les entreprises ont soumis les avis de panne requis au Conseil. Voici un résumé général des causes des pannes de service.

Tableau 17. Causes des interruptions de service majeures du 8 mars 2023 à aujourd'hui

Causes des interruptions de service	Nombre d'interruptions de service déclarées pour chaque cause
Erreur de procédure (par exemple, mise à jour du logiciel ou du matériel…)	4
Actions de tiers (par exemple, coupures de fibres)	2
Événements météorologiques (y compris ceux qui ont provoqué des pannes d'électricité)	5

États-Unis

Aperçu de la législation et des cadres réglementaires sur la résilience

La Commission fédérale des communications (FCC) est le principal organisme de régulation des télécommunications aux États-Unis. La FCC réglemente les communications interétatiques et internationales par radio, télévision, fil, satellite et câble dans les 50 États, dans le District de Columbia et dans les territoires des États-Unis. Agence indépendante du gouvernement des États-Unis supervisée par le Congrès, la FCC est l'agence fédérale responsable de la mise en œuvre et de l'application de la législation et de la réglementation américaines en matière de communications.

La ***Communications Act of 1934*** a combiné et organisé la réglementation fédérale des communications téléphoniques, télégraphiques et radiophoniques. Cette loi a permis de créer la FCC pour superviser et réglementer ces industries. Cette loi est mise à jour périodiquement pour ajouter des dispositions qui régissent les nouvelles technologies de communication, comme la télévision par ondes hertziennes, par câble et par satellite.

La *Communications Act*, telle qu'amendée, est une loi de grande envergure qui réglemente les communications téléphoniques, télégraphiques, télévisuelles et radiophoniques aux États-Unis. Ses sept sous-chapitres réglementent pratiquement tous les aspects de l'industrie des communications et de la radiodiffusion, y compris l'attribution des fréquences, les tarifs et les redevances, les normes, la concurrence, les conditions d'accès des abonnés, les messages publicitaires, la radiodiffusion dans l'intérêt public, l'utilisation des systèmes de communication par les pouvoirs publics. Cette loi prévoit également une réglementation et une surveillance plus détaillées grâce à la création de la FCC.

La ***Telecommunications Act of 1996*** a constitué la première révision majeure de la législation sur les télécommunications en près de 62 ans après la *Communications Act*. L'objectif de cette loi est de permettre à n'importe qui d'entrer dans n'importe quelle entreprise de communication – de permettre à n'importe quelle entreprise de communication de concurrencer n'importe

quelle autre entreprise sur n'importe quel marché. Cette loi contient des dispositions qui permettent à la FCC d'élaborer des règles équitables pour cette nouvelle ère de concurrence.

L'**ordonnance relative à l'Internet ouvert de 2015 de la FCC** adopte des règles solides et durables fondées sur de multiples autorisations légales afin de protéger l'Internet ouvert et garantir que les Américains profitent des avantages économiques, sociaux et civiques d'un Internet ouvert aujourd'hui et à l'avenir.

La ***Digital Equity Act of 2021*** a été établie par la *Bipartisan Infrastructure Law*, également appelée *Infrastructure Investment and Jobs Act* (articles 60301-60307). En vertu de cette loi, la National Telecommunications and Information Administration (NTIA) utilisera les données sur les « populations couvertes » (le Census Bureau des États-Unis et la NTIA ont rassemblé et analysé les données fédérales pour déterminer et quantifier les huit différentes « populations couvertes » définies par la *Digital Equity Act of 2021*, qui, dans l'ensemble, ont historiquement connu des taux plus faibles d'utilisation des ordinateurs et d'Internet) et la disponibilité et l'adoption relatives de la large bande comme intrants dans sa formule de financement pour allouer des fonds aux États (y compris les 50 États, le District de Columbia et Porto Rico) en vue de la planification de l'équité numérique et de l'octroi de subventions pour la capacité. Le Census Bureau des États-Unis et la NTIA fournissent les données de la *Digital Equity Act* par l'intermédiaire de leur visualiseur de population (*Population Viewer*) et des fichiers de données afin que les utilisateurs puissent déterminer les besoins des populations non desservies et mal desservies et contribuer à y répondre.

Dans le cadre de la *Consolidated Appropriations Act of 2021*, la ***Access Broadband Act of 2021*** a été créée pour améliorer l'accès à Internet haute vitesse en étendant les réseaux à large bande aux collectivités qui en ont besoin. En outre, cette loi exige que la NTIA publie des estimations des répercussions économiques de ces efforts de déploiement de la large bande sur les économies locales, y compris tout effet sur les petites entreprises ou les emplois. Pour répondre à cette exigence, le Census Bureau des États-Unis et la NTIA ont créé le tableau de bord de l'accès à la large bande (***Access Broadband Dashboard***) pour les décideurs politiques et le public afin d'évaluer comment les changements dans la disponibilité et l'adoption de la large bande pourraient influencer les économies locales.

Initiatives en vue d'améliorer la puissance et la résilience du réseau

La ***Bipartisan Infrastructure Law*** prévoit un financement de 65 milliards de dollars pour aider à atteindre l'objectif de connecter tous les Américains à un Internet haute vitesse abordable et fiable.

Quatre agences dirigent cet effort : la National Telecommunications and Information Administration (NTIA), la Commission fédérale des communications (FCC), le Department of the Treasury, et le United States Department of Agriculture (USDA).

Cette initiative nationale comprend de nombreux programmes différents :

- Programme de connectivité abordable (*Affordable Connectivity Program*) : Ce programme aide les personnes dans le besoin à payer le service et la technologie Internet haute vitesse.
- Programme de déploiement, d'accès et d'équité de la large bande (*Broadband Equity, Access, and Deployment Program*) : Ce programme construit l'infrastructure d'Internet haute vitesse là où c'est nécessaire, soutient la formation professionnelle, fournit l'équipement nécessaire et encourage les partenariats pour que tout le monde puisse être en ligne.
- Programme d'infrastructure à large bande (Broadband Infrastructure Program) : Un programme destiné aux États et aux fournisseurs de serviceInternet pour soutenir les

projets d'infrastructure d'Internet haute vitesse. Il vise à étendre le service Internet dans les zones qui n'y ont pas accès.

- Fonds pour les projets d'investissement (Capital Projects Fund) : Ce programme aide les gouvernements des États à financer des projets d'investissement et d'infrastructure. Il vise à l'expansion d'Internet haute vitesse pour fournir des services essentiels.
- Programme pilote Connecter les communautés minoritaires (*Connecting Minority Communities Pilot Program*) : Ce programme aide les collèges et les institutions qui desservent les communautés minoritaires et tribales. Il fournit des fonds pour l'achat d'équipement Internet et l'embauche de personnel pour aider avec la technologie.
- Programmes de la *Digital Equity Act* : Cette loi prévoit 2,75 milliards de dollars pour établir trois programmes de subventions en vue de promouvoir l'équité et l'inclusion numériques. Ces programmes visent à garantir que toutes les personnes et les communautés disposent des compétences, de la technologie et des capacités nécessaires pour tirer pleinement parti de l'économie numérique.
- Programme de subventions pour les infrastructures intermédiaires à large bande (*Enabling Middle Mile Broadband Infrastructure Grant Program*) : Ce programme permet d'étendre l'infrastructure intermédiaire. Il vise à réduire le coût de la connexion des zones non desservies et mal desservies.
- Programme de prêts et de subventions « ReConnect » (*ReConnect Loan and Grant*) : Ce programme aide à étendre l'accès Internet haute vitesse dans les zones rurales. Les fonds servent à financer la construction, les installations et l'équipement.
- Programme de subvention pour la planification de l'équité numérique dans les États (*State Digital Equity Planning Grant Program*) : Un programme de subvention de 60 millions de dollars pour les États, les territoires et les gouvernements tribaux afin d'élaborer des plans d'équité numérique.
- Programme tribal de connectivité à large bande (*Tribal Broadband Connectivity*) : Ce programme aide les communautés tribales à développer l'accès et l'adoption d'Internet haute vitesse sur les terres tribales.

Programme de recherche et développement sur l'infrastructure des réseaux mobiles sécurisés et résilients et sur les communications d'urgence (*Secure and Resilient Mobile Network Infrastructure and Emergency Communications Research and development Program*)

Le Programme de recherche et développement sur l'infrastructure des réseaux mobiles sécurisés et résilients et sur les communications d'urgence (*Secure and Resilient Mobile Network Infrastructure and Emergency Communications Research and development Program*) de la Direction des sciences et technologie (S&T) du Département de la Sécurité intérieure apporte un soutien direct en matière de recherche et développement (R&D) aux priorités essentielles de la Cybersecurity & Infrastructure Security Agency (CISA) liées à la sécurisation et à la résilience de l'infrastructure 5G, à la mobilité pour les missions gouvernementales et aux capacités de communication d'urgence.

Les solutions élaborées dans le cadre de ces programmes de R&D interdépendants contribueront à sécuriser l'infrastructure des réseaux mobiles existants et de nouvelle génération pour les missions et les cas d'utilisation du gouvernement fédéral, ainsi qu'à sécuriser et à améliorer les capacités des systèmes de communication essentiels utilisés par les premiers intervenants du pays.

Le vaste projet de R&D sur l'infrastructure des réseaux mobiles sécurisés et résilients et les communications d'urgence est géré par l'Office of Mission Capability and Support de la Direction des S&T et contribue aux efforts complémentaires de R&D suivants :

- Projet de R&D sur l'infrastructure des réseaux mobiles sécurisés et résilients;
- Projet de R&D sur les communications d'urgence.

Plan national de communication d'urgence

Le Plan national de communication d'urgence (*National Emergency Communications Plan*) est le plan stratégique des États-Unis en vue de renforcer et d'améliorer les capacités de communication d'urgence. Le Plan s'inscrit dans la mission complexe de maintien et d'amélioration des capacités de communication d'urgence pour les intervenants et sert de feuille de route aux États-Unis pour assurer l'interopérabilité des communications d'urgence pour tous les ordres de gouvernement.

Le titre XVIII de la *Homeland Security Act* de 2002, telle que modifiée, exige que la CISA élabore le Plan afin de « fournir des recommandations sur la manière dont les États-Unis devraient soutenir et promouvoir la capacité des fournisseurs de services d'intervention d'urgence et des responsables gouvernementaux concernés à continuer de communiquer en cas de catastrophe et à assurer, accélérer et atteindre l'interopérabilité des communications d'urgence à l'échelle nationale » [*Traduction*]. Cette loi ordonne également à la CISA d'élaborer et de mettre à jour périodiquement le Plan en coordination avec les parties prenantes fédérales, étatiques, locales, territoriales, tribales et privées.

Diversification de la chaîne d'approvisionnement

Le gouvernement américain a récemment lancé le Fonds d'innovation pour la chaîne d'approvisionnement des services publics sans fil (*Public Wireless Supply Chain Innovation Fund*) [en anglais seulement], dont l'objectif principal est de diversifier les chaînes d'approvisionnement. Ce fonds prévoit un investissement de 1,5 milliard de dollars dans le développement de réseaux ouverts et interopérables.

L'objectif du Fonds d'innovation est de favoriser la concurrence, de réduire les coûts pour les consommateurs et les opérateurs de réseaux, de soutenir l'innovation dans l'écosystème mondial des télécommunications et de renforcer la chaîne d'approvisionnement de la 5G. Plus précisément, le premier cycle vise à étendre et à améliorer les essais afin de démontrer la viabilité de nouvelles approches et d'éliminer les obstacles à l'adoption de technologies sans fil comme les réseaux d'accès radioélectrique (RAN) ouverts. Les activités de recherche, de développement et d'essai menées dans le cadre du premier cycle seront les suivantes :

- Étendre les activités d'essai et d'évaluation acceptées par l'industrie pour évaluer et faciliter l'interopérabilité, le rendement ou la sécurité des réseaux d'accès radio 5G normalisés, ouverts et interopérables;
- Élaborer des méthodologies d'essai, nouvelles ou améliorées, pour vérifier, évaluer et valider l'interopérabilité, le rendement ou la sécurité de ces réseaux, y compris leurs composantes.

Les objectifs généraux sont notamment de permettre aux entreprises innovantes, en particulier les petites et moyennes entreprises, d'être compétitives sur un marché historiquement dominé par quelques fournisseurs, dont certains présentent un risque élevé en matière de sécurité.

Initiatives en vue d'améliorer la cybersécurité

Le décret 13800, intitulé « *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* » (Renforcer la cybersécurité des réseaux fédéraux et des infrastructures essentielles), a été publié le 11 mai 2017. À l'alinéa 2 d), le décret exige que les secrétaires au Commerce et à la Sécurité intérieure « mènent conjointement un processus ouvert et transparent pour déterminer et promouvoir les mesures prises par les parties prenantes

appropriées afin d'améliorer la résilience d'Internet et de l'écosystème des communications et d'encourager la collaboration dans le but de réduire considérablement les menaces perpétrées par des attaques automatisées et distribuées (par exemple, les réseaux de zombies). » [*Traduction*]

Royaume-Uni

Aperçu de la législation et des cadres réglementaires sur la résilience

L'Office of Communications (Ofcom) est l'organisme de réglementation et l'autorité en matière de concurrence pour les industries de la communication au Royaume-Uni. Il réglemente les secteurs de la télévision et de la radio, des télécommunications de lignes fixes, de la téléphonie mobile, des services postaux, ainsi que les ondes sur lesquelles fonctionnent les appareils sans fil.

La ***Communications Act 2003***, qui a remplacé la quasi-totalité de l'ancienne *Telecommunications Act 1984*, est la loi de base qui a institué l'Ofcom en tant qu'organisme de régulation de l'industrie des communications au sens large et qui a mis en œuvre le nouveau cadre réglementaire européen qui est entré en vigueur en juillet 2003. Au lieu de l'ancien régime d'attribution de licence de la *Telecommunications Act*, cette nouvelle loi réglemente les fournisseurs de services de communication au moyen d'autorisations générales qui doivent être respectées pour pouvoir opérer sur le marché.

L'article 51 définit les sujets qui peuvent être inclus par l'Ofcom dans les Conditions générales de participation (*General Conditions of Entitlement*). L'alinéa 51(1)c) précise qu'il s'agit de « conditions qui prévoient les dispositions que l'Ofcom estime appropriées pour assurer le fonctionnement correct et efficace des réseaux publics de communications électroniques » [*Traduction*] et autorise ainsi l'Ofcom à mettre en œuvre l'article 23 de la Directive concernant le service universel, intitulé « Intégrité du réseau ». Il l'a fait au moyen de la condition 3 des conditions de participation :

> **3. Fonctionnement correct et efficace du réseau**
>
> 3.1 Le fournisseur de services de communication prend toutes les mesures pratiquement réalisables pour maintenir, dans toute la mesure du possible : a) le fonctionnement correct et efficace du réseau téléphonique public qu'il fournit en permanence dans des emplacements fixes; et b) en cas de panne catastrophique du réseau ou en cas de force majeure, la disponibilité du réseau téléphonique public et des services téléphoniques accessibles au public qu'il fournit dans des emplacements fixes; et c) l'accès ininterrompu aux services d'urgence dans le cadre de tout service téléphonique accessible au public offert dans des emplacements fixes.
>
> 3.2 Le fournisseur de services de communication veille à ce que les restrictions qu'il impose à l'accès et à l'utilisation d'un réseau téléphonique public qu'il fournit dans des emplacements fixes pour assurer le respect du paragraphe 3.1 ci-dessus soient proportionnées, non discriminatoires et fondées sur des critères objectifs définis à l'avance.
>
> 3.3 Aux fins de la présente condition, le terme « fournisseur de services de communication » désigne une personne qui fournit un réseau téléphonique public dans des emplacements fixes ou des services téléphoniques accessibles au public dans des emplacements fixes. [*Traduction*]

L'alinéa 51(1)e) précise qu'il s'agit de « conditions qui exigent ou réglementent la fourniture, la disponibilité et l'utilisation, en cas de catastrophe, des réseaux de communications

électroniques, des services de communications électroniques et des installations associées » [*Traduction*] et permet ainsi l'Ofcom à mettre en œuvre des conditions qui imposent aux fournisseurs d'aider les gouvernements centraux et locaux en cas d'urgence.

Le paragraphe 12 de l'annexe A de la directive d'autorisation le permet expressément (mais ne l'impose pas) et maintient les obligations antérieures imposées aux opérateurs du service téléphonique public dans le cadre de leurs anciennes licences.

Voici les dispositions en vue d'assurer la résilience face aux catastrophes naturelles :

> **5. Planification d'urgence**
>
> 5.1 Sous réserve du paragraphe 5.3, le fournisseur de services de communication doit, à la demande et en consultation avec :
>
> a) les autorités responsables des services d'urgence;
>
> b) les services des gouvernements centraux et locaux que l'Ofcom peut désigner de temps à autre aux fins de la présente condition,
>
> prendre des dispositions pour la fourniture ou le rétablissement rapide des services de communication qui sont pratiquement réalisables et qui peuvent être raisonnablement nécessaires en cas de catastrophe.
>
> 5.2 Sous réserve du paragraphe 5.3, le fournisseur de services de communication doit, à la demande de toute personne désignée à cet effet dans ces dispositions, mettre en œuvre ces dispositions dans la mesure où il est raisonnable et possible de le faire.
>
> 5.3 Aucune disposition de la présente condition n'empêche le fournisseur de services de communication de :
>
> a) recouvrer des frais encourus pour l'élaboration ou la mise en œuvre de ces dispositions; ou
>
> b) subordonner la mise en œuvre de ces dispositions à l'obligation d'être indemnisé par la personne pour laquelle les dispositions doivent être mises en œuvre pour tous les frais encourus du fait de la mise en œuvre.
>
> 5.4 Aux fins de la présente condition :
>
> a) le terme « fournisseur de services de communication » désigne une personne qui fournit un réseau téléphonique public ou des services téléphoniques accessibles au public;
>
> b) le terme « catastrophe » comprend tout incident majeur qui a un effet significatif sur le grand public; et à cette fin, un incident majeur inclut tout incident de contamination par des substances radioactives ou d'autres matériaux toxiques. [*Traduction*]

Code de pratique sur la sécurité des télécommunications (*Telecommunications Security Code of Practice*)

Le cadre établi par la ***Telecommunications (Security) Act 2021*** **(*TSA*)** comprend trois niveaux :

1. des obligations de sécurité générales renforcées pour les fournisseurs de services de télécommunication publics. Ces obligations sont énoncées dans les nouveaux articles 105A et 105C de la *Loi*, tels que modifiés par la *TSA*.

2. des mesures de sécurité particulières (ci-après dénommées « exigences »). Elles sont énoncées dans les *Electronic Communications (Security Measures) Regulations 2022* (*Règlement*) et détaillent les mesures particulières à prendre en plus des obligations générales prévues par la *Loi*.
3. des orientations techniques. Ce code de pratique fournit des lignes directrices détaillées aux grands et moyens fournisseurs de réseaux de communications électroniques publics ou services de communications électroniques publics (ci-après dénommés « fournisseurs de services de télécommunication publics ») sur l'approche privilégiée par le gouvernement pour démontrer la conformité à l'égard des obligations prévues par la *Loi* et les exigences prévues par le *Règlement*.

Non-conformité aux nouvelles obligations de sécurité prévues par la *Loi* ou les exigences prévues par le *Règlement* :

- En cas de non-conformité aux nouvelles obligations de sécurité ou des exigences de sécurité particulières, l'Ofcom pourra émettre aux fournisseurs un avis d'infraction qui précise qu'ils ne sont pas en conformité et qu'ils doivent prendre des mesures correctives. L'Ofcom peut également ordonner aux fournisseurs de services de télécommunication de prendre des mesures provisoires pour combler les lacunes en matière de sécurité au cours du processus d'application.
- En outre, en cas de non-conformité, y compris lorsqu'un fournisseur ne s'est pas conformé à un avis d'infraction, l'Ofcom peut imposer des sanctions financières. Le montant des sanctions financières que l'Ofcom peut imposer dans ces cas a été mis à jour au moyen de la *TSA*.
- De plus amples renseignements sur la manière dont l'Ofcom utilisera ses pouvoirs et réglementera le cadre seront contenus dans ses orientations procédurales.

Ces nouvelles réglementations, élaborées en collaboration avec le National Cyber Security Centre (NCSC) et l'Ofcom, définissent les mesures particulières que doivent prendre les fournisseurs de services de télécommunication publics britanniques pour respecter les obligations qui leur incombent en vertu de la *Loi*. L'Ofcom a reçu le pouvoir de leur infliger des amendes qui peuvent atteindre 10 % de leur chiffre d'affaires s'ils ne se conforment pas avec suffisamment de zèle. Toutefois, l'Ofcom reconnaît que les orientations définies dans le code de pratique ne sont pas le seul moyen pour les fournisseurs de se conformer aux nouvelles obligations de sécurité et aux exigences particulières en matière de sécurité. Les fournisseurs de services de télécommunication peuvent choisir de se conformer à ces nouvelles obligations et exigences particulières en matière de sécurité en adoptant des solutions techniques ou des approches différentes de celles spécifiées dans le code de pratique. Dans ces cas, l'Ofcom peut demander au fournisseur d'expliquer les raisons pour lesquelles il n'agit pas conformément aux dispositions du code de pratique afin d'évaluer s'il remplit toujours ses obligations légales en vertu du cadre de sécurité.

Stratégie du Royaume-Uni en matière d'infrastructure sans fil

Initiatives en vue d'améliorer la cybersécurité

Le National Cyber Security Centre est un organisme du gouvernement britannique qui fournit des conseils et du soutien aux secteurs public et privé sur la manière d'éviter les menaces à la sécurité informatique. Basé à Londres, il est devenu opérationnel en octobre 2016.
Aucune initiative majeure n'a été notée.

Initiatives en vue d'améliorer la couverture

La grande priorité stratégique du gouvernement britannique est de promouvoir une concurrence efficace et l'investissement dans des réseaux numériques de classe mondiale. L'investissement est essentiel afin d'améliorer les résultats des consommateurs en termes de choix, de qualité du service, d'innovation et de prix à long terme. Le gouvernement estime que la promotion de l'investissement devrait être prioritaire par rapport aux interventions en vue de réduire davantage les prix de détail à court terme, compte tenu de ces avantages à plus long terme.

Le gouvernement a défini une série de résultats pour atteindre cette priorité stratégique :

- Une stabilité et une clarté réglementaires accrues, grâce à des périodes d'examen du marché plus longues (cinq ans) et à un cadre dans lequel les entreprises qui réalisent des investissements importants et risqués peuvent être assurées que toute réglementation reflète un retour sur investissement équitable, proportionnel au niveau de risque.
- La reconnaissance de la convergence des utilisations des réseaux par les entreprises et les consommateurs, en procédant, le cas échéant, à des analyses de marché de l'accès unifié.
- Une réglementation uniquement lorsque et dans la mesure où cela est nécessaire pour répondre aux préoccupations en matière de concurrence et pour garantir la protection des intérêts des consommateurs à mesure que les marchés de la fibre deviennent plus concurrentiels.
- La reconnaissance des différences dans les conditions du marché local à travers le Royaume-Uni, en adoptant, le cas échéant, une approche géographiquement différenciée de la réglementation des marchés de gros. Dans les régions où la concurrence entre les réseaux est réelle ou potentielle, la nécessité d'une réglementation serait moindre.
- La possibilité pour les entreprises de développer de nouvelles approches afin de réduire les coûts de déploiement et de gérer les risques au moyen d'ententes commerciales.

Le moyen le plus efficace de fournir rapidement une connectivité entièrement en fibre à l'échelle nationale est de promouvoir la concurrence et l'investissement commercial dans la mesure du possible, et d'intervenir si nécessaire. Le gouvernement britannique estime ce qui suit :

- Au moins un tiers (et potentiellement beaucoup plus élevé) des locaux du Royaume-Uni pourraient accueillir au moins trois réseaux concurrents dotés d'une capacité d'un gigabit.
- Près de la moitié (ou moins s'il y a plus de trois zones de réseau) des locaux sont susceptibles de se trouver dans des zones qui pourraient accueillir la concurrence entre deux réseaux dotés d'une capacité d'un gigabit.
- Il est probable que certaines zones du pays (environ 10 % des locaux) ne bénéficieront pas d'investissements bien que commercialement viables pour au moins un opérateur.
- Le gouvernement utilisera des mécanismes de « concurrence pour le marché » afin de garantir l'investissement dans les zones. Le nouveau Code des communications électroniques européen (CCEE), par exemple, permet de désigner des zones dans lesquelles aucun opérateur n'a indiqué son intention de se déployer;
- Dans les 10 % de locaux restants, il est peu probable que le marché puisse à lui seul assurer le déploiement du réseau et un financement supplémentaire sera nécessaire pour assurer une couverture nationale.

Cette stratégie repose sur la réalisation de cinq objectifs :

1. Réduire autant que possible le coût du déploiement des réseaux en fibre en éliminant les obstacles au déploiement, qui augmentent les coûts et entraînent des retards.
2. Favoriser l'entrée sur le marché et l'expansion d'autres opérateurs de réseaux grâce à un accès facile aux conduits et aux poteaux d'Openreach, accompagné d'un accès à l'infrastructure d'autres services publics (par exemple, les égouts).
3. Une réglementation stable et à long terme qui incite à investir dans des réseaux concurrentiels.
4. Une approche « de l'extérieur vers l'intérieur » en matière de déploiement qui signifie que la connectivité dotée d'une capacité d'un gigabit est atteinte en même temps dans toutes les régions du Royaume-Uni et qu'aucune région n'est systématiquement laissée pour compte.
5. Un processus de transition pour augmenter la demande pour des services entièrement par fibre.

Les zones susceptibles de ne pas être viables commercialement pour un déploiement entièrement en fibre nécessiteront un financement supplémentaire d'une manière ou d'une autre. Le gouvernement britannique estime qu'il s'agit d'environ 10 % des locaux au Royaume-Uni. Ces zones, souvent rurales, ne doivent pas être obligées d'attendre que le reste du pays soit connecté pour avoir accès à des réseaux entièrement en fibre. Une connectivité généralisée permet aux petites entreprises d'accéder à une clientèle mondiale et aux individus de travailler plus efficacement.

Le gouvernement britannique entend poursuivre une stratégie « de l'extérieur vers l'intérieur », c'est-à-dire que si la concurrence entre les réseaux dessert les zones commercialement viables, le gouvernement soutiendra en même temps l'investissement dans les zones les plus difficiles d'accès. Le financement supplémentaire, quelle qu'en soit la source, devrait être de l'ordre de 3 à 5 milliards de livres sterling. Pour s'assurer que la fourniture de fibre dans ces zones commence tôt, le gouvernement donnera la priorité à la fourniture de réseaux entièrement en fibre dans le cadre du Programme de large bande extrêmement rapide (*Superfast Broadband Programme*) de Building Digital UK (BDUK) existant, qui a déjà permis à plus de 200 000 locaux situés dans des zones essentiellement rurales de bénéficier de la fibre optique jusqu'aux locaux de l'abonné (FTTP) depuis mars 2018.

La phase 3 du Programme vise à assurer une couverture extrêmement rapide dans la plus grande partie possible des 5 % restants du pays, et le gouvernement va maintenant maximiser le nombre de locaux à couvrir entièrement par la fibre. Le gouvernement britannique a déjà dégagé une somme d'environ 200 millions de livres sterling dans le cadre du Programme existant qui peut être utilisée à cette fin.

Stratégie de diversification de la 5G

Le gouvernement britannique a entrepris un examen approfondi des dispositions relatives à l'approvisionnement de l'infrastructure nationale essentielle de télécommunications du Royaume-Uni. L'examen de la chaîne d'approvisionnement en télécommunications de 2019 a mis en évidence la nécessité de gérer et d'atténuer les risques relatifs aux fournisseurs à haut risque, d'introduire un nouveau cadre de sécurité solide pour les télécommunications et de créer une base d'approvisionnement plus diversifiée et plus compétitive pour les réseaux de télécommunications.

Le gouvernement a pris des décisions importantes pour limiter et exclure les vendeurs à haut risque de l'infrastructure des télécommunications du Royaume-Uni et a proposé une législation pour donner à ces décisions un statut légal. La stratégie de diversification de la 5G présente des plans ciblés et ambitieux pour diversifier le marché mondial de l'approvisionnement en télécommunications, en se concentrant sur les domaines d'activité clés suivants :

- Soutenir les fournisseurs titulaires afin de garantir leur résilience et leur capacité à approvisionner le marché à court terme, tout en soutenant leur transition vers la structure de marché émergent.
- Attirer de nouveaux fournisseurs sur le marché britannique afin de renforcer la résilience et la concurrence, en donnant la priorité aux déploiements qui s'inscrivent dans la vision à long terme.
- Accélérer les solutions d'interfaces ouvertes et leur déploiement afin que le Royaume-Uni ne soit pas tributaire d'un seul fournisseur et commence à réaliser sa vision à long terme d'un marché plus ouvert et innovant.
- Un marché des télécommunications concurrentiel et dynamique.
- Le Royaume-Uni a élaboré des principes du réseau d'accès radioélectrique (RAN) ouvert, Open RAN principles – GOV.UK (www.gov.uk) [en anglais seulement], qui renvoient directement à la stratégie de diversification, ainsi que des travaux de recherche et développement en cours soutenus par le gouvernement et les essais relatifs au RAN ouvert (par exemple, SmartRAN Open Network Interoperability Centre [SONIC] Labs – Case study – GOV.UK [www.gov.uk]) [en anglais seulement].

Australie

Aperçu de la législation des cadres réglementaires sur la résilience

L'Australian Communications and Media Authority (ACMA) est le principal organisme de réglementation des télécommunications en Australie. L'Australian Competition and Consumer Commission (ACCC) est responsable de la réglementation de la concurrence.

L'ACCC :

- évalue et fait respecter les conditions d'accès au réseau national à large bande (*National Broadband Network* [NBN]) dans le cadre d'un engagement spécial à l'égard de l'accès de NBN Co.;
- met en œuvre l'engagement de séparation structurelle de Telstra et le plan de migration des clients de Telstra vers le NBN);
- fixe les prix de gros et les conditions d'accès de gros pour les services déclarés;
- assure le suivi des prix et de la concurrence dans le secteur des communications et établit des rapports à ce sujet;
- enquête sur les allégations de conduite anticoncurrentielle dans le secteur des communications.

Le ministère responsable des initiatives en matière de télécommunications et de la surveillance est le ministère des Infrastructures, des Transports, du Développement régional, des Communications et des Arts.

La *Telecommunications Act 1997* est la principale loi qui régit les télécommunications en Australie. Son objectif est de protéger les intérêts à long terme des utilisateurs finals des services de distribution et de garantir des services accessibles et abordables pour les Australiens. Cette loi établit une distinction entre les entreprises (c'est-à-dire les propriétaires et les opérateurs d'infrastructures) et les autres entités qui fournissent des services aux utilisateurs finals, appelées fournisseurs de services de distribution ou fournisseurs de services de communication.

La *Telecommunications (Consumer Protection and Service Standards) Act 1999* établit le régime australien pour le service universel et d'autres services de télécommunication d'intérêt public.

Initiatives en vue d'améliorer la puissance et la résilience du réseau

Les programmes d'incitation et de subvention financés par le gouvernement de l'Australie, le ministère des Infrastructures, des Transports, du Développement régional, des Communications et des Arts, sont les suivants :

Le **Programme de renforcement des réseaux mobiles (*Mobile Network Hardening*)** est une initiative du gouvernement de l'Australie qui aide les opérateurs de réseaux mobiles, les fournisseurs d'infrastructures et les gestionnaires d'infrastructures à améliorer la résilience de l'infrastructure des télécommunications des réseaux mobiles régionaux d'Australie à :

- prévenir les pannes en cas de catastrophe naturelle;
- renforcer la résilience des installations de télécommunications pour leur permettre de fonctionner plus longtemps pendant les feux de brousse et toute autre catastrophe naturelle;
- permettre le rétablissement rapide des services après une panne.

La première étape du programme a été financée par le Programme de renforcement des télécommunications contre les catastrophes naturelles (*Strengthening Telecommunications Against Natural* Disasters *Programme*) du gouvernement, annoncée en janvier 2020. Dans le cadre du Plan pour une meilleure connectivité dans les régions et les zones rurales de l'Australie (*Better Connectivity Plan for Regional and Rural Australia*), annoncé dans le budget de 2022-2023, le gouvernement s'est engagé à financer d'autres étapes du programme. Ce nouveau financement s'inscrit dans le cadre de l'engagement pris par le gouvernement en vue d'améliorer la résilience des communications dans les zones rurales, régionales et reculées de l'Australie dans le cadre du Plan pour une meilleure connectivité.

La première étape du Programme de renforcement des réseaux mobiles prévoit un financement de 23,5 millions de dollars (taxe sur les produits et les services [TPS] incluse) à Optus, Telstra et TPG TPG, les opérateurs de réseaux mobiles, en deux étapes, pour la réalisation d'environ 1 000 projets en vue de renforcer la résilience de l'infrastructure régionale des télécommunications.

La première étape consiste à financer Optus, Telstra et TPG afin d'augmenter l'autonomie de la batterie de secours de 467 stations de base financées dans le cadre des deux premières étapes du Programme pour les zones sans réseau mobile (*Mobile Black Spot Program*) du gouvernement. Ces améliorations permettront d'augmenter la durée de fonctionnement de ces stations de base à au moins 12 heures. À ce jour, 461 mises à niveau ont été réalisées et les sites restants devraient être achevés en 2023.

La deuxième étape consiste à financer Optus, Telstra et TPG pour réaliser plus de 530 améliorations de la résilience sur des sites de stations de base de téléphonie mobile dans toute l'Australie. Ces améliorations concernent :

- le déploiement de nouvelles génératrices portables et permanentes pour fournir une alimentation de secours supplémentaire en cas de panne de courant;
- la mise à niveau des systèmes de batteries afin d'augmenter la capacité d'alimentation de secours;
- l'ajout de dispositifs d'extension des batteries afin d'améliorer la capacité d'alimentation de secours existante sur des sites clés au sein des réseaux mobiles;
- la transmission au sein des groupes de réseaux mobiles régionaux afin de réduire les points de défaillance uniques du réseau;
- le renforcement physique des sites contre les dommages causés par les feux de brousse.

Le gouvernement a engagé jusqu'à 16,5 millions de dollars (TPS incluse) dans la deuxième étape du Programme de renforcement des réseaux mobiles pour financer des projets

supplémentaires en vue d'améliorer la résilience de l'infrastructure des réseaux mobiles dans les zones rurales, régionales et reculées de l'Australie.

Le gouvernement a consulté le public, l'industrie des télécommunications et les parties prenantes du gouvernement sur la conception de cette étape, y compris sur le projet de lignes directrices pour l'octroi de subventions.

Une subvention temporaire pour le déploiement d'infrastructures de télécommunications a été accordée par le gouvernement de l'Australie en 2022. La subvention a été annoncée dans le cadre du **Programme de renforcement des télécommunications contre les catastrophes naturelles (*Strengthening Telecommunications Against Natural Disasters Program*)**. Jusqu'à 7,7 millions de dollars étaient disponibles pour cette subvention. (Remarque : La subvention est maintenant terminée et n'est plus disponible.) Les objectifs du programme étaient les suivants :

- Améliorer la résilience des services de télécommunication dans les collectivités qui ont récemment été touchées par de graves feux de brousse ou qui risquent de subir des catastrophes naturelles à l'avenir.
- Renforcer la capacité à rétablir les services dans les zones touchées par les feux de brousse ou les catastrophes naturelles en déployant rapidement des installations temporaires pour combler les lacunes causées par les pannes.

Le **Programme d'innovation en matière de résilience des télécommunications face aux catastrophes (*Telecommunications Disaster Resilience Innovation Program*)** encouragera le développement de nouvelles technologies afin de fournir des solutions pour la résilience des services de télécommunication en cas de catastrophe, en particulier dans les collectivités régionales, rurales et éloignées, ainsi que dans les communautés des Premières Nations.

L'engagement de 50 millions de dollars a été annoncé et financé dans le cadre du Plan pour une meilleure connectivité dans les régions et les zones rurales de l'Australie (*Better Connectivity Plan for Regional and Rural Australia*) du gouvernement de l'Australie et s'étendra sur la période 2022-2025. Les projets financés amélioreront la préparation des réseaux de télécommunications australiens face aux risques climatiques croissants, notamment à l'augmentation prévue de la fréquence et de la gravité des catastrophes naturelles en Australie. Le programme sera mis en œuvre au moyen de deux séries de subventions par concours :

- La première phase se concentre sur le financement de solutions innovantes qui renforceront la résilience des services de télécommunication face aux conséquences des pannes d'électricité. Cette approche tient compte du fait que les pannes d'électricité restent l'une des causes les plus fréquentes de toutes les pannes de services de télécommunication en cas de catastrophe.
- La deuxième phase se concentre sur d'autres technologies de télécommunications innovantes (à l'exclusion des solutions qui reposent sur l'énergie, qui seront financées dans le cadre de la première phase) qui amélioreront la résilience, la redondance et la disponibilité des services de télécommunication pendant ou après une catastrophe naturelle.

Pour **renforcer les capacités des infrastructures temporaires**, le gouvernement de l'Australie a co-investi avec l'industrie des télécommunications pour acheter des installations de communication portables, notamment des cellules sur roues, des centraux mobiles sur roues et des camions Road Muster du NBN, qui peuvent être positionnées dans les zones sinistrées afin de rétablir rapidement les services de communication.

Cet investissement signifie que l'infrastructure de communication temporaire est prête à prendre la route en cas de besoin, ce qui permet aux Australiens de rester en contact avec leur famille

et les services essentiels, et de s'assurer que les achats essentiels de nourriture, d'eau et de carburant peuvent être effectués.

Un financement a été accordé à NBN Co. pour l'achat de cinq camions satellitaires Road Muster supplémentaires et de douze trousses de satellites portables afin de fournir une connectivité là où cela est nécessaire en cas d'urgence. Ils ont tous été livrés et placés à des endroits stratégiques en Australie afin de mieux répondre aux situations d'urgence.

Fourniture de connexions par satellite aux services d'urgence et aux centres d'évacuation

Le gouvernement a amélioré la connectivité des stations des services d'incendie et des centres d'évacuation dans toute l'Australie afin de soutenir leur travail essentiel et de fournir une connectivité d'urgence aux collectivités.

Ce financement a permis à NBN Co. d'installer des connexions par satellite Sky Muster dans les stations des services d'incendie en milieu rural et dans les centres d'évacuation désignés de l'Australie**.**

Initiatives en vue d'améliorer la cybersécurité

L'Australian Cyber Security Centre (ACSC) dirige les efforts du gouvernement australien afin d'améliorer la cybersécurité.

L'ACSC est un centre de collaboration et d'échange de renseignements des secteurs privé et public sur la cybersécurité, afin de prévenir et de combattre les menaces et de minimiser les dommages causés aux Australiens. Il fournit des conseils et de l'aide à l'ensemble de l'économie, y compris aux infrastructures et systèmes essentiels d'intérêt national, aux administrations fédérales, régionales et locales, aux petites et moyennes entreprises, au monde universitaire, aux organismes à but non lucratif et à la communauté australienne.

Plus précisément, l'ACSC a pour fonction de :

- répondre aux menaces et aux incidents de cybersécurité en tant qu'équipe d'intervention en cas d'urgence informatique de l'Australie;
- collaborer avec les secteurs privé et public pour échanger des renseignements sur les menaces et accroître la résilience;
- sensibiliser les gouvernements, l'industrie et la collectivité à la cybersécurité;
- fournir des renseignements, des conseils et de l'aide en matière de cybersécurité à tous les Australiens.

Le personnel de la Division de la politique de cybersécurité du ministère de l'Intérieur est installé dans les mêmes locaux que le personnel de l'ACSC afin de collaborer à la fourniture de conseils stratégiques au gouvernement.

Le gouvernement de l'Australie a modifié la *Security of Critical Infrastructure Act 2018* (*Loi SOCI*) en décembre 2021. Les entreprises et les fournisseurs de services de distribution ont désormais de nouvelles obligations en matière de sécurité :

- aviser l'ACSC de l'Australian Signals Directorate (ASD) si un incident de cybersécurité a des répercussions importantes sur une infrastructure essentielle (à compter du 7 juillet 2022);
- fournir au CISC du ministère de l'Intérieur certains renseignements sur les infrastructures essentielles afin de les inclure dans un registre (à compter du 7 octobre 2022).

Les 12 premiers mois (à compter du 8 juillet 2022) sont considérés comme une phase d'apprentissage et de familiarisation. Le CISC se concentrera sur l'éducation, le soutien et la

collaboration avec les entités pour comprendre les seuils de déclaration relatifs à chaque secteur.

Pendant cette période, les mesures d'application ne peuvent être prises qu'en cas de non-conformité flagrante, comme l'omission de déclarer des incidents critiques, plutôt qu'en ce qui concerne le respect des délais de déclaration ou le niveau de détail d'un rapport.

Les mécanismes d'application prévus aux articles 68 et 101 de la *Telecommunications Act*, qui concernent la non-conformité à une condition de licence ou d'une détermination de service, s'appliquent aux nouveaux instruments.

Initiatives en vue d'améliorer la couverture

Le NBN de l'Australie a été annoncé en 2009. Cette politique visait à améliorer la disponibilité et le rendement de la large bande en Australie et à faciliter la séparation structurelle de Telstra en fournissant une option en fibre à son réseau en cuivre.

Le NBN est construit et géré par une entreprise publique, NBN Co. (aujourd'hui connue sous le nom de nbnTM). Un des principes fondamentauxl est que nbnTM ne fournit que des services de gros aux fournisseurs de services de détail et ne dessert pas les utilisateurs finals. Cette politique est établie dans la législation, de sorte que toute proposition de changement devrait être soumise au Parlement.

Le plan initial du NBN prévoyait d'équiper 93 % des locaux d'une connexion en fibre. Les 7 % de locaux restants seraient desservis soit par un nouveau service par satellite, soit par un service terrestre sans fil fixe (c'est-à-dire un service vers un lieu fixe, comme une maison, plutôt qu'un service mobile).

Le cadre réglementaire du NBN a été établi au moyen de deux lois :

- *National Broadband Network Companies Act 2011;*
- *Telecommunications Legislation Amendment (National Broadband Network Measures—Access Arrangements) Act* 2011.

Récemment, le gouvernement de l'Australie s'est engagé à investir 2,4 milliards de dollars dans le déploiement de la fibre dans les collectivités du pays. Ce nouvel investissement permettra à 1,5 million de foyers et d'entreprises supplémentaires actuellement desservis par la fibre jusqu'au nœud (FTTN) de passer à la fibre jusqu'aux locaux de l'abonné (FTTP).

Le FTTP est estimé comme meilleur que la FTTN (plus grande vitesse et fiabilité), et les deux sont meilleurs que le cuivre, car elles sont plus rapides, meilleures sur les longues distances, ont une plus grande largeur de bande, sont plus évolutives, et sont plus fiables et stables. Ces améliorations permettront d'offrir des vitesses de connexion à large bande plus rapides, une meilleure fiabilité, une plus grande efficacité énergétique et une capacité de données supplémentaire.

Nouvelle-Zélande

Aperçu de la législation et des cadres réglementaires sur la résilience

En Nouvelle-Zélande, plusieurs organismes gouvernementaux ainsi que des agences sont chargés de réglementer l'espace des télécommunications. Le ministère des Entreprises, de l'Innovation et de l'Emploi, la New Zealand Commerce Commission and le Telecommunications Carrier Forum (TCF) jouent un rôle clé dans la législation, la réglementation et la fourniture de services de télécommunication en Nouvelle-Zélande.

La *Telecommunication Act 2001* sert de base à la réglementation et à la législation. Cette loi permet au TCF de réglementer la prestation de services de télécommunication dans le pays.

Initiatives en vue d'améliorer la puissance et la résilience du réseau

Dans le cadre du **Programme d'amélioration de la capacité rurale (*Rural Capacity Upgrade Programme*)**, les tours cellulaires existantes seront modernisées et de nouvelles tours seront construites dans les zones rurales où le rendement est médiocre. La fibre, une couverture de ligne d'abonné numérique à très haut débit (VDSL) supplémentaire et d'autres technologies sans fil seront également déployées dans les zones encombrées.
Dans le cadre de cette initiative, 13 entrepreneurs du secteur privé ont signé des contrats avec Crown Infrastructure Partners pour effectuer les travaux. Le programme sera financé par les 47 millions de dollars du fonds gouvernemental de réponse et de relance à la COVID-19.

Le **Programme pour les utilisateurs éloignés (*Remote Users Scheme*)** vise à équiper le plus grand nombre possible de foyers éloignés de l'infrastructure de connectivité nécessaire pour accéder aux services à large bande. Dans le budget 2022, 15 millions de dollars ont été alloués au financement du Programme pour les utilisateurs éloignés, dans le cadre d'une enveloppe plus large de 60 millions de dollars pour la connectivité rurale, annoncée plus tôt dans l'année.

Le **Fonds pour les zones sans réseau mobile (*Mobile Black Spot Fund*)** permet d'améliorer la couverture mobile sur environ 1 400 kilomètres de routes nationales et dans plus de 168 sites touristiques où aucune couverture n'existe actuellement. Le programme aura une incidence directe sur la sécurité publique, en fournissant une meilleure couverture de téléphonie mobile sur les tronçons d'autoroutes de l'État. Il améliorera également l'expérience des visiteurs en offrant une nouvelle couverture dans les lieux touristiques.
Crown Infrastructure Partners gère les accords contractuels du Programme.

Initiatives en vue d'améliorer la cybersécurité

Le principal organisme gouvernemental chargé de définir la politique en matière de cybersécurité en Nouvelle-Zélande est le Département du Premier ministre et du Cabinet (DPMC).

La Nouvelle-Zélande a mis en place un plan de cybersécurité. Le Plan d'intervention d'urgence en matière de cybersécurité (*Cyber Security Emergency Response Plan*) définit le cadre de la réponse du gouvernement à une situation d'urgence en matière de cybersécurité afin que :

- les agences et les fonctionnaires comprennent leur rôle et leurs responsabilités en cas d'urgence liée à la cybersécurité;
- le secteur privé comprend l'approche du gouvernement;
- la réponse est coordonnée, appropriée et efficace lors d'une urgence liée à la cybersécurité;
- après une urgence liée à la cybersécurité, les services et les opérations sont rétablis rapidement et les leçons appropriées sont tirées et mises en œuvre.

Depuis 2013, le Plan a guidé la réponse de la Nouvelle-Zélande aux urgences liées à la cybersécurité. Tout au long de son existence, il a été mis à jour pour atteindre les objectifs de la stratégie de cybersécurité, s'adapter à l'évolution de l'environnement et refléter les leçons tirées des incidents et des exercices.
Le Plan fait partie du Système de sécurité nationale (*National Security System*) de la Nouvelle-Zélande. Il est géré par le DPMC et est rédigé en collaboration avec d'autres agences qui jouent un rôle en cybersécurité.

Initiatives en vue d'améliorer la couverture

Le **Programme de la large bande ultrarapide (Ultra-Fast Broadband Programme)** a été l'un des projets d'infrastructure les plus importants et les plus ambitieux jamais entrepris en Nouvelle-Zélande. Il a permis à environ 87 % des Néo-Zélandais, dans plus de 390 villes, d'avoir accès à la fibre optique avant la fin de 2022.

Près de 1,8 milliard de dollars ont été investis dans l'infrastructure de la large bande ultrarapide pour permettre au plus grand nombre possible de Néo-Zélandais de profiter des avantages sociaux et économiques d'une large bande plus rapide. Crown Infrastructure Partners (anciennement Crown Fibre Holdings) a été créée en tant que société d'État pour gérer l'investissement du gouvernement dans la large bande ultrarapide.

La large bande ultrarapide utilise des câbles à fibre optique pour acheminer la fibre jusqu'à l'abonné. Elle est plus appropriée dans les zones urbaines à forte densité de population. Elle est supérieure à la technologie du cuivre qui a été déployée en Nouvelle-Zélande au cours du siècle dernier. Les utilisateurs de la large bande ultrarapide peuvent accéder à des vitesses proches de 1 000 mégabits par seconde.

L'initiative de la large bande ultrarapide a été lancée en 2008 en réponse aux tendances mondiales en matière de télécommunications en Asie du Sud-Est et à la qualité relativement faible de l'Internet en Nouvelle-Zélande.

La qualité de la large bande en Nouvelle-Zélande s'est considérablement améliorée ces derniers temps. Il y a dix ans, la vitesse Internet moyenne en Nouvelle-Zélande était inférieure à celle du Royaume-Uni et de l'Australie. Grâce au déploiement efficace de la fibre optique et de liaisons par câble sous-marin supplémentaires, la Nouvelle-Zélande se situe désormais bien au-dessus de la moyenne de l'Organisation de coopération et de développement économique (OCDE) et dans une position similaire à celle des États-Unis, avec des vitesses Internet de 33 mbps en moyenne.

Japon

Aperçu de la législation et des cadres réglementaires sur la résilience

Le ministère des Affaires intérieures et des Communications (MAIC) est l'organisme de régulation des télécommunications (plus précisément le Bureau des télécommunications). Son rôle consiste à formuler des politiques, à attribuer des licences, à gérer les radiofréquences, à promouvoir la concurrence, à protéger les droits des consommateurs et à assurer le bon déroulement des opérations.

Initiatives en vue d'améliorer la puissance et la résilience du réseau

Plusieurs initiatives pour améliorer la résilience en cas d'urgence et de catastrophe naturelle

- **Système d'alerte précoce aux tremblements de terre :** Le Japon dispose d'un solide système d'alerte précoce aux tremblements de terre qui détecte les activités sismiques et émet des alertes au public par l'intermédiaire de divers moyens de communication, notamment les téléphones mobiles, la télévision et la radio. Ce système fournit de précieuses secondes ou minutes d'alerte avant l'arrivée des ondes sismiques, ce qui permet à la population de prendre des mesures de protection et contribue à prévenir les perturbations des infrastructures de télécommunications.
- **Fourniture de renseignements sur les catastrophes et les évacuations au moyen des communications sans fil à adresses multiples :** La communication sans fil à adresses multiples est un système qui permet de transmettre rapidement et avec précision des renseignements aux communautés locales par l'intermédiaire de sirènes,

de haut-parleurs et d'autres moyens au moment où une catastrophe se produit. Plus précisément, les haut-parleurs des sirènes et les récepteurs domestiques sont classés dans la catégorie des communications sans fil à adresses multiples. Des récepteurs domestiques et des radios d'urgence sont distribués aux personnes qui se trouvent dans les zones où le son des sirènes ne parvient pas.

- **Fourniture d'une alerte rapide et d'autres renseignements sur les catastrophes par courrier électronique d'information sur les catastrophes.**
- **Échange de renseignements sur les catastrophes au moyen d'un système particulier (J-Alert).** Le système d'échange de renseignements sur les catastrophes (J-Alert) est un système qui convertit les renseignements provenant des organisations publiques en XHL, en courrier électronique et dans d'autres formats, et les transmet aux médias et aux entreprises de communication. J-Alert peut transmettre efficacement et rapidement des renseignements provenant de tous les participants au système dans un certain format.
- **Maintien des communications dans les zones sinistrées grâce à l'unité de coordination de la gestion (MDRU).** Une unité de ressources mobile et déployable de technologie de l'information et des communications (TIC) est une unité de TIC mobile destinée aux communications en cas de catastrophe. Elle se compose de dispositifs de communication et de dispositifs de traitement et de stockage de l'information montés sur un conteneur ou un véhicule mobile. Une unité peut être amenée dans les zones sinistrées peu de temps après une catastrophe et servir d'infrastructure de téléphonie ou de communication.
- **Maintien des communications dans les zones sinistrées grâce à des systèmes portables de communication par satellite :** Un système portable de communication par satellite prend des images animées des zones sinistrées et envoie les données par satellite aux quartiers généraux des catastrophes et à d'autres bureaux concernés, qui utilisent ces images pour élaborer des plans de contre-mesure.
- Les bureaux de développement régional du ministère de l'Aménagement du territoire, des Infrastructures, des Transports et du Tourisme ont créé des stations fixes dans lesquelles sont installés plusieurs systèmes portables de communication par satellite afin de se préparer aux catastrophes.
- **Systèmes d'alimentation de secours** : Au Japon, les fournisseurs de services de télécommunication sont tenus de mettre en place des systèmes d'alimentation de secours pour maintenir le fonctionnement des infrastructures essentielles pendant les pannes d'électricité causées par des catastrophes. Ces systèmes de secours comprennent les systèmes d'alimentations sans interruption (ASI) et les génératrices de secours.
- **Câbles à fibre optique souterrains** : Pour se protéger des dommages causés par les tremblements de terre et autres catastrophes, le Japon a installé sous terre une grande partie de son infrastructure de télécommunications, y compris les câbles à fibre optique. Cela permet de réduire le risque de perturbation des réseaux de communication en cas d'urgence.

Initiatives en vue d'améliorer la cybersécurité

Depuis 2005, la « Politique de cybersécurité pour la protection des infrastructures essentielles » est définie comme un plan d'action commun entre le gouvernement, chargé de promouvoir les mesures indépendantes en matière de cybersécurité des infrastructures essentielles prises par les exploitants d'infrastructures essentielles et de mettre en œuvre d'autres mesures nécessaires, et les exploitants d'infrastructures essentielles qui mettent en œuvre de manière indépendante des mesures de protection pertinentes. La nouvelle édition a été publiée en 2022.

- La *Basic Act on Cybersecurity* énonce la politique de base du Japon en matière de cybersécurité ainsi que les responsabilités fondamentales des gouvernements nationaux et locaux. En vertu de la *Basic Act on Cybersecurity*, les exploitants d'infrastructures essentielles, y compris certaines entreprises de télécommunications, doivent s'efforcer de sécuriser la cybersécurité de manière volontaire et proactive et de coopérer avec les mesures de cybersécurité mises en œuvre par les gouvernements nationaux et locaux.

- En vertu de la *Telecommunications Business Act*, les opérateurs de services de télécommunications ont l'obligation de protéger le secret des télécommunications et de maintenir et d'exploiter certaines installations de télécommunications conformément aux normes techniques applicables établies par le ministère des Affaires intérieures et des Communications. Ces normes techniques comprennent certaines exigences en matière de sécurité des réseaux.

- Le 16 décembre 2022, le gouvernement japonais a approuvé une décision du Cabinet sur les documents stratégiques relatifs à la sécurité : la Stratégie de sécurité nationale, la Stratégie de défense nationale et le Programme de renforcement de la défense. La Stratégie de sécurité nationale est la base de la stratégie de sécurité nationale du Japon pour les dix prochaines années, en définissant les stratégies diplomatiques et de défense en réponse au nouvel environnement de sécurité. La Stratégie de défense nationale, rebaptisée Lignes directrices du Programme de défense nationale, définit la stratégie de défense de la Force japonaise d'autodéfense (FJA) pour les dix prochaines années, en fixant des objectifs pour la sécurité nationale et en décrivant les approches et les moyens à mettre en œuvre pour les atteindre. Le Programme de renforcement de la défense, rebaptisé Programme de défense à moyen terme, désigne un plan de développement à moyen et long terme qui comprend le niveau de capacité de défense et le plan d'approvisionnement.

Initiatives en vue d'améliorer la couverture

Le taux de couverture nationale pour les services à large bande par fibre optique dans les ménages était de 99,1 % à la fin du mois de mars 2020, et les services ne sont pas disponibles pour près de 530 000 ménages au Japon. D'après le taux de couverture préfectorale pour les services à large bande par fibre optique, le développement du réseau à large bande par fibre optique a été retardé dans les préfectures qui comptent de nombreuses îles ou régions montagneuses éloignées.

Le gouvernement actuel a pour objectif de porter la zone couverte par la fibre optique à plus de 99,9 % de la masse continentale du pays d'ici 2028.

Union européenne

Aperçu de la législation et des cadres réglementaires sur la résilience

L'Organe des régulateurs européens des communications électroniques (ORECE) est l'organisme de réglementation de l'Union européenne. Il est composé de représentants des autorités réglementaires nationales (ARN) de chaque État membre de l'Union européenne.

Son rôle principal est de promouvoir l'application cohérente du cadre réglementaire de l'Union européenne pour les communications électroniques, de garantir la concurrence et de préserver les intérêts des consommateurs et des utilisateurs finals.

L'ORECE fournit des orientations et des conseils à la Commission européenne, contribue à l'élaboration d'approches communes en matière de réglementation et à l'harmonisation du secteur des télécommunications dans l'ensemble de l'Union européenne.

L'un des principaux objectifs de l'Union européenne est de réduire la vulnérabilité des infrastructures essentielles et d'accroître leur résilience. Un niveau de protection adéquat doit être assuré et les effets préjudiciables des perturbations sur la société et les citoyens doivent être limités autant que possible.

Juhan Lepassaar, directeur exécutif de l'Agence de l'Union européenne pour la cybersécurité (ENISA), déclare que « la résilience des infrastructures et des technologies essentielles de l'Union européenne dépendra fortement de notre capacité à réaliser des investissements stratégiques. Je suis convaincu que nous disposons des compétences et des aptitudes nécessaires pour atteindre notre objectif, qui est de veiller à ce que nous disposions des ressources adéquates pour continuer à développer nos capacités en matière de cybersécurité dans tous les secteurs économiques de l'Union européenne » [*Traduction*].

L'Union européenne a commencé en 2009 à réglementer la cyberrésilience des fournisseurs de services de communications électroniques dans le cadre réglementaire des télécommunications de l'Union européenne depuis la réforme des télécommunications, puis la réglementation a étendue grâce à la Directive sur la sécurité des réseaux et des systèmes d'information (Directive SRI) aux opérateurs de services essentiels et aux fournisseurs de services numériques, qui comprennent notamment les fournisseurs d'infrastructures numériques et les services d'informatique en nuage.

Initiatives en vue d'améliorer la puissance et la résilience du réseau

Les fournisseurs de services de communications électroniques de l'Union européenne sont tenus de déclarer les incidents de sécurité qui ont des répercussions importantes sur la continuité des services de communications électroniques aux ARN des télécommunications de chaque État membre de l'Union européenne.

Chaque année, les ARN communiquent à l'ENISA un résumé d'une sélection de ces incidents, c'est-à-dire les incidents les plus importants, en fonction d'un ensemble de seuils convenus à l'échelle de l'Union européenne. C'est la 11^{e} année que l'ENISA publie un rapport annuel sur les incidents dans le secteur des télécommunications. L'ENISA a commencé à publier ces rapports annuels en 2012. La déclaration obligatoire des incidents fait partie du cadre réglementaire des télécommunications de l'Union européenne depuis la réforme des télécommunications de 2009 : L'alinéa 13a) de la directive relative au cadre (2009/140/CE) est entrée en vigueur en 2011.

L'obligation de déclarer les incidents en vertu de l'alinéa 13a) visait surtout les incidents de sécurité qui ont des répercussions importantes sur le fonctionnement de chaque catégorie de services de télécommunication. Au fil des ans, les organismes de régulation ont convenu de se concentrer principalement sur les pannes de réseau ou de service (incidents de type A – panne de service, par exemple, continuité, disponibilité – une panne due à une une coupure de câble causée par une erreur de l'opérateur d'une machine d'excavation utilisée lors de la construction d'une route serait classée dans la catégorie des incidents de type A).

Cela exclurait de la portée de ces rapports les attaques ciblées, telles que l'utilisation des vulnérabilités du protocole du système de signalisation no 7, les fraudes par usurpation de carte SIM, ou même des attaques plus étendues qui ne provoquent cependant pas de pannes. La mise à jour des règles de l'Union européenne en matière de télécommunications, à savoir le Code des communications électroniques européen (CCEE), qui devait être harmonisé dans les États membres d'ici la fin de 2020, prévoit un champ d'application plus large pour les exigences

relatives à la déclaration des incidents à l'article 40. Ces exigences incluent explicitement, par exemple, la divulgation de renseignements confidentiels. En 2021, l'ENISA a reçu pour la deuxième fois trois rapports d'incidents de type B (divulgation de renseignements confidentiels).

Il est important de noter que les incidents de sécurité dans les télécommunications qui sont déclarés aux autorités nationales ne concernent que les incidents majeurs, c'est-à-dire ceux qui ont des répercussions importantes. Les incidents de moindre importance, qui ne touchent que de petits pourcentages de la population, comme les attaques d'usurpation de carte SIM, ne sont pas déclarés.

En vertu de l'article 40 du CCEE, les exigences de déclaration des incidents ont un champ d'application plus large, incluant non seulement les pannes, mais aussi, par exemple, la divulgation de renseignements confidentiels. En outre, le champ d'application de l'EECC s'étend à un plus grand nombre de services, y compris non seulement les opérateurs de services de télécommunication traditionnels, mais aussi, par exemple, les fournisseurs de services de communication par contournement (tels que les services de messagerie comme Viber et WhatsApp). En 2020, les lignes directrices relatives aux rapports annuels ont été mises à jour pour inclure de nouveaux seuils pour les rapports annuels de déclaration à l'ENISA. Il s'agit de paramètres quantitatifs et qualitatifs ainsi que la déclaration des incidents de sécurité qui touchent non seulement les services de téléphonie et Internet fixes et mobiles, mais aussi les services de communications interpersonnelles par numéro ou les services de communications interpersonnelles sans numéro (services de communications par contournement).

Initiatives en vue d'améliorer la cybersécurité

L'Union européenne a également étendu cette réglementation des télécommunications aux opérateurs de services essentiels et aux fournisseurs de services numériques, qui comprennent notamment les fournisseurs d'infrastructures numériques et les services d'informatique en nuage.

La Directive SRI représente la première législation européenne en matière de cybersécurité, et son objectif est d'atteindre un niveau commun élevé de cybersécurité pour tous les États membres. L'un des trois piliers de la Directive SRI est la mise en œuvre de la gestion des risques et des exigences en matière de déclaration des incidents.

L'ENISA évalue et mesure chaque année l'incidence de la Directive SRI sur la cybersécurité. Le rapport de 2022 de l'ENISA marque la troisième itération du rapport de l'ENISA sur les investissements de la Directive SRI, qui recueille des données sur la façon dont les opérateurs de services essentiels et les fournisseurs de services numériques désignés dans la Directive SRI de l'Union européenne investissent leurs budgets de cybersécurité et sur la façon dont ces investissements ont été influencés par la Directive SRI.

Investissements dans la cybersécurité dans l'Union européenne : Les fonds sont-ils suffisants pour répondre aux nouvelles normes de cybersécurité? (Investissements de la Directive SRI en 2022) [en anglais seulement]

Le 16 janvier 2023, la Directive (UE) 2022/2555 (connue sous le nom de Directive SRI2) est entrée en vigueur afin de remplacer la directive (UE) 2016/1148. L'ENISA considère que la Directive SRI2 améliore le niveau actuel de cybersécurité dans l'Union européenne par :

- la création du réseau d'organisations de liaison en cas de cybercrises (*Cyber Crises Liaison Organisation Network* [CyCLONe]);
- l'amélioration du niveau d'harmonisation des exigences en matière de sécurité et de déclaration;

- la promotion de nouveaux domaines d'intérêts, tels que la chaîne d'approvisionnement, la gestion des vulnérabilités, l'Internet central et la cyberhygiène, dans les stratégies nationales de cybersécurité des États membres;
- l'introduction d'idées nouvelles, telles que l'évaluation par les pairs, pour renforcer la collaboration et le partage des connaissances entre les États membres;
- la couverture d'une plus grande partie de l'économie et de la société en incluant davantage de secteurs, ce qui signifie qu'un plus grand nombre d'entités sont obligées de prendre des mesures pour améliorer leur niveau de cybersécurité.

La *Loi sur la cyberrésilience*, qui a été présentée en novembre 2022, met en place des exigences minimales en matière de cybersécurité pour les produits et les logiciels qui sont mis sur le marché unique, quel que soit leur lieu de production. Elle comprend les acteurs du secteur des télécommunications. Ce faisant, l'Europe comble un vide juridique. La *Loi* relèvera le niveau de cybersécurité « par défaut » dans tous les produits et introduira une notion de « cybersécurité dès la conception ».

Alors qu'il sera possible de faire des autodéclarations de conformité pour 90 % des produits, pour une trentaine de produits, les plus critiques en termes de cyberrisque – comme les pare-feu industriels, les routeurs ou les systèmes d'exploitation – l'examen de conformité devra être effectué par un tiers. La Commission pourra demander le retrait du marché d'un produit qui présente un cyberrisque.

Cette législation a le potentiel d'établir une norme mondiale en matière de cybersécurité. En effet, la nouvelle politique de cybersécurité annoncée par les États-Unis il y a un mois s'inspire fortement de la Directive SRI et de la *Loi sur la cyberrésilience*.

L'Union européenne continue de veiller à la mise en œuvre de la boîte à outils de la cybersécurité de la 5G afin de déployer des réseaux sécurisés. Tous les États membres ont décidé à l'unanimité d'exclure les fournisseurs à haut risque de leurs réseaux (centraux et RAN). Bien que 23 États membres ont adopté des lois à cet effet, seuls sept d'entre eux les ont mises en œuvre et ont exclu d'une manière ou d'une autre les fournisseurs qu'ils considéraient comme un risque pour la sécurité.

Initiatives en vue d'améliorer la couverture

Le volet « Numérique » (2021-2027) de la deuxième génération du programme Mécanisme pour l'interconnexion en Europe (*Connecting Europe Facility*) visait à soutenir et à catalyser les investissements dans les infrastructures de connectivité numérique d'intérêt commun. Le programme dispose d'un budget total de 2,065 milliards d'euros, dont 1,7 milliard est géré par l'Agence exécutive européenne pour la santé et le numérique. Les mesures qu'il est prévu de soutenir dans le cadre du volet « Numérique » de la deuxième génération du programme Mécanisme pour l'interconnexion en Europe sont les suivantes :

- le déploiement de réseaux à très haute capacité, y compris les systèmes 5G, capables de fournir une connectivité dotée d'une capacité d'un gigabit dans les zones où se trouvent les moteurs socio-économiques (par exemple, les écoles, les universités, les hôpitaux, les centres de transport, les administrations publiques), et l'accès à ces réseaux;
- la couverture ininterrompue des systèmes 5G sur tous les grands axes de transport, y compris les réseaux de transport transeuropéens;
- le déploiement de nouveaux réseaux de base ou l'amélioration significative des réseaux existants, y compris les câbles sous-marins, à la fois à l'intérieur des États membres de l'Union européenne et entre ceux-ci et les pays tiers;

- la mise en œuvre d'infrastructures de connectivité numérique liées à des projets transfrontaliers dans les domaines du transport et de l'énergie, et le soutien aux plateformes numériques opérationnelles directement associées à ces infrastructures.

Le volet « Télécommunications » (2014-2020) du Mécanisme pour l'interconnexion en Europe (*Connecting Europe Facility*) a facilité l'interaction transfrontalière entre les administrations publiques, les entreprises et les citoyens, en déployant des infrastructures de services numériques, la connectivité dans les communautés locales (WiFi4EU) et les réseaux à large bande (au moyen d'instruments de capitaux propres et de prêts).
Doté d'un budget d'environ 1 milliard d'euros, dont 203 millions sont désormais gérés par l'Agence exécutive européenne pour la santé et le numérique, le programme a soutenu deux types de services numériques :

- les services numériques réutilisables qui peuvent être intégrés ou combinés à d'autres projets, qui couvrent l'identification électronique, la signature électronique, la facturation électronique, la livraison électronique et la traduction automatisée (éléments de base);
- les infrastructures de services numériques spécifiques qui couvrent des domaines tels que la cybersécurité, la cybersanté, la plateforme européenne pour les emplois et les compétences numériques, le système d'interconnexion des registres du commerce, Europeana, les marchés publics en ligne, l'échange électronique d'informations sur la sécurité sociale, les données publiques ouvertes, le portail européen e-justice, l'Internet plus sûr et le règlement des litiges en ligne.

L'Europe à large bande (*Broadband Europe*) fait la promotion la stratégie de la Commission européenne sur la connectivité pour une société européenne dotée d'une capacité d'un gigabit d'ici 2025, ainsi que de la vision définie par la décennie numérique pour la transformation numérique de l'Europe d'ici 2030, afin de connecter les citoyens et les entreprises de l'Europe à des réseaux à très haute capacité.

Cette vision de la société dotée d'une capacité d'un Gigabit d'ici 2025 repose sur trois objectifs stratégiques principaux :

1. la connectivité dotée d'une capacité d'un gigabit pour tous les principaux moteurs socio-économiques;
2. la couverture 5G ininterrompue pour toutes les zones urbaines et les principales voies de transport terrestre.
3. l'accès à une connectivité d'au moins 100 mbps pour tous les ménages européens.

L'ambition de la décennie numérique de l'Europe est que d'ici 2030, tous les foyers européens soient couverts par un réseau doté d'une capacité d'au moins un gigabit et que toutes les zones peuplées soient couvertes par la 5G.

4.2 Résultats réglementaires des pannes et perturbations de réseau

Cybersécurité

Tableau 18. Pannes ou dégradations liées à la cybersécurité

ADMIN.	DATE	TYPE D'INFRA-STRUCTURE	DESCRIPTION DE LA PANNE	DESCRIPTION DES RÉSULTATS
Union européenne	26-09-2020	Réseau sans fil	En septembre 2020, le fournisseur de service de télécommunications (FST) Magyar Telekom (filiale de Deutsche Telekom) a connu une panne causée par un déni de service distribué (DDoS). Selon Magyar, le volume de l'attaque était dix fois supérieur au volume de trafic généralement observé lors d'attaques DDoS.	Il était impossible de vérifier si des mesures réglementaires avaient été prises à la suite de cette panne (rapports d'incidents, enquêtes, mesures législatives, recommandations, amendes, etc.).
Union européenne	03-05-2022	Satellite	En mai 2022, le FST Orange a connu une panne lorsque les services de Viasat (un opérateur de satellites américain) ont été interrompus par un « cyberévénement ». La panne a touché environ 40 000 abonnés à Internet par satellite dans l'Union européenne.	Il était impossible de vérifier si des mesures réglementaires avaient été prises à la suite de cette panne (rapports d'incidents, enquêtes, mesures législatives, recommandations, amendes, etc.).
Corée du Sud	29-01-2023	Réseau sans fil	En janvier 2023, le FST sud-coréen LG U+ a connu des perturbations du réseau de ses services de données mobiles. Les perturbations ont duré en moyenne 63 minutes et seraient dues à une attaque DDoS.	Le ministère des Sciences et des Technologies de l'information et des Communications et l'Agence sud-coréenne de sécurité Internet ont ouvert une enquête sur les récentes atteintes à la sécurité des données et les pannes. Le ministère a adressé un avertissement sévère à LG U+ concernant l'absence d'un système de base de réaction en cas d'infraction. Le ministère a également demandé à LG U+ de mettre en œuvre des mesures correctives responsables et

ADMIN.	DATE	TYPE D'INFRA-STRUCTURE	DESCRIPTION DE LA PANNE	DESCRIPTION DES RÉSULTATS
				d'encourager l'amélioration des politiques, y compris la révision de la réglementation concernant les principaux FST en matière de système de réaction en cas d'infraction.

Facteurs environnementaux

Tableau 19. Pannes ou perturbations liées à l'environnement

ADMIN.	DATE	TYPE D'INFRA-STRUCTURE	DESCRIPTION DE LA PANNE	DESCRIPTION DES RÉSULTATS
Nouvelle-Zélande	7-12-2019	Réseau sans fil et filaire – terrestre	En décembre 2019, le FST Spark de la Nouvelle-Zélande a connu une panne causée par des pluies torrentielles et des inondations. La panne s'est produite lorsqu'un câble à fibres optiques a été sectionné entre les villes d'Ashburton et de Timaru, ce qui a privé de service des milliers de clients.	Il était impossible de vérifier si des mesures réglementaires avaient été prises à la suite de cette panne (rapports d'incidents, enquêtes, mesures législatives, recommandations, amendes, etc.).
Australie	2020-01-17	Réseau sans fil et filaire – terrestre	En janvier 2020, l'Australie a connu une grave saison de feux de brousse qui a provoqué des pannes sur tous les principaux réseaux de FST. Selon l'Australian Communications and Media Authority (ACMA), près de 1 400 installations de télécommunications ont été directement ou indirectement touchées par les feux de brousse de l'été, au cours desquels l'interruption moyenne a été de trois jours et demi et la plus longue de 23 jours. La cause principale de la majorité des pannes était les pannes de courant. Le Réseau national à large bande (*National Broadband Network*) a déployé des génératrices pour rétablir l'alimentation électrique des	En avril 2020, l'ACMA a publié un rapport qui décrit en détail les impacts des feux de brousse de 2019 - 2020 sur le réseau des FST. Les observations comprennent l'analyse des causes profondes et l'analyse des mesures de rétablissement. Aucune recommandation ou mesure législative n'a été formulée.

ADMIN.	DATE	TYPE D'INFRA-STRUCTURE	DESCRIPTION DE LA PANNE	DESCRIPTION DES RÉSULTATS
			services une fois que les feux de brousse étaient passés.	
Nouvelle-Zélande	2023-01-27	Réseau sans fil et filaire – terrestre	En janvier 2023, la ville d'Auckland en Nouvelle-Zélande a connu un épisode météorologique violent qui a provoqué de petites inondations localisées. Les inondations ont entraîné des pannes dans les réseaux des FST (Chorus et Spark) en raison de pannes de courant.	Il était impossible de vérifier si des mesures réglementaires avaient été prises à la suite de cette panne (rapports d'incidents, enquêtes, mesures législatives, recommandations, amendes, etc.).
Nouvelle-Zélande	2023-02-13	Réseau sans fil et filaire – terrestre	En février 2023, la Nouvelle-Zélande a été frappée par le cyclone Gabrielle, qui a provoqué d'importantes pannes et des dégâts considérables dans tout le pays. Cet événement a touché tous les principaux FST néo-zélandais (Vondafone, 2degrees, etc.) qui ont connu des pannes généralisées en raison des dommages causés à l'infrastructure ou des pannes de courant dans les stations cellulaires.	En réponse immédiate à l'événement, les FST et les équipes d'intervention d'urgence se sont efforcés de réparer les réseaux touchés. Ils se sont appuyés en grande partie sur le déploiement de génératrices de secours sur les sites touchés. Il était impossible de vérifier si des mesures réglementaires avaient été prises à la suite de cette panne (rapports d'incidents, enquêtes, mesures législatives, recommandations, amendes, etc.).

Erreurs opérationnelles

Tableau 20. Pannes ou perturbations opérationnelles

ADMIN.	DATE	TYPE D'INFRA-STRUCTURE	DESCRIPTION DE LA PANNE	DESCRIPTION DES RÉSULTATS
Royaume-Uni	2018-06-12	Réseau sans fil	En décembre 2018, le FST O2 a connu une panne de réseau majeure qui a entraîné une perte de services de données pour la majorité de ses clients sur ses réseaux 2G, 3G et 4G. La cause première de la panne a été déterminée comme étant un certificat logiciel expiré.	Il était impossible de vérifier si des mesures réglementaires avaient été prises à la suite de cette panne (rapports d'incidents, enquêtes, mesures législatives, recommandations, amendes, etc.).

ADMIN.	DATE	TYPE D'INFRA-STRUCTURE	DESCRIPTION DE LA PANNE	DESCRIPTION DES RÉSULTATS
Nouvelle-Zélande	2019-03-13	Réseau sans fil	En mars 2019, le TSP Spark a connu une panne qui a privé les clients d'une région d'Auckland de services de voix, de données mobiles et de messagerie texte pendant trois jours. La cause de la panne a été déterminée comme étant un problème avec la liaison par fibre optique Chorus qui relie la tour cellulaire de la région au reste du réseau Spark.	Il était impossible de vérifier si des mesures réglementaires avaient été prises à la suite de cette panne (rapports d'incidents, enquêtes, mesures législatives, recommandations, amendes, etc.).
Royaume-Uni	17/10//19	Réseau sans fil	En octobre 2019, le FST britannique Three a connu une panne qui a touché les services de voix, de texte et de données de millions de ses clients. La cause a été déterminée comme étant une erreur survenue lors de réparations de routine de l'infrastructure du réseau 3G de Three.	Il était impossible de vérifier si des mesures réglementaires avaient été prises à la suite de cette panne (rapports d'incidents, enquêtes, mesures législatives, recommandations, amendes, etc.).
Union européenne	2020-11-23	Réseau sans fil	En mars 2019, le FST Vodafone a connu une panne généralisée qui a touché plus de 100 000 utilisateurs au sein de son réseau allemand. La panne a duré environ cinq heures pour la plupart des clients et la cause a été déterminée comme étant un bris de l'équipement de régulation.	Il a été impossible de déterminer si des mesures réglementaires avaient été prises pour cette panne (rapports d'incidents, enquêtes, mesures législatives, recommandations, amendes, etc.).
Corée du Sud	2021-01-10	Réseau sans fil et filaire – terrestre	En octobre 2021, le FST sud-coréen KT Corp a connu des pannes généralisées des services Internet et téléphoniques en raison d'une erreur d'acheminement. L'erreur d'acheminement a été causée par l'erreur d'un employé d'un sous-traitant de KT. Le réseau a été rétabli en moins d'une heure.	Conformément à sa politique d'indemnisation, KT a versé près de 40 milliards de wons (33,97 millions de dollars) en indemnités aux clients de ses services filaires et sans fil. En outre, KT a déclaré qu'il intégrerait un banc d'essai qui simulera le processus d'acheminement avant qu'il ne soit exécuté, afin d'éviter qu'il ne se reproduise, et que KT développerait un système

ADMIN.	DATE	TYPE D'INFRA-STRUCTURE	DESCRIPTION DE LA PANNE	DESCRIPTION DES RÉSULTATS
				existant qui bloque la diffusion des erreurs d'acheminement.
Japon	2021-10-14	Réseau sans fil	En octobre 2021, le FST japonais Nippon Telegraph and Telephone (NTT) Docomo a connu une panne de réseau qui a touché environ 12,9 millions d'utilisateurs. La panne a été causée par un dysfonctionnement lors de travaux sur le réseau d'équipements de paiement de NTT Docomo, et les utilisateurs concernés n'ont pas eu accès aux services de voix ou de données pendant 29 heures.	Le ministère des Affaires intérieures et des Communications (MAIC) a décrit l'incident comme ayant un impact sociétal énorme et a déclaré que des mesures suffisantes devaient être prises pour s'assurer qu'il ne se reproduise pas. NTT Docomo a publié un rapport d'incident et a introduit un nouveau système pour contrôler séparément les téléphones mobiles en cas de défaillance du système.
Nouvelle-Zélande	2022-03-02	Réseau sans fil	En février 2022, le FST 2degree a connu une panne qui a touché des milliers de clients dans toute la Nouvelle-Zélande. Les clients concernés n'auraient pas eu accès au réseau du FST pendant plus d'une heure. La cause de la panne est inconnue, mais elle a été déclarée comme un « problème interne » par un représentant de 2degree.	Il était impossible de vérifier si des mesures réglementaires avaient été prises à la suite de cette panne (rapports d'incidents, enquêtes, mesures législatives, recommandations, amendes, etc.).
Japon	2022-05-07	Réseau sans fil	En juillet 2022, le FST japonais KDDI Corporation a connu une panne de réseau qui a touché près de 22,78 millions de clients des services de voix sur évolution long terme (VoLTE) et 7,65 millions de clients des services de données (4G/5G) sur une période de trois jours. La panne s'est produite lors de travaux d'entretien de routine, lorsqu'un routeur pour les appels VoLTE a été remplacé, ce qui a entraîné une panne des services de messagerie texte et d'appels téléphoniques (y compris la ligne d'urgence).	KDDI a remis un rapport d'incident au MAIC le 29 juillet 2022. Ce rapport présente une vue d'ensemble de l'incident (cause, portée et impact), un aperçu des mesures de prévention pour éviter toute récidive et une description du remboursement accordé aux clients concernés (environ 200 yens par clients).

ADMIN.	DATE	TYPE D'INFRA-STRUCTURE	DESCRIPTION DE LA PANNE	DESCRIPTION DES RÉSULTATS
Nouvelle-Zélande	2022-10-04	Réseau sans fil	En octobre 2022, un problème technique a empêché des milliers de clients de 2degree d'accéder aux services d'appel, de messagerie texte et de données. La panne a duré environ 2 heures avant d'être résolue.	Il était impossible de vérifier si des mesures réglementaires avaient été prises à la suite de cette panne (rapports d'incidents, enquêtes, mesures législatives, recommandations, amendes, etc.).
Japon	2022-12-17	Réseau sans fil	En décembre 2022, le FST japonais NTT Docomo a connu une panne de son réseau de données en raison d'un dysfonctionnement de l'équipement de communication. La panne n'a touché que les services de données mobiles et n'a pas touché les services d'appels vocaux.	Le MAIC a adressé un « avertissement sévère » à NTT Docomo et a publié des orientations, en demandant à NTT de mettre en œuvre diverses mesures pour éviter qu'une telle situation ne se reproduise.
Australie	2023-01-03	Réseau sans fil	En mars 2023, le FST Optus a connu une panne qui a touché des zones rurales notamment Copmanhurst, Whiteman Creek, Jackadgery. Des centaines de clients ont été dans l'impossibilité de passer des appels téléphoniques ou d'envoyer ou de recevoir des messages texte. De plus le service des pompiers rural de Copmanhurst était dans l'incapaticté d'utiliser les applications ACTIV qui les préviennent en cas d'urgence et leur permettent de communiquer directement les uns avec les autres lorsqu'ils répondent à des appels d'urgence.	Il était impossible de vérifier si des mesures réglementaires avaient été prises à la suite de cette panne (rapports d'incidents, enquêtes, mesures législatives, recommandations, amendes, etc.).
Japon	2023-03-04	Réseau filaire – terrestre	En avril 2023, les fournisseurs de services de télécommunications japonais NTT East et West ont connu une panne de réseau qui a touché 446 000 lignes Internet et 233 000 lignes fixes. Les services touchés comprenaient les appels aux	Lors d'une conférence de presse en ligne, les responsables de NTT ont reconnu que la panne constituait un « incident grave » au regard de la loi. Le MAIC pourrait prendre des mesures administratives, mais l'incident

ADMIN.	DATE	TYPE D'INFRA-STRUCTURE	DESCRIPTION DE LA PANNE	DESCRIPTION DES RÉSULTATS
			services d'urgence, tels que le 110 et le 119. La cause de la panne a été déclarée comme une « défaillance de l'équipement » et les services ont été rétablis dans un délai d'environ 3 heures.	fait toujours l'objet d'une enquête.
Royaume-Uni	2023-04-04	Réseau sans fil	En avril 2023, le FST britannique Virgin Media a connu une panne qui a touché l'accès aux services Internet à large bande de plus de 50 000 clients. La cause première du problème a été déterminée comme étant un problème technique.	Il était impossible de vérifier si des mesures réglementaires avaient été prises à la suite de cette panne (rapports d'incidents, enquêtes, mesures législatives, recommandations, amendes, etc.).
Union européenne	2023-04-14	Réseau sans fil	En avril 2023, le FST Vondafone a connu une panne qui a touché son réseau de téléphonie mobile aux Pays-Bas. La panne a affecté la capacité des clients à passer des appels, y compris aux services d'urgence. La cause de la panne a été déterminée comme étant un dysfonctionnement interne.	Il était impossible de vérifier si des mesures réglementaires avaient été prises à la suite de cette panne (rapports d'incidents, enquêtes, mesures législatives, recommandations, amendes, etc.).
Australie	2023-04-17	Satellite	En avril 2023, le fournisseur de services par satellite Inmarsat a connu une panne sur son satellite I-4 F1 qui fournit des services par bande L pour l'Asie de l'Est et la région du Pacifique. La cause de la panne est une perte d'énergie due à la perte de puissance de l'un de ses panneaux solaires. La panne a eu des répercussions sur divers services fournis par le satellite, notamment les signaux GPS utilisés par les systèmes horticoles, les systèmes de sécurité maritime et l'industrie du transport maritime.	Le 19 avril, Inmarsat a confirmé que tous les services de sécurité et les services de réseau mondial à large bande avaient été rétablis. Cependant, les organismes de réglementation n'ont pas prévu de sanctions publiques ni de rapports.
États-Unis	2023-04-25	Réseau sans fil	En avril 2023, Shenandoah Telecommunications	Pour régler cette affaire, la Commission fédérale des

ADMIN.	DATE	TYPE D'INFRA-STRUCTURE	DESCRIPTION DE LA PANNE	DESCRIPTION DES RÉSULTATS
			Company (Shentel) a connu une panne des services d'acheminement des appels d'urgence 9-1-1 dans les comtés du Wyoming, de Lewis et de McDowell. La panne a été causée par une erreur opérationnelle alors que Shentel remplaçait les contrôleurs de session en périphérie et assurait la transition des clients à un nouveau service d'acheminement des appels 9-1-1.	communications (FCC) a demandé à Shentel de mettre en œuvre un plan de conformité et de payer une amende civile de 227 200 dollars.
Australie	2023-09-05	Réseau sans fil	En mai 2023, le FST australien Telstra Group Limited a connu une panne majeure qui a touché les clients de la Nouvelle-Galles du Sud et du Queensland. Les clients concernés ont rencontré des problèmes pour passer et recevoir des appels et des messages texte. Cependant, Telstra a déclaré que les appels vers triple-0 et l'utilisation des données mobiles n'étaient pas touchés par la panne. La panne a été causée par un problème lié à une mise à niveau planifiée du réseau, qui a eu des effets d'entraînement.	Il était impossible de vérifier si des mesures réglementaires avaient été prises à la suite de cette panne (rapports d'incidents, enquêtes, mesures législatives, recommandations, amendes, etc.).

Facteurs tiers

Tableau 21. Pannes et perturbations liées à des facteurs tiers

ADMIN.	DATE	TYPE D'INFRA-STRUCTURE	DESCRIPTION DE LA PANNE	DESCRIPTION DES RÉSULTATS
États-Unis	2020-06-15	Réseau sans fil	En juin 2020, T-Mobile a subi une panne qui a empêché des clients d'utiliser les services de VoLTE et de messagerie texte. Au départ, la cause était considérée	Le 15 juin 2020, la FCC a annoncé qu'elle lancerait une enquête. L'enquête s'est conclue par un plan de conformité et par un règlement

ADMIN.	DATE	TYPE D'INFRA-STRUCTURE	DESCRIPTION DE LA PANNE	DESCRIPTION DES RÉSULTATS
			comme une attaque DDoS, mais il s'est avéré qu'il s'agissait d'un problème de surcharge causée par la défaillance d'un circuit en fibre loué auprès d'un fournisseur tiers dans le sud-est du pays. Le problème a été résolu le jour même à 22 h 3 (heure normale du Pacifique).	à l'amiable de 19,5 millions de dollars.
Japon	2022-09-12	Réseau sans fil	En septembre 2022, le FST japonais Rakuten Mobile, Inc. a connu une panne de réseau qui a privé 110 000 clients de son service de téléphonie et 1,3 million de clients de son service de transmission de données. La cause de la panne est dysfonctionnement d'un logiciel d'un centre de données.	Le MAIC a adressé un avertissement au fournisseur de services de communication et a inspecté le centre de données pour confirmer que des mesures correctives ont été mises en place.
Australie	2023-04-20	Réseau sans fil	En avril 2023, le FST australien MATE a connu une panne majeure qui a touché les services Internet à large bande et mobiles de clients dans toute l'Australie. Les perturbations les plus importantes se sont fait sentir dans les États de Nouvelle-Galles du Sud, de Victoria et de l'Australie-Occidentale. La cause de la panne est due à une défaillance technique dans un centre de données à Sydney.	Il était impossible de vérifier si des mesures réglementaires avaient été prises à la suite de cette panne (rapports d'incidents, enquêtes, mesures législatives, recommandations, amendes, etc.).

Dommages involontaires ou intentionnels

Tableau 22. Pannes et perturbations liées à des dommages involontaires ou intentionnels

ADMIN.	DATE	TYPE D'INFRA-STRUCTURE	DESCRIPTION DE LA PANNE	DESCRIPTION DES RÉSULTATS
Corée du Sud	2018-11-15	Réseau sans fil et	En novembre 2018, le FST sud-coréen KT Corp. a connu une panne qui a paralysé son	Pour discuter des contre-mesures, des représentants de KT et de South Korean Broadband ont assisté

ADMIN.	DATE	TYPE D'INFRA-STRUCTURE	DESCRIPTION DE LA PANNE	DESCRIPTION DES RÉSULTATS
		filaire – terrestre	réseau filaire, mobile et Internet dans certains secteurs de Séoul. La cause est due à un incendie dans le sous-sol où se trouvait la station de base de KT. Il a fallu 10 heures pour éteindre complètement l'incendie et la panne a duré environ 24 heures au total.	le dimanche matin à une réunion gouvernementale à laquelle participaient également le ministre des Sciences et des TIC et la Commission des communications coréenne. KT a prévu d'indemniser les personnes touchées et s'est engagé à mettre en place des mesures rigoureuses pour éviter qu'un tel incident se reproduise.
Nouvelle-Zélande	2020-11-05	Réseau sans fil	En mai 2020, le FST Spark a connu une panne des services de téléphonie mobile, de messagerie texte et de transmission de données parce qu'une personne mal intentionnée a mis le feu à une tour cellulaire. Le lendemain, Spark a déployé une tour cellulaire temporaire pour augmenter la capacité dans le secteur pendant la réparation de l'autre tour cellulaire.	Il était impossible de vérifier si des mesures réglementaires avaient été prises à la suite de cette panne (rapports d'incidents, enquêtes, mesures législatives, recommandations, amendes, etc.).
Union européenne	2022-04-27	Réseau filaire – terrestre	En avril 2022, le réseau de télécommunications français a connu une panne majeure en raison d'actes de vandalisme coordonnés. Des clients des quatre coins de la France n'avaient plus accès au réseau à large bande parce que des personnes mal intentionnées avaient endommagé plusieurs câbles souterrains.	À la suite de cet incident, une enquête a été lancée par la police locale et la Fédération française des télécommunications. L'enquête n'a donné lieu à aucune mesure réglementaire (rapports d'incidents, enquêtes, mesures législatives, recommandations, amendes, etc.).
Nouvelle-Zélande	2022-05-13	Réseau filaire – terrestre	En mai 2020, le FST Chorus a connu une panne de ses services Internet par fibre après qu'un rongeur ait rongé des câbles à fibre optique. La panne a touché environ 1 000 clients et a duré au total 33 heures.	Il était impossible de vérifier si des mesures réglementaires avaient été prises à la suite de cette panne (rapports d'incidents, enquêtes, mesures législatives, recommandations, amendes, etc.).
Royaume-Uni	2022-10-21	Réseau filaire – sous-marin	En octobre 2022, des FST shetlandais ont connu une panne qui a affecté les services filaires, mobiles et	Déclarée comme un incident majeur, cette panne de réseau a été déclarée à l'Office of Communications (Ofcom) en vertu de la *Telecommunications*

ADMIN.	DATE	TYPE D'INFRA-STRUCTURE	DESCRIPTION DE LA PANNE	DESCRIPTION DES RÉSULTATS
			Internet. La panne a été causée par une coupure d'un câble sous-marin qui relie l'île au réseau continental écossais. Un chalutier enregistré au Royaume-Uni est soupçonné d'avoir endommagé par accident le câble.	*(Security) Act 2021*. L'examen de l'Ofcom a noté que le rétablissement des services a été réalisé en augmentant la production d'énergie à la source. Au cours des dix jours suivant l'incident, des réparations ont été effectuées sur les câbles à fibre optique primaires et secondaires vers les îles, ce qui a permis de rétablir les services de manière permanente. De plus, dans le cadre de son programme R100, le gouvernement écossais a installé 16 nouveaux câbles sous-marins qui relient 15 îles écossaises à des services à large bande plus rapides et plus fiables.
Union européenne	2023-02-16	Réseau filaire – terrestre	En février 2023, le FST Deutsche Telekom a connu une panne qui a affecté le groupe Lufthansa, compagnie aérienne de premier plan, et a causé d'importants retards et annulations de vols. La panne a été causée par des entrepreneurs en construction qui travaillaient pour l'entreprise ferroviaire publique Deutsche Bahn et qui ont accidentellement sectionné quatre câbles enfouis à plus de 16 pieds (4,8 mètres) de profondeur.	Il était impossible de vérifier si des mesures réglementaires avaient été prises à la suite de cette panne (rapports d'incidents, enquêtes, mesures législatives, recommandations, amendes, etc.).

4.3 Analyse des initiatives de satellites en orbite basse des administrations

Cette analyse des satellites en orbite basse (LEO) dans les différentes administrations est un portrait actuel de certains des exemples de couverture par satellite LEO observés dans les différentes administrations évaluées. Il convient de noter qu'il s'agit d'une technologie très dynamique et changeante. Gartner s'attend à ce que les renseignements présentés ci-dessous soient obsolètes en quelques semaines (et non en quelques mois ou années). L'évaluation portait sur les catégories de base que sont les services Internet, de messagerie texte et de téléphonie.

Tableau 23. Analyse des initiatives de satellites LEO des administrations

Admin.	Description des initiatives de satellites LEO en cours
États-Unis	▪ La Commission fédérale des communications (FCC) a approuvé les licences (en anglais seulement) pour le déploiement de constellations de satellites LEO des entreprises suivantes : SpaceX, Telesat, Kepler, LeoSat et Project Kuiper (en anglais seulement). Ces licences autorisent les entreprises à fournir des services Internet par satellite aux entités américaines (en anglais seulement). ▪ En janvier 2022, la FCC a accordé à l'entreprise Lynk, basée en Virginie, la première licence qui permet d'offrir des communications directes par satellite vers un téléphone ordinaire (SCS). La FCC désigne la couverture supplémentaire depuis l'espace par l'acronyme « SCS » (*Supplemental-Coverage-From-Space*). Il semblerait que l'industrie utilise désormais la « communication directe aux appareils » (*Direct to Device* [D2D]), mais cela pourrait encore changer. ▪ En 2022, Lynk (en anglais seulement) a effectué des essais précommerciaux au cours desquels elle a réussi à utiliser la couverture supplémentaire depuis l'espace pour connecter 6 000 appareils afin d'envoyer et de recevoir des messages. L'objectif actuel est de lancer des services commerciaux au printemps 2023 (en anglais seulement). ▪ AT&T a demandé à la FCC l'autorisation d'utiliser la couverture supplémentaire depuis l'espace d'AST SpaceMobile sur une partie de son spectre commercial. AT&T a effectué des essais de transmission directe par satellite vers téléphone (en anglais seulement) avec AST SpaceMobile sur le spectre de la bande 14, mais la licence nationale du spectre pour ces ondes appartient à FirstNet Authority. ▪ En août 2022, SpaceX et T-Mobile ont annoncé un plan en vue de fournir un service depuis l'espace (en anglais seulement) aux téléphones mobiles dans les zones non couvertes par le réseau cellulaire de T-Mobile.
Royaume-Uni	▪ En avril 2023, le ministère de la Science, de l'Innovation et de la Technologie a annoncé que la société OneWeb, basée à Londres, déploiera (en partenariat avec BT et Clarus) sa technologie Internet par satellite LEO pour offrir des services Internet par satellite aux clients des îles Shetland et de l'île de Lundy. L'essai réalisé par la société OneWeb a été annoncé dans le cadre de la stratégie d'infrastructure sans fil (en anglais seulement) du ministère.
Australie	▪ En mars 2022, Telstra et la société britannique OneWeb ont signé une entente (en anglais seulement) de dix ans qui prévoit que Telstra construise et entretienne trois nouveaux téléports en Australie afin de fournir un réseau d'information et de support au sol dans l'hémisphère sud pour la flotte croissante de satellites LEO de OneWeb.
Nouvelle-Zélande	▪ En 2023, deux des plus grands fournisseurs de services de télécommunication de la Nouvelle-Zélande, One NZ et 2degrees (en anglais seulement), ont signé des ententes avec des fournisseurs de services par satellite (SpaceX et Lynk, respectivement). Les services initiaux seront limités aux messages textes, et les services de voix et de données suivront.
Japon	▪ En décembre 2022, KDDI et SpaceX (en anglais seulement) ont lancé la première tour mobile au Japon alimentée par SpaceX et ont commencé à offrir commercialement des services Internet par satellite à Hatsushima. KDDI compte étendre la couverture à un total de 1 200 tours éloignées.

Admin.	Description des initiatives de satellites LEO en cours
	▪ En novembre 2022, le quatrième opérateur de réseau de télécommunications en importance du Japon, Rakuten Mobile, a reçu une licence de station expérimentale (en anglais seulement) préliminaire pour effectuer une série d'essais de communication mobile et de vérifications préliminaires au Japon. En avril 2023, Rakuten Mobile et le concepteur et fabricant de satellites AST SpaceMobile, basé aux États-Unis, ont réalisé le premier appel vocal bidirectionnel (en anglais seulement) au monde avec des téléphones mobiles standard en utilisant le satellite BlueWalker 3 (BW3).
Union européenne	▪ Dans le cadre du Programme de l'Union européenne pour une connectivité sécurisée, le Parlement européen et la Commission européenne ont annoncé des plans de déploiement d'une constellation de satellites de l'Union européenne appelée « IRIS² (Infrastructure de résilience, d'interconnexion et de sécurité par satellites) » [en anglais seulement]. (Consortium de Deutsche Telekom et d'Orange [en anglais seulement]) ▪ Le Programme de l'Union européenne pour une connectivité sécurisée suivra une approche progressive, dont l'objectif est de fournir les premiers services (Internet et téléphonie directe) en 2024 et d'atteindre une capacité opérationnelle totale d'ici 2027.

4.4 Références

États-Unis

- Federal Communications Commission | The US (fcc.gov) (en anglais seulement)
- About the FCC | Federal Communications Commission (en anglais seulement)
- *Telecommunications Act of 1996* | Federal Communications Commission (fcc.gov) [en anglais seulement]
- Laws & Regulations - Telecommunications Industry: A Research Guide - Research Guides at Library of Congress (loc.gov) [en anglais seulement]
- *Telecommunications Act of 1996* | Federal Communications Commission (fcc.gov) [en anglais seulement]
- FCC Releases Open Internet Order | Federal Communications Commission (en anglais seulement)
- *Digital Equity Act of 2021* (census.gov) [en anglais seulement]
- Programs | Internet for All (en anglais seulement)
- FCC Acts to Improve Network Resiliency During Disasters | Federal Communications Commission (en anglais seulement)
- Executive Order on Improving the Nation's Cybersecurity | The White House (en anglais seulement)
- Federal Funding | BroadbandUSA (doc.gov) [en anglais seulement]
- Secure and Resilient Mobile Network Infrastructure and Emergency Communications R&D Program | Homeland Security (dhs.gov) [en anglais seulement]
- Emergency Communications R&D Project | Homeland Security (dhs.gov) [en anglais seulement]
- Emergency Communications | Cybersecurity and Infrastructure Security Agency CISA (en anglais seulement)
- Statewide Communication Interoperability Plans Workshops | CISA (en anglais seulement)
- Biden-Harris Administration Launches $1.5 Billion Innovation Fund to Develop a More Competitive and Diverse Telecommunications Supply Chain | National Telecommunications and Information Administration (ntia.gov) [en anglais seulement]
- Wireless Innovation Fund Notice of Funding Opportunity | National Telecommunications and Information Administration (ntia.gov) [en anglais seulement]
- Connect America Fund (CAF) | Federal Communications Commission (fcc.gov) [en anglais seulement]
- Lifeline Program for Low-Income Consumers | Federal Communications Commission (fcc.gov) [en anglais seulement]
- E-Rate - Schools & Libraries USF Program | Federal Communications Commission (fcc.gov) [en anglais seulement]
- Rural Healthcare Program | Federal Communications Commission (fcc.gov) [en anglais seulement]
- 911 and E911 Services | Federal Communications Commission (fcc.gov) [en anglais seulement]
- AT&T, Verizon, others fined for 911 outages | Light Reading (en anglais seulement)
- Verizon, Straight Path pay $614 million civil penalty to U.S. FCC: statement | Reuters (en anglais seulement)
- Data Protection Laws and Regulations Report 2022-2023 US (iclg.com) [en anglais seulement]
- New US Privacy Law May Give Telecoms Free Pass on $200 Million Fines (vice.com) [en anglais seulement]
- VIII. Privacy — *Telephone Consumer Protection Act* (fdic.gov) [en anglais seulement]

- Data Protection Laws and Regulations Report 2022-2023 US (iclg.com) [en anglais seulement]

Royaume-Uni

- Home - Ofcom (en anglais seulement)
- What is Ofcom? - Ofcom (en anglais seulement)
- Telecoms security: proposal for new regulations and code of practice - GOV.UK (en anglais seulement)
- Telecommunications Networks – a vital part of the Critical National Infrastructure, v1.1 - EC-RRG (publishing.service.gov.uk) [en anglais seulement]
- Future Telecoms Infrastructure Review.pdf (en anglais seulement)
- E02781980 Telecommunications Security CoP Accessible.pdf (en anglais seulement)
- Ofcom fines O2 £150,000 for providing inaccurate and incomplete information - Ofcom (en anglais seulement)
- Ofcom fines O2 £10.5m for overcharging customers - Ofcom (en anglais seulement)
- Ofcom fines Sepura £1.5m for breaking competition law - Ofcom (en anglais seulement)
- Ofcom fines BT £42,500 over inaccurate information (en anglais seulement)
- The Electronic Communications (Universal Service) (Broadband) Order 2018 (legislation.gov.uk) [en anglais seulement]
- Statement: Delivering the Broadband Universal Service - Ofcom (en anglais seulement)
- UK government imposes its own security obligations on telecoms sector - Telecoms.com (en anglais seulement)
- Regulation of VoIP Services: Access to the Emergency Services - Ofcom (en anglais seulement)
- Emergency Services Network: overview - GOV.UK (www.gov.uk) [en anglais seulement]
- Investment in telecoms innovation and R&D - GOV.UK (www.gov.uk) [en anglais seulement]
- 5G Supply Chain Diversification Strategy - GOV.UK (www.gov.uk) [en anglais seulement]
- UK Wireless Infrastructure Strategy - GOV.UK (www.gov.uk) [en anglais seulement]

Australie

- Homepage | ACMA (en anglais seulement)
- Fines, warnings and the ACMA's 2021-22 priorities: The telco industry in May (holdingredlich.com) [en anglais seulement]
- Telstra pays $1.5 million penalty for breaching customer rights | ACMA (en anglais seulement)
- Australian telecommunications firms fined $22.1 mln for false internet speed claims | Reuters (en anglais seulement)
- TPG forced to pay $2m fine after High Court loss - Telco/ISP - iTnews (en anglais seulement)
- NBN Co faces $30-a-day fines for unfixed faults - Telco/ISP - iTnews (en anglais seulement)
- Telstra Triple Zero outage: Report reveals 1400 calls were unable to be connected (smh.com.au) [en anglais seulement]
- iTWire - Telstra could face big fine over triple-zero outage (en anglais seulement)
- Strengthening Telecommunications Against Natural Disasters (STAND) - Temporary Telecommunications Infrastructure Deployment | business.gov.au (en anglais seulement)
- Telecommunications Disaster Resilience Innovation Program | Department of Infrastructure, Transport, Regional Development, Communications and the Arts (en anglais seulement)
- USO | ACMA (en anglais seulement)
- Universal Service Obligation | Department of Infrastructure, Transport, Regional Development, Communications and the Arts (en anglais seulement)
- National Broadband Network | Department of Infrastructure, Transport, Regional Development, Communications and the Arts (en anglais seulement)

- NBN legislative framework | Department of Infrastructure, Transport, Regional Development, Communications and the Arts (en anglais seulement)
- National Broadband Network – Parliament of Australia (aph.gov.au) [en anglais seulement]
- NBN Co welcomes $2.4 billion Government investment to enable 1.5 million more homes and businesses to upgrade to full fibre nbn | nbn (en anglais seulement)
- Provision of Satellite Connections to Emergency Services and Evacuation Centres | Department of Infrastructure, Transport, Regional Development, Communications and the Arts (en anglais seulement)
- Boosting temporary infrastructure capabilities | Department of Infrastructure, Transport, Regional Development, Communications and the Arts (en anglais seulement)
- Cyber Security | Australian Signals Directorate (asd.gov.au) [en anglais seulement]
- Telecommunications security reforms | Department of Infrastructure, Transport, Regional Development, Communications and the Arts (en anglais seulement)
- Cyber-security-incident-reporting.pdf (en anglais seulement)

Nouvelle-Zélande

- Ministry of Business, Innovation & Enterprise: Emergency Call Services (en anglais seulement)
- Emergency Calls in New Zealand | 2degrees (en anglais seulement)
- Universal Service Obligation | Department of Infrastructure, Transport, Regional Development, Communications and the Arts (en anglais seulement)
- *Telecommunications Act 2001* No 103 (as at 01 September 2022), Public Act – New Zealand Legislation (en anglais seulement)
- A review of New Zealand Telecommunications: Legislation, Regulations and Recommendations | Telsoc (en anglais seulement)
- Govt releases vision for New Zealand's digital connectivity future | Ministry of Business, Innovation & Employment (mbie.govt.nz) [en anglais seulement]
- Homes, businesses to benefit from upgrade to rural broadband | Beehive.govt.nz (en anglais seulement)
- More rural broadband for regional communities | Beehive.govt.nz (en anglais seulement)
- Govt delivers connectivity for rural and remote households | Beehive.govt.nz (en anglais seulement)
- Broadband and mobile programmes | Ministry of Business, Innovation & Employment (mbie.govt.nz) [en anglais seulement]
- New Zealand - Data Protection Overview | Guidance Note | DataGuidance (en anglais seulement)
- Consolidated Telecommunications Information Privacy Code 2020 | Legal research | DataGuidance (en anglais seulement)
- New Zealand - Data Protection Overview | Guidance Note | DataGuidance (en anglais seulement)
- New Zealand's Cyber Security Emergency Response Plan | Department of the Prime Minister and Cabinet (DPMC) [en anglais seulement]

Japon

- *Telecommunications Information Privacy Code 2020* (en anglais seulement)

- Japan: *Telecommunications Business Act* amendments introducing new regulations for cookies and user identification information - Baker McKenzie InsightPlus (en anglais seulement)
- Key telecommunications laws, regulations and policies in Japan - DLA Piper Telecommunications Laws of the World (dlapiperintelligence.com) [en anglais seulement]
- New Japanese Regulation on Telecomunications Businesses Provided by Foreign Business Operators | PwC Japan Group en anglais seulement)
- Telecoms, Media & Internet Laws and Regulations Report 2023 Japan (iclg.com) [en anglais seulement]
- Ribbon Deploys Colt Japan's Emergency Calling Service | Ribbon Communications (en anglais seulement)
- *Disaster Countermeasures Basic Act* - Climate Change Laws of the World (climate-laws.org) [en anglais seulement]
- Access System Technologies for Service Diversification | NTT Technical Review (ntt-review.jp) [en anglais seulement]
- National center of Incident readiness and Strategy for Cybersecurity | NISC (en anglais seulement)
- Japan to bring fiber-optic networks to 99.9% of households by 2028 | The Japan Times (en anglais seulement)

Union européenne

- The NIS2 Directive: A high common level of cybersecurity in the EU | Think Tank | European Parliament (en anglais seulement)
- NIS Directive — ENISA (en anglais seulement)
- For Telcos — ENISA (en anglais seulement)
- Telecom Security Incidents 2021 — ENISA (en anglais seulement)
- *Loi sur la cyberrésilience* | Bâtir l'avenir numérique de l'Europe
- Connecting Europe Facility (CEF Digital) | EU Funding Overview (en anglais seulement)
- Prise en charge du déploiement du haut débit - Bâtir l'avenir numérique de l'Europe
- NIS Investments 2022 — ENISA (en anglais seulement)
- NIS Investments Report 2021 — ENISA (en anglais seulement)
- NIS Investments Report 2020 — ENISA (en anglais seulement)
- Enabling and managing end-to-end resilience — ENISA (en anglais seulement)
- ENISA Report Highlights Resilience of Telecom Sector in Facing the Pandemic — ENISA (en anglais seulement)

Structure organisationnelle et gouvernance – Références :

- What We Do | Federal Communications Commission (en anglais seulement)
- About CISA | CISA (en anglais seulement)
- About NTIA | National Telecommunications and Information Administration (en anglais seulement)
- What is Ofcom? - Ofcom (en anglais seulement)
- Department for Science, Innovation and Technology - GOV.UK (en anglais seulement)
- About the ACCC | ACCC (en anglais seulement)
- ACMA-statement-of-intent-pdf.pdf (en anglais seulement)
- New Zealand Infrastructure Commission/Te Waihanga Act 2019 No 51 (as at 01 September 2022), Public Act Contents – New Zealand Legislation (en anglais seulement)
- Information Brochure on the MSIT (en anglais seulement)
- Bundesnetzagentur - About us (en anglais seulement)
- Arcep | Arcep

- Why Korea fell 27 spots in world internet speed rankings to 32nd place last year (en anglais seulement)
- Korea's internet speed ranking falls to 34th: report (en anglais seulement)

Facteurs gouvernementaux pour l'amélioration de la résilience – Références :

- Biden-Harris Administration Launches $1.5 Billion Innovation Fund to Develop a More Competitive and Diverse Telecommunications Supply Chain | National Telecommunications and Information Administration (ntia.gov) [en anglais seulement]
- E02781980_Telecommunications_Security_CoP_Accessible.pdf (en anglais seulement)
- Provision of Satellite Connections to Emergency Services and Evacuation Centres | Department of Infrastructure, Transport, Regional Development, Communications and the Arts (en anglais seulement)
- Cyber Security | Australian Signals Directorate (asd.gov.au) [en anglais seulement]
- Telecommunications security reforms | Department of Infrastructure, Transport, Regional Development, Communications and the Arts (en anglais seulement)
- National Broadband Network – Parliament of Australia (aph.gov.au) [en anglais seulement]
- NBN legislative framework | Department of Infrastructure, Transport, Regional Development, Communications and the Arts (en anglais seulement)
- NBN Co welcomes $2.4 billion Government investment to enable 1.5 million more homes and businesses to upgrade to full fibre nbn | nbn (en anglais seulement)
- Homes, businesses to benefit from upgrade to rural broadband | Beehive.govt.nz (en anglais seulement)
- New Zealand's Cyber Security Emergency Response Plan (en anglais seulement)
- Japan Sets Aside $450 Million Fund for 6G - Telecom Review Asia Pacific (en anglais seulement)
- The Booklet of Best Practicesof resilient ICT systems in JAPAN (en anglais seulement)
- Japan to bring fiber-optic networks to 99.9% of households by 2028 | The Japan Times (en anglais seulement)
- EU Adaptation Strategy (en anglais seulement)

Obligations réglementaires – Références :

- Universal Service | Federal Communications Commission (fcc.gov) [en anglais seulement]
- 911 and E911 Services | Federal Communications Commission (fcc.gov) [en anglais seulement]
- AT&T, Verizon, others fined for 911 outages | Light Reading (en anglais seulement)
- Verizon, Straight Path pay $614 million civil penalty to U.S. FCC: statement | Reuters (en anglais seulement)
- Telecommunications service obligations | Ministry of Business, Innovation & Employment (mbie.govt.nz) [en anglais seulement]
- The Customer Service Guarantee | ACMA (en anglais seulement)
- Automatic compensation: What you need to know - Ofcom (en anglais seulement)
- Emergency call services | Ministry of Business, Innovation & Employment (mbie.govt.nz) [en anglais seulement]
- Bundesnetzagentur - Public safety (en anglais seulement)
- BSI - Legal basis (en anglais seulement)
- Telecoms, Media & Internet Laws and Regulations Report 2023 Japan (iclg.com) [en anglais seulement]
- Ribbon Deploys Colt Japan's Emergency Calling Service | Ribbon Communications (en anglais seulement)
- EUR-Lex - l24108h - Services de télécommunications abordables : droits des utilisateurs

- Communications Security, Reliability, and Interoperability Council | Federal Communications Commission (en anglais seulement)
- CSRIC_WG 9_Backup_Power_Reccomendations_11-24-2014.pdf (en anglais seulement)
- Inventory of Reports (en anglais seulement)
- Our network security and network resilience work - Ofcom (en anglais seulement)
- Guidance: Protecting access to emergency organisations when there is a power cut at the customer's premises (en anglais seulement)
- The NIS Regulations 2018 - GOV.UK (en anglais seulement)
- Impacts of the 2019-20 bushfires on the telecommunications network | ACMA (en anglais seulement)
- Federal Network Agency - Security requirements (en anglais seulement)
- Code Compliance | NZ Telecommunications Forum (en anglais seulement)
- ETSI TR 102 445 V1.2.1 (2023-04) Emergency Communications (EMTEL); Overview of Emergency Communications Network Resilience and Preparedness (en anglais seulement)

Mesures volontaires de l'industrie – Références :

- Communications Security, Reliability, and Interoperability Council | Federal Communications Commission (en anglais seulement)
- Communications Security, Reliability, and Interoperability Reports | Federal Communications Commission (en anglais seulement)
- Disaster Information Reporting System (DIRS) | Federal Communications Commission (en anglais seulement)
- Electronic Communications Resilience and Response Group (en anglais seulement)
- ETSI TR 102 445 V1.2.1 (2023-04) Emergency Communications (EMTEL); Overview of Emergency Communications Network Resilience and Preparedness (en anglais seulement)

Autres initiatives et technologies – Références :

- FCC approves SpaceX, Telesat, LeoSat and Kepler internet constellations - SpaceNews (en anglais seulement)
- International Bureau Grants Kuiper Satellite Modification | Federal Communications Commission (en anglais seulement)
- Engadget - Amazon secures key FCC approval to deploy its Project Kuiper broadband satellites (en anglais seulement)
- FCC grants Lynk first license for commercial satellite-direct-to-phone service - Urgent Comms (en anglais seulement)
- Lynk announces deployments, plans for spring satellite-direct-to-phone commercial service - Urgent Comms (en anglais seulement)
- Nextivity supports satellite-direct-to-phone operations on FirstNet spectrum, looks to upgrade HPUE next year - Urgent Comms (en anglais seulement)
- Ars Technica - A Virginia company has connected mobile phones directly to satellites (en anglais seulement)
- Arts Technica - Forget 5G wireless, SpaceX and T-Mobile want to offer Zero-G coverage (en anglais seulement)
- https://www.uktech.news/deep-tech/oneweb-trials-20230411 (en anglais seulement)
- Telstra signs 10-year teleport support deal with OneWeb | ZDNET (en anglais seulement)
- One NZ and 2degrees sign up with satellite providers (en anglais seulement)
- KDDI launches the 1st Mobile Tower powered by SpaceX's Starlink in Japan (en anglais seulement)
- Rakuten Mobile given preliminary licences to test LEO (en anglais seulement)

- Rakuten Mobile and AST SpaceMobile claim a 'first' with ground-breaking mobile broadband call (en anglais seulement)
- Welcome IRIS²: Infrastructure for Resilience, Interconnectivity and Security by Satellite (en anglais seulement)
- Deutsche Telekom and Orange head up consortium in bid for EU satellite constellation (en anglais seulement)