

BÂTIR UN **CANADA SÉCURITAIRE** ET **RÉSILIENT**
Réseau à large bande de sécurité publique
Bureau temporaire de coordination nationale

Rapport d'étape sur le Réseau à large bande de sécurité publique

Vers la prochaine génération de communication de la sécurité publique au Canada

Partenaires en gestion des urgences en collaboration avec le gouvernement du Canada

No de cat. : PS4-255/2019F-PDF
ISBN : 978-0-660-31616-1

Table des matières



Sommaire exécutif

Le Bureau temporaire de coordination nationale (BTCN) mis sur pied en juillet 2018 a pour mandat d'élaborer des options et des recommandations à l'intention des premiers intervenants et du personnel de la sécurité publique du Canada à propos du réseau à large bande de sécurité publique (RLBSP). Le BTCN a consulté des intervenants et des experts du terrain, a examiné les études et la documentation actuellement disponibles, ainsi que des rapports de projets pilotes et d'essais, et a réalisé une analyse exhaustive en vue d'élaborer les recommandations soumises dans le présent rapport d'étape. Le BTCN présentera un document de politique au début de 2020. Il convient de noter que ce document se veut un indicateur des progrès réalisés dans le cadre des activités du BTCN; il est par ailleurs entendu que les nouvelles informations d'importance qui sont recueillies entre l'élaboration du présent rapport et celle du document de politique pourraient influencer les recommandations.

Composition du Bureau temporaire de coordination nationale

Fédéral	Provincial et territorial	Non gouvernemental
Agence des services frontaliers du Canada	Gouvernement de l'Alberta	Association canadienne des chefs de police
Centre des sciences pour la sécurité de Recherche et développement pour la défense Canada	Gouvernement de l'Ontario	Association canadienne des chefs de pompiers
Gendarmerie royale du Canada	Gouvernement de la Colombie-Britannique	Chefs paramédics du Canada
Innovation, Sciences et Développement économique Canada	Gouvernement de la Nouvelle-Écosse	Fédération canadienne des municipalités
Ministère de la Défense nationale du Canada	Gouvernement de la Saskatchewan	
Sécurité publique Canada	Gouvernement du Manitoba	
Service canadien du renseignement de sécurité	Gouvernement du Nouveau-Brunswick	
	Gouvernement du Québec	
	Gouvernement du Yukon	

Qu’est-ce qu’un RLBSP?

Le RLBSP est un réseau national de communication sans fil et, à l’instar des réseaux cellulaires, celui-ci permet de transmettre des données d’utilisateurs du point A au point B lors de séances de communication. Le RLBSP est mis à profit de manière à soutenir un large éventail de systèmes, d’applications et de services connexes de l’écosystème global des communications de la sécurité publique. Contrairement aux réseaux cellulaires commerciaux, le RLBSP est conçu pour répondre aux besoins distincts des utilisateurs de la sécurité publique.

Ce que nous avons entendu

La communauté de la sécurité publique continue de travailler sans relâche à l’amélioration des communications en matière de sécurité publique, et en définitive à l’amélioration des interventions d’urgence et des opérations quotidiennes de son secteur. Dans le cadre des activités de sensibilisation et de mobilisation du BTCN, les premiers intervenants et les membres de la communauté de la sécurité publique consultés ont souligné l’importance de disposer d’un système de communication interopérable et sécurisé qui garantit le respect des priorités et des droits de préemption en cas de nécessité et qui permet d’assurer une couverture uniforme adéquate, et ce, tout en demeurant durable et abordable pour les utilisateurs. Étant considéré la manière dont les communications évoluent dans la sphère de la sécurité publique et le développement de la large bande sans fil, le RLBSP se veut un réseau mobile de transmission de données à haute vitesse qui permettrait d’améliorer grandement l’efficacité des interventions et des communications en matière de sécurité publique. Le BTCN s’emploie donc à élaborer des options et des recommandations qui répondent aux besoins et aux exigences des utilisateurs et des intervenants futurs du RLBSP.

Principes du RLBSP

Pour satisfaire aux besoins des premiers intervenants et améliorer leurs capacités en matière de communication, le RLBSP doit offrir un service équitable à l’ensemble de la communauté de la sécurité publique. La qualité de l’expérience est le fondement du RLBSP, car celle-ci témoigne de l’universalité de son service et constitue la base des neuf principes présentés ci-après.

1. Interopérabilité : Le RLBSP permet à ses utilisateurs de communiquer et partager de l’information, conformément aux autorisations prévues, et ce, en tout temps et depuis tout lieu où celui-ci est accessible.

2. Permanence de l’accès au réseau : Que ce soit dans le cadre de leurs activités quotidiennes, ou encore d’événements ou d’urgences d’importance majeure, les utilisateurs du réseau doivent disposer en permanence d’un accès immédiat et ininterrompu au RLBSP, partout où celui-ci s’étend.

3. Couverture : Le RLBSP offrira, à tout le moins, une couverture équivalente à celle de la technologie commerciale à large bande et devra étendre sa couverture aux zones et collectivités urbaines, rurales, autochtones et éloignées qui sont mal desservies, ou améliorer sa couverture dans ces régions.

4. Résilience et robustesse : Le RLBSP doit être résilient et robuste pour répondre aux exigences en matière d'accès au réseau.

5. Prestation des services essentiels à la mission : Le RLBSP permettra de fournir aux utilisateurs de la sécurité publique des services essentiels à la mission (SEM) qui seront hébergés par le réseau.

6. Sécurité : Le RLBSP doit comprendre des mécanismes de sécurité qui répondent aux exigences de confiance des organisations d'utilisateurs du RLBSP et de celles qui se servent de ce dernier pour échanger des données.

7. Durabilité : Le RLBSP doit répondre aux besoins de la première génération d'intervenants sans compromettre sa capacité de satisfaire aux besoins des futurs intervenants.

8. Abordabilité : Le RLBSP doit être abordable pour l'ensemble de la communauté d'utilisateurs.

9. Utilisation du spectre : Le RLBSP utilisera le spectre de manière efficace.

Options de prestation de services

Innovation, Sciences et Développement économique Canada (ISDE) a alloué 20 MHz de la bande de 700 MHz à des fins de sécurité publique (ci-après la « bande 14 »). Le BTCN recommande que le spectre alloué soit utilisé dans un réseau partagé à des fins commerciales et des fins de sécurité publique, ce type de réseau permettant les deux types d'utilisations susmentionnées et offrant un accès prioritaire et des droits de préemption aux utilisateurs de la sécurité publique, en cas de nécessité. Il est assumé que le trafic de la sécurité publique et le trafic commercial qui passent par le spectre de la bande 14 seront dirigés vers leurs réseaux centraux respectifs. Ceci aura pour effet de dissiper les inquiétudes en matière de sécurité et de confidentialité pour ce qui est d'assurer la protection et la sécurité des données et des informations qui sont transportées par l'entremise du réseau. Un réseau partagé à des fins commerciales et des fins de sécurité publique garantit l'usage efficace du spectre, car celui-ci permet l'utilisation commerciale de la capacité excédentaire du spectre, tout en offrant des mécanismes d'accès prioritaire et des droits de préemption aux utilisateurs de la sécurité publique. Une telle approche respecte par ailleurs l'esprit de la *Loi sur la radiodiffusion* et de la *Loi sur les télécommunications*.

Le RLBSP pourrait être exploité de plusieurs différentes façons, chaque approche possible étant associée à un ensemble d'acteurs, à une distribution des fonctions, à des risques et à des possibilités qui lui sont propres. Ainsi, le BTCN envisage quatre approches de prestation de services pour le RLBSP du Canada. Ces approches sont de nature notionnelle, l'objectif n'étant pas de déterminer l'approche de prestation de services ou le cadre de gouvernance du RLBSP que l'on adoptera au bout du compte. À la lumière de l'évaluation fondée sur les principes du RLBSP, le déploiement d'un unique réseau de sécurité publique, par un seul opérateur de réseau mobile (ORM, communément appelé en anglais « mobile

network operator » ou « MNO ») ou un groupe d'ORM qui travaillent de concert et de manière coordonnée, représente la solution qui offre la plus forte probabilité de succès. On évaluera de façon plus approfondie la faisabilité de ces approches en fonction des cadres de gouvernance potentiels et en rendra compte dans le document de politique.

Reconnaissant le risque que pose le statu quo pour l'interopérabilité des communications, le BTCN s'engage à continuer d'assumer un rôle de leadership afin de garantir la mise en œuvre d'un RLBSP national et interopérable au Canada.

Prochaines étapes

Le BTCN poursuivra ses efforts en vue d'élaborer un document de politique exhaustif qu'il soumettra aux ministres fédéral-provinciaux-territoriaux (FPT) responsables de la gestion des urgences. Ce document de politique se penchera sur les lacunes en matière d'analyse, y compris les options de gouvernance, traitera des présentes recommandations et constatations de façon plus détaillée et proposera une marche à suivre pour la mise en œuvre d'un RLBSP au Canada qui permettra la meilleure application possible des principes qui le régissent, tout en conciliant les différents intérêts des intervenants.

Rapport d’étape sur le Réseau à large bande de sécurité publique

Objet

L’objet du présent rapport d’étape est de permettre au Bureau temporaire de coordination nationale (BTCN) de partager de l’information avec les intervenants à l’égard des progrès accomplis à ce jour pour mettre en place un réseau à large bande de sécurité publique (RLBSP) au Canada. Celui-ci présente les conclusions et les recommandations formulées jusqu’à maintenant à propos des options et des exigences applicables au RLBSP du Canada, tout en relevant les lacunes au chapitre de la recherche et en présentant une feuille de route.

Ce rapport d’étape se veut un document de référence. Le BTCN a pour intention de veiller à ce que l’approche recommandée pour le RLBSP du Canada réponde aux besoins de la communauté de la sécurité publique, qu’elle soit viable à long terme et qu’elle convienne à tous les intervenants. Il convient également de noter que toutes les recommandations ci-incluses pourraient évoluer et être peaufinées alors que le BTCN poursuit son travail et continue de mobiliser les intervenants.

Il est tout aussi important de préciser les éléments qui ne relèvent pas du mandat actuel du BTCN et qui conséquemment ne feront pas l’objet du présent rapport d’étape, dont les applications et l’architecture du réseau; les coûts et la mise en œuvre; l’élaboration d’exigences techniques détaillées; et l’écosystème connexe de communications en matière de sécurité publique.

Le BTCN reconnaît que les lecteurs du présent document posséderont différents degrés de connaissance au sujet des communications d’urgence et des RLBSP. On s’est donc consciemment efforcés d’employer un langage non technique et d’inclure au rapport un glossaire et une liste d’acronymes.

Le document de politique que soumettra le BTCN comprendra des recommandations qui soutiennent l'établissement d'un RLBSP au Canada et qui s'appuient sur le portrait global que l'on a dégagé des discussions et des activités menées auprès des intervenants, des experts du terrain et de la communauté d'utilisateurs. Le document de politique sera présenté au début de 2020 aux ministres fédéral-provinciaux-territoriaux (FPT) responsables de la gestion des urgences. On partagera aussi le document de politique avec Innovation, Sciences et Développement économique Canada (ISDE) en guise complément au document de décisions qu'il a publié en juin 2017. Le document de politique offrira des renseignements utiles sur la manière dont le RLBSP pourrait être mis en œuvre au Canada.

Contexte et historique

Chaque jour, les Canadiens comptent sur les premiers intervenants et le personnel de sécurité publique pour intervenir avec rapidité et efficacité en cas d'incidents communs et de situations d'urgence. Les premiers intervenants et le personnel de sécurité publique sont responsables de la protection et de la sécurité de plus de 36 millions de Canadiens d'un bout à l'autre du pays. Outre la question de l'utilisation quotidienne, il convient de noter que pour intervenir efficacement dans le cadre de catastrophes majeures, d'urgences et d'événements prévus, on doit disposer de capacités de communication de phonie et de données qui sont fiables et interopérables entre les administrations et les divers intervenants d'urgence. Dans certains cas, ces incidents et événements exigent même que l'on obtienne le soutien de partenaires internationaux. Aucun ordre de gouvernement ne possède un organisme doté de la capacité et de l'expertise nécessaires pour intervenir unilatéralement lors de tels incidents[1]. Or, la population s'attend à ce que les efforts de coordination requis soient menés conjointement par tous les organes gouvernementaux pertinents en vue d'assurer la sécurité des Canadiens, y compris celles de la communauté de la sécurité publique, ainsi que la protection des biens.

Pour bien comprendre les avantages et la nécessité d'un RLBSP, il est important d'envisager l'évolution des communications et de leur utilisation au cours des dernières décennies, tant à des fins commerciales qu'à des fins de sécurité publique.

Évolution des communications dans la sphère commerciale

Dans le secteur commercial, de nouvelles technologies font régulièrement leur apparition sur le marché et, au fil du temps, les consommateurs adoptent généralement les technologies éprouvées dont les prix diminuent. Avant le 20e siècle, le principal mode de communication était le réseau téléphonique commuté public (RTCP). Ce système permettait une transmission audio bidirectionnelle entre les utilisateurs, et pendant plus de cent ans, cette technologie s'est appliquée uniquement aux informations vocales. Toutefois, entre 1965 et 1975, les bases nécessaires à l'Internet moderne ont été

[1] Sécurité publique Canada. Janvier 2011. Stratégie d'interopérabilité des communications pour le Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntrprblt-strtg/ntrprblt-strtg-fra.pdf.

jetées[2]. On compte parmi ces efforts la création des modems : des dispositifs qui sont capables d'utiliser des tonalités audio pour établir une connexion entre des ordinateurs situés à différents endroits physiques, et ce, au moyen du RTCP. Entre le milieu des années 1980 et le milieu des années 1990, le World Wide Web et les premiers fournisseurs de services Internet ont vu le jour. En 1992, on diffusait des données audio et vidéo sur Internet pour la première fois et en 1993, on comptait au total 600 sites Internet dans le monde!

Au tournant du siècle, on a mis au point de nouvelles technologies qui permettaient d'assurer une connectivité à large bande[3]. Celles-ci offraient par ailleurs un débit binaire beaucoup plus élevé et permettaient désormais d'établir des connexions Internet sans passer par le RTCP, ainsi que d'utiliser les réseaux de câbles modernes et les nouveaux réseaux sans fil pour accéder à Internet et au World Wide Web. La connectivité à large bande est responsable de la croissance explosive d'Internet, ainsi que des progrès spectaculaires réalisés sur le plan de la quantité de données (y compris l'information vidéo et audio de grande qualité), que les gens de partout dans le monde peuvent partager presque instantanément.

Parallèlement aux progrès relatifs à Internet et au RTCP, les communications sans fil connaissaient aussi une révolution. Bien que les premiers essais de téléphonie mobile fussent réalisés entre 1918 et 1924, ce n'est qu'à la fin des années 1970 que les véritables réseaux sans fil « commerciaux » ont commencé à s'implanter[4]. Comme dans le cas du RTCP, la principale utilisation des réseaux mobiles à leur origine était la téléphonie. Avec l'apparition de la connectivité à large bande, les réseaux sans fil mobiles ont rapidement migré vers un environnement qui était bien adapté pour permettre l'accès à Internet et au World Wide Web. Le premier service Internet accessible depuis un appareil sans fil a vu le jour en 1999 au Japon et, depuis ce temps, l'évolution rapide des technologies a eu pour effet d'accroître la vitesse des réseaux mobiles de manière spectaculaire, en faisant ainsi le moyen idéal pour accéder à Internet de façon mobile. Les services mobiles sans fil sont maintenant si répandus que certaines régions ont maintenant accès à Internet exclusivement par l'entremise des réseaux cellulaires, plutôt que de dépendre du RTCP ou des réseaux câblés traditionnels.

[2] Consulter le lien https://www.livescience.com/20727-internet-history.html pour obtenir un portrait général de l'histoire d'Internet (dernière consultation le 21 mars 2019).
[3] Pour obtenir de plus amples renseignements, consulter le lien https://www.uswitch.com/broadband/guides/broadband_history/ (dernière consultation le 21 mars 2019) et le lien https://fr.wikipedia.org/wiki/Acc%C3%A8s_%C3%A0_Internet (dernière consultation le 21 mars 2019).
[4] Pour consulter la ligne du temps globale de l'évolution des communications sans fil mobiles, voir le lien https://www.timetoast.com/timelines/history-of-mobile-phones-7e561d96-e442-4495-9d71-3d0789eaaab4 (dernière consultation le 21 mars 2019).

Évolution des communications dans la sphère de la sécurité publique

Pour ce qui est des communications en matière de sécurité publique, l'évolution des technologies a suivi une trajectoire légèrement différente. Encore aujourd'hui, ce domaine s'appuie sur des technologies différentes de celles utilisées dans le secteur commercial. Cela pourrait notamment s'expliquer par le degré de fiabilité et de sécurité perçu des services commerciaux[5]. Cette divergence a cependant empêché de doter les premiers intervenants de capacités à la fine pointe de la technologie.

Les communications entre premiers intervenants se font généralement par l'entremise d'appareils radio portatifs et de radios pour véhicules. Ainsi, les services de police ont intégré des systèmes de communications radio bidirectionnelles à leurs voitures de patrouille dès les années 1930[6]. Comme c'est le cas pour d'autres technologies, on se concentrait alors sur les communications vocales. Au cours des décennies suivantes, l'utilisation des appareils radio portatifs n'a pas beaucoup changé, bien que leur emploi se soit étendu à tous les domaines de premières interventions, comme ceux des pompiers et des ambulanciers paramédicaux. La principale ressource nécessaire aux radios mobiles est le spectre des radiofréquences. L'un des désavantages de cette technologie, qui était particulièrement présent au tout début, est l'utilisation sous-optimale de ce spectre, les transmissions radio entre utilisateurs étant susceptibles d'accaparer les ressources et donc de donner lieu à des situations où les autres utilisateurs sont incapables de transmettre ou de recevoir de l'information. Toutefois, l'une des principales caractéristiques des radios mobiles terrestres (RMT) réside dans leur capacité à assurer des services de phonie largement accessibles. Ces derniers permettent à deux utilisateurs de communiquer entre eux ou à un utilisateur de communiquer avec plusieurs autres personnes sans être directement connecté à l'infrastructure (c.-à-d. les stations de base radio ne sont pas forcément requis).

Au fil du temps, les réseaux de RMT soutenant les services de phonie essentiels à la mission ont évolué de manière à utiliser plus efficacement le spectre (bien que loin d'être aussi efficaces que les réseaux cellulaires) en passant de la transmission analogique à la transmission numérique. De plus, dans le cadre de certaines initiatives, comme le Project 25 (P25) en Amérique du Nord, on a commencé à utiliser des fonctions de sécurité accrue (p. ex. le chiffrement numérique), ainsi que les services de transmission de données à bande passante étroite (p. ex. les simples messages textes)[7]. Bien qu'à la lumière de ces progrès, les systèmes de RMT soient demeurés pertinents et essentiels pour les premiers intervenants, leurs désavantages ont amené plusieurs d'entre eux à se tourner vers les services cellulaires commerciaux, ceux-ci leur permettant d'utiliser des services de transmission de données à large bande passante en guise de complément à leurs services de phonie essentiels à la mission. Cela dit, ces offres commerciales ne présentent pas le

[5] Séances de mobilisation des intervenants organisées par l'équipe de travail fédérale sur le RLBSP, octobre 2017 à mars 2018.
[6] Pour obtenir un aperçu de l'utilisation des radios bidirectionnelles par les premiers intervenants, voir le lien http://blog.techwholesale.com/2015/11/07/police-and-emergency-responders-two-way-radios/ (dernière consultation le 21 mars 2019).
[7] Pour obtenir de plus amples renseignements sur le P25, voir le lien http://www.project25.org/index.php/technology/p25-history (dernière consultation le 21 mars 2019).

même degré de fiabilité et la même garantie d'accès que les systèmes de RMT, et ne possèdent pas certaines de leurs fonctions de sécurité.

Capacités de liaison des communications commerciales et des communications en matière de sécurité publique

Suivant la mise en œuvre du RLBSP, les premiers intervenants auront le meilleur des deux mondes. Le RLBSP fournira aux utilisateurs une expérience semblable à celle qu'offre la technologie cellulaire actuelle pour appareils portatifs et véhicules, mais il possédera un degré accru de fonctionnalité, de sécurité, de fiabilité et de garantie d'accès qui se rapproche davantage de ce que proposent les systèmes traditionnels de RMT. Les deux systèmes seront probablement exploités de façon conjointe pendant plusieurs années, jusqu'à ce que le degré de fiabilité des services offerts par l'entremise des réseaux mobiles à large bande soit le même que celui des réseaux de RMT. D'ici là, la majorité des intervenants de la sécurité publique porteront sur eux en tout temps un combiné de RMT et un téléphone cellulaire.

Qu'est-ce qu'un RLBSP?

Aujourd'hui, les nouvelles technologies permettent d'améliorer la sûreté et la sécurité des Canadiens et du personnel de sécurité publique, car elles ont pour effet de renforcer les capacités en matière de communications, ainsi que la coordination et les interventions des premiers intervenants et des gouvernements. Le déploiement d'un RLBSP national et interopérable représente l'une de ces utilisations technologiques. Un RLBSP consiste en un réseau sécurisé de communication de données, à haute vitesse et sans-fil, que peuvent utiliser les premiers intervenants et les membres du personnel de la sécurité publique pour communiquer entre eux et obtenir de l'information lors de situations d'urgence et d'événements prévus, et dans l'exercice de leurs fonctions au quotidien. Bien qu'il puisse s'appuyer sur l'infrastructure des opérateurs de réseau mobile (ORM), le RLBSP demeure un réseau distinct et séparé qui est spécialement conçu pour répondre aux besoins particuliers des intervenants.

Le RLBSP sera un élément clé du vaste écosystème de communications en matière de sécurité publique. En tant que pilier de l'écosystème, le réseau sera mis à profit de manière à soutenir un large éventail de systèmes, d'applications et de services de la sécurité publique. Il renforcera l'efficacité et la sécurité des premiers intervenants et de la communauté de la sécurité publique en prenant en charge plusieurs fonctionnalités de communication sans fil qui permettent d'améliorer la coordination, les interventions et la connaissance de la situation.

Les réseaux commerciaux actuels, bien qu'ils offrent des services mobiles, pourraient ne pas répondre aux normes en matière de sécurité, de fiabilité et de qualité de service qui sont attendues de la part des utilisateurs potentiels du RLBSP. Le réseau se distinguera des services commerciaux actuellement offerts du fait qu'il permettra le développement et l'utilisation d'applications riches en informations, lesquelles soutiendront les intervenants dans la prestation de leurs

services et n'existent toujours pas au Canada. Le RLBSP consistera principalement en une couche sécurisée de l'infrastructure actuelle et permettra la prestation d'un éventail de services mobiles à large bande aux utilisateurs de la sécurité publique. Il convient aussi de noter que les utilisateurs pourraient comprendre autant des machines autonomes que des personnes. À titre d'exemple : l'utilisation d'appareils et de détecteurs dépendant de l'Internet des objets (IdO) et de l'Internet des objets pour sauver des vies (IdOSdV) pour communiquer et partager de l'information par l'entremise du RLBSP. Ces appareils pourraient notamment comprendre des caméras, des alarmes et différents capteurs environnementaux. La transition vers les « villes intelligentes » amènera chacune de nos collectivités à utiliser des milliers d'appareils du genre[8]. Cette tendance fournit une raison supplémentaire de veiller à ce qu'une infrastructure soit mise en place pour soutenir la transmission sécuritaire et fiable de données au sein des réseaux qui ne sont pas exclusivement destinés aux utilisateurs commerciaux.

Un RLBSP diffère d'un service prioritaire sans fil, soit un service de phonie fondé sur un abonnement qui permet d'octroyer au personnel essentiel un accès au prochain canal radio sans fil qui est accessible, tout en réduisant l'incidence sur l'accès des consommateurs à cette même infrastructure sans fil[9].

Le carré marron de la *figure 1* regroupe les éléments qui sont considérés comme des parties intégrantes d'un RLBSP. Les autres éléments qui apparaissent dans le carré blanc de la figure représentent les réseaux, les systèmes, les services et les applications externes que le RLBSP prendrait en charge. Ce diagramme est tiré du rapport « Description de l'architecture du RLBSP » du Centre des sciences pour la sécurité de Recherche et développement pour la défense Canada (CSS de RDDC)[10]. Ce rapport décrit d'un point de vue technique la manière dont le RLBSP interagirait avec plusieurs de ces composantes externes.

[8] Pour consulter un article bref sur les villes intelligentes et l'Internet des objets, voir la page https://www.information-age.com/smart-city-technology-123473905/ (dernière consultation le 21 mars 2019).
[9] Gouvernement du Canada. Août 2011. Service prioritaire sans fil (SPSF). http://www.ic.gc.ca/eic/site/et-tdu.nsf/fra/h_wj00016.html
[10] FOURNIER, J., C. LUCENTE, D. SKIDMORE et L. SAMSON. Description de l'architecture du RLBSP. Rapport scientifique. Janvier 2019. DRDC-RDDC-2018-R236.

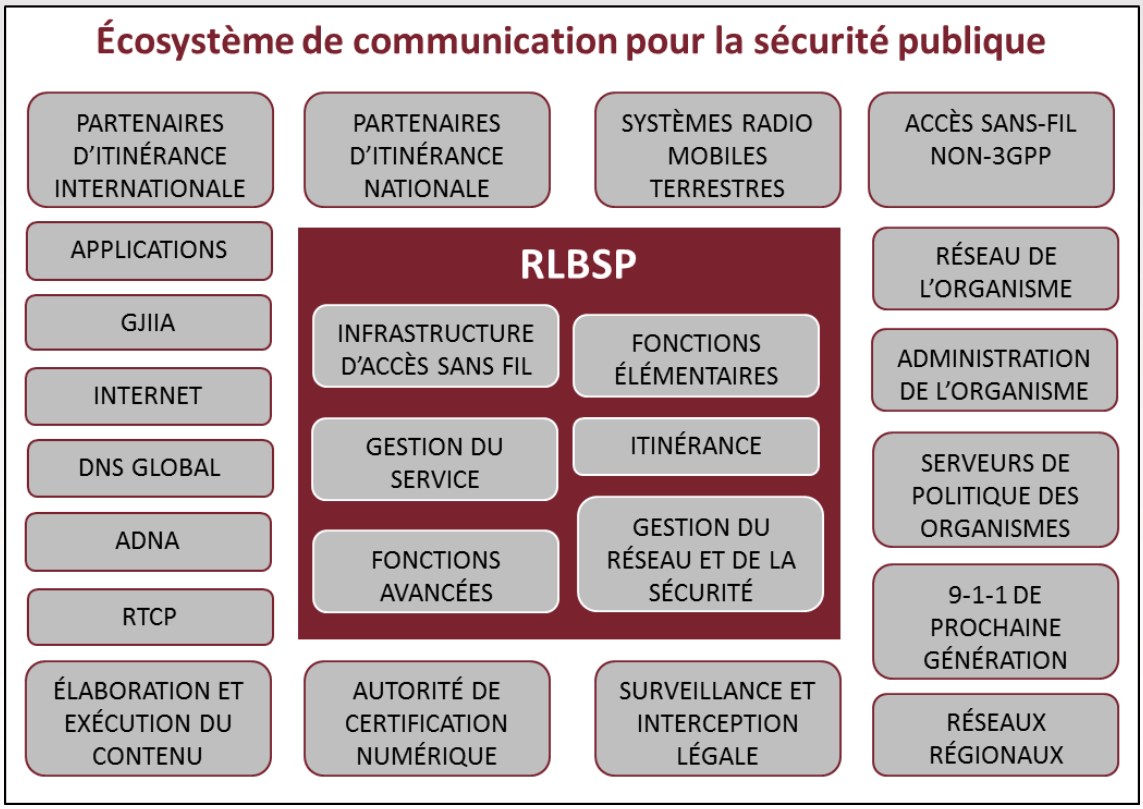

Figure 1 - Écosystèmes des communications en matière de sécurité publique (source : Description de l'architecture du RLBSP)

À l'examen de la *figure 1*, nous constatons que le RLBSP comprend les composantes de base nécessaires pour offrir un service mobile sans fil à large bande. Celui-ci compte notamment l'infrastructure, les fonctions de base, les fonctions améliorées, la gestion de service (p. ex. la gestion des abonnés, la facturation, etc.), ainsi que l'itinérance et la gestion du réseau et de la sécurité. Les systèmes et les données d'organismes ne font PAS partie du RLBSP actuel. Le RLBSP est plutôt l'intermédiaire par l'entremise duquel ses utilisateurs peuvent accéder aux données de leurs organismes respectifs, pourvu qu'ils disposent d'une autorisation d'accès. À ce chapitre, le RLBSP offre aux organismes de sécurité publique un environnement et un outil habilitant pour utiliser de nouvelles applications et services et interagir les uns avec les autres.

Pourquoi le Canada a-t-il besoin d'un RLBSP?

Les Canadiens dépendent de plus en plus des services sans fil dans leur quotidien, notamment pour demeurer en contact avec leur famille, consommer du contenu en ligne ou travailler pendant des déplacements. La consommation de données continue d'augmenter, et il s'agit d'une augmentation qui se poursuivra dans un avenir prévisible en raison de l'arrivée de la cinquième génération (5G), de l'augmentation du nombre d'utilisateurs, de la demande des applications destinées à

large bande, des types d'appareils, des villes intelligentes et de l'expansion de l'IdO[11]. Les premiers intervenants et le personnel de sécurité publique jouent un rôle crucial dans la protection des Canadiens au quotidien et ils devraient disposer de la meilleure technologie disponible pour renforcer et améliorer leurs interventions.

Actuellement, les premiers intervenants et le personnel de sécurité publique du Canada s'appuient principalement sur les systèmes de RMT et utilisent des appareils radio portatifs et des radios pour véhicules pour communiquer dans le cadre d'activités quotidiennes et d'opérations d'urgence. De nombreux systèmes de RMT du Canada utilisent un spectre à bande étroite, la majorité d'entre eux se limitant aux communications vocales, alors que certains peuvent prendre en charge des applications à faible consommation de données. Les systèmes de RMT ne sont pas capables de transmettre les volumes importants de données dont ont de plus en plus besoin les premiers intervenants pour répondre aux demandes actuelles et futures.

De plus, au fil du temps, ces systèmes de RMT ont évolué aux échelles municipales et provinciales et ont par la suite été déployés sans que l'on tienne compte des exigences d'interopérabilité nationale. Mis à part quelques exceptions provinciales et régionales, il en résulte une fragmentation importante à différentes échelles au Canada. Au point de vue national, et au sein des mêmes territoires de compétences, les organismes de sécurité publique qui utilisent divers systèmes dans différentes parties du spectre radio ne sont pas en mesure de communiquer entre eux, à moins de partager des appareils. Cela a pour effet de créer des silos de communication qui ne sont pas interopérables. Conséquemment, dans certains territoires de compétences, les rapports d'exercice et les rapports après action font état de difficultés considérables au chapitre des systèmes de communications non interopérables. Dans la région de la capitale nationale (RCN), par exemple, les organismes d'application de la loi, le personnel des trois services, et les services de transports de multiples ordres de compétence mènent tous leurs activités au sein de la cité parlementaire et de la RCN sans disposer de systèmes de communication pleinement interopérables.

Un RLBSP servirait de technologie complémentaire aux systèmes de RMT à moyen terme (10 à 15 ans[12]), ce qui permettrait la prise en charge d'un nombre accru d'applications à haute consommation de données et de communications vocales interopérables nationales. L'objectif ultime étant de veiller au développement du RLBSP afin d'en faire un réseau mature qui sera la principale plateforme de communication des intervenants.

Actuellement, les premiers intervenants se servent des réseaux commerciaux pour combler leurs besoins en matière de données mobiles. Les organismes qui utilisent présentement les réseaux mobiles commerciaux configurent leurs systèmes de sorte que seuls leurs membres puissent y accéder, ou ils configurent des applications qui restreignent l'accès aux

[11] Voir le lien https://crtc.gc.ca/fra/publications/reports/policymonitoring/2018/index.htm (dernière consultation le 9 avril 2019)
[12] Lignes directrices approuvées par les ministres FPT responsables de la gestion des urgences. Mai 2018

utilisateurs autorisés. Les organismes se sont donc isolés dans des silos virtuels. De plus, les réseaux commerciaux ne sont pas forcément conçus pour répondre aux besoins de la sécurité publique. À titre d'exemple, les fournisseurs commerciaux augmentent couramment leur couverture lors des périodes prévues de congestion des réseaux, comme les événements sportifs ou les concerts. Cela dit, les périodes imprévues de congestion des réseaux sans fil lors d'événements inopinés peuvent entraîner une dégradation des services et donc compromettre les capacités de communication des intervenants lors de moments critiques. Ainsi, les systèmes commerciaux actuels pourraient avoir de la difficulté à soutenir la transmission de données à large bande pour les applications existantes et émergentes dont ont besoin les utilisateurs du RLBSP. Cette incapacité des utilisateurs de la sécurité publique à communiquer efficacement, en particulier entre les administrations, les disciplines et les ordres de gouvernement, représente une menace pour la sûreté et la sécurité des premiers intervenants et des Canadiens[13].

Le RLBSP soutiendra la création d'un écosystème d'applications de la sécurité publique qui permettra de répondre à ce problème de non-interopérabilité. Le RLBSP vise à démanteler les silos de communication de données du point de vue de la technologie en offrant un réseau sécurisé hautement accessible à tous les premiers intervenants et le personnel de la sécurité publique du Canada. Bien qu'il puisse exploiter l'infrastructure de plusieurs réseaux mobiles, il s'agira d'un réseau unique, de sorte que l'on puisse satisfaire le plus efficacement possible aux exigences des intervenants et satisfaire les principes du RLBSP décrit plus tard dans ce rapport.

Un RLBSP soutiendrait les objectifs de la *Stratégie d'interopérabilité des communications pour le Canada (SICC)* qui, par l'entremise de son plan d'action, vise à renforcer et à améliorer l'interopérabilité des communications vocales et de la transmission de données[14]. L'ensemble des ordres de gouvernement et des associations d'intervenants d'urgence ont appuyé la SICC en janvier 2011, ainsi que son plan d'action en mars 2013.

Le RLBSP offrira aux intervenants novateurs qui sont disposés à l'utiliser un mécanisme pour interagir entre eux et partager de l'information dans l'intérêt public. À elle seule, la mise en place du RLBSP ne permettra pas l'avancement des cinq piliers du Continuum canadien d'interopérabilité des communications trouvé dans le SICC. Il faudra donc assurer un degré élevé de leadership, de planification et de collaboration[15].

D'autres initiatives de communications en matière de sécurité publique, comme les services 9-1-1 de prochaine génération (services 9-1-1 de PG) et le Système national d'alertes au public (SNAP), servent de compléments au RLBSP.

---

[13] Sécurité publique Canada. Janvier 2011. Stratégie d'interopérabilité des communications pour le Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntrprblt-strtg/ntrprblt-strtg-fra.pdf
[14] Ibidem
[15] Sécurité publique Canada. Janvier 2011. Continuum canadien d'interopérabilité des communications. https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntrprblt-strtg/ntrprblt-strtg-ann1-fra.jpg

Ces deux initiatives ont pour objet d'améliorer la gestion et les communications lors des situations d'urgence dans l'ensemble du pays.

En juin 2017, le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) a exigé que tous les fournisseurs de services téléphoniques et mobiles mettent leurs réseaux à jour, de sorte qu'ils soient prêts à offrir des services de phonie et de messagerie texte 9-1-1 de PG d'ici juin et décembre 2020, respectivement. Suivant la mise en œuvre des services 9-1-1 de PG, les Canadiens pourraient ultimement diffuser en continu des images vidéo d'un incident, envoyer des photos des dommages causés par un accident ou d'un suspect en fuite, ou envoyer des renseignements médicaux personnels, notamment en ce qui concerne les besoins en matière d'accessibilité, ce qui pourrait grandement faciliter les interventions d'urgence[16]. Le SNAP, aussi connu sous le nom « En alerte », fournit aux organismes de gestion des urgences de partout au pays la capacité d'alerte normalisée de transmettre des messages d'urgence susceptibles de sauver des vies directement à la télévision, à la radio et aux appareils mobiles compatibles (p. ex. les téléphones intelligents LTE). Le système « En alerte » a la capacité d'avertir rapidement les Canadiens des risques imminents ou actuels qui mettent leur vie ou des biens en danger, comme les incendies; les catastrophes naturelles; les incidents biologiques, dangereux, environnementaux, terroristes et civils; et les alertes Amber. Ces capacités pourraient générer une quantité importante de données devant être transmises aux intervenants par l'entremise du RLBSP.

Un RLBSP pourrait également améliorer la préparation aux incidents, les interventions menées dans le cadre de ces derniers et le rétablissement qui s'ensuit. À titre d'exemple, en cas de tornade d'envergure, un RLBSP pourrait permettre à un ensemble d'outils de cartographie et de notification de transmettre des alertes, des avertissements et des messages aux organismes de sécurité publique en vue d'assurer l'efficacité de leur processus décisionnel. Cette capacité soutient la quatrième priorité de la *Stratégie de sécurité civile pour le Canada : Vers un 2030 marqué par la résilience*, laquelle a été appuyée par les ministres FPT responsables de la gestion des urgences. La quatrième priorité de la stratégie vise à améliorer les capacités et la coordination en matière d'intervention en cas de catastrophes et à stimuler le développement de nouvelles capacités en encourageant les gouvernements FPT à travailler de concert avec leurs partenaires en gestion des urgences à l'élaboration de systèmes de communication interopérables en matière de sécurité publique[17].

De plus, par l'entremise d'un cas pratique (un incendie de végétation simulé en milieu périurbain), on a démontré qu'un RLBSP avait la « capacité d'offrir des services de communication à large bande de manière intelligente aux premiers intervenants, et ce, lors de conditions difficiles dans lesquelles d'autres systèmes se fondant sur une technologie

[16] Conseil de la radiodiffusion et des télécommunications canadiennes. Juin 2017. Le CRTC crée un environnement plus sûr pour les Canadiens en favorisant l'accès à des services 9-1-1 améliorés et novateurs. https://www.canada.ca/fr/radiodiffusion-telecommunications/nouvelles/2017/06/le_crtc_cree_un_environnementplussurpourlescanadiensenfavorisant.html
[17] Sécurité publique Canada. Janvier 2019. Stratégie de sécurité civile pour la Canada : Vers un 2030 marqué par la résilience. https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/mrgncy-mngmnt-strtgy/index-fr.aspx

semblable ne seraient pas en mesure d'en faire autant » [traduction][18]. Dans le cadre de ce cas pratique, le RLBSP offrait une meilleure connaissance de la situation, ce qui a permis d'améliorer les interventions, de réduire le nombre de victimes, et d'accroître l'efficacité des ressources humaines et matérielles.

Allocation de spectre dans la bande de 700 MHz aux fins de la sécurité publique

Les activités d'allocation de spectre menées récemment ont donné lieu à la création d'un canal qui permet l'utilisation, à des fins de communication en matière de sécurité publique, de 20 MHz de spectre dans la bande de 700 MHz (ci-après la « bande 14 », appelée au Canada le « spectre à large bande destiné à la sécurité publique dans la bande de 700 MHz »[19]). En mars 2012, ISDE (alors Industrie Canada) a octroyé un bloc de 5+5 MHz du précieux spectre de la bande de 700 MHz aux communications à large bande en matière de sécurité publique[20]. Des consultations stratégiques ont par la suite été menées en vue de recueillir des commentaires sur la désignation de l'utilisation du spectre de 5+5 MHz, appelé le bloc D. Dans son budget de 2015, le gouvernement du Canada a annoncé que ces 10 MHz supplémentaires du spectre de 700 MHz seraient aussi consacrés à l'utilisation de la large bande de la sécurité publique[21]. Le gouvernement a également alloué la somme de 3 millions de dollars sur deux ans, à compter de 2016-2017, à la prise de mesures initiales pour mettre sur pied un RLBSP.

En juin 2017, ISDE a publié un avis de décision qui confirmait l'allocation de 20 MHz du spectre de 700 MHz à l'utilisation de la large bande pour la sécurité publique[22]. L'avis de décision confirmait par ailleurs les points suivants :

- Le spectre dans ces bandes ne sera pas mis aux enchères;
- L'utilisation commerciale de la capacité inutilisée sera permise pourvu que les utilisateurs de la sécurité publique aient la priorité et des droits de préemption sur toute forme d'utilisation commerciale;

[18] FOURNIER, J. et C. LUCENTE. Public safety broadband network use-case—wildland-urban interface fire. Recherche et développement pour la défense Canada. Rapport scientifique. 2017. DRDC-RDDC-2017-R116.
[19] Innovation, Sciences et Développement économique Canada. Juin 2017. Décisions se rapportant au cadre politique, technique et de délivrance de licences pour l'utilisation du spectre à large bande destiné à la sécurité publique, et ce, dans les bandes de 758 à 763 MHz et de 788 à 793 MHz (bloc D), ainsi que de 763 à 768 MHz et de 793 à 798 MHz (bloc SPLB). http://www.ic.gc.ca/eic/site/smt-gst.nsf/fra/sf11289.html
[20] Innovation, Sciences et Développement économique Canada. Août 2012. Consultation sur un cadre politique, technique et de délivrance de licences pour l'utilisation du spectre à large bande de la sécurité publique dans les bandes 758-763 MHz et 788-793 MHz (bloc D) et 763-768 MHz et 793-798 MHz (bloc SPLB). http://www.ic.gc.ca/eic/site/smt-gst.nsf/fra/sf10459.html
[21] Gouvernement du Canada. Avril 2015. Le budget de 2015. https://www.budget.gc.ca/2015/docs/plan/toc-tdm-fra.html
[22] Innovation, Sciences et Développement économique Canada. Juin 2017. Décisions se rapportant au cadre politique, technique et de délivrance de licences pour l'utilisation du spectre à large bande destiné à la sécurité publique, et ce, dans les bandes de 758 à 763 MHz et de 788 à 793 MHz (bloc D), ainsi que de 763 à 768 MHz et de 793 à 798 MHz (bloc SPLB). http://www.ic.gc.ca/eic/site/smt-gst.nsf/fra/sf11289.html

- Des licences de spectre seront attribuées directement à une entité du réseau de sécurité publique ou à plusieurs d'entre elles;

- Aucune technologie particulière ne sera imposée, mais toute technologie utilisant ce spectre doit assurer une interopérabilité nationale et transfrontalière et garantir une capacité de priorité et de préemption pour les services de sécurité publique.

Suivant cette confirmation, en tant que membre de l'équipe de travail fédérale sur le RLBSP, ISDE a soumis une demande de renseignements en novembre 2017 en vue de recueillir les points de vue des industries des technologies de l'information et des communications et des télécommunications sur les sujets suivants : modèle opérationnel viable; modèle de gouvernance; et écosystème des applications, des services et des appareils en vue d'orienter l'approche du gouvernement du Canada à l'égard d'un RLBSP au Canada[23]. Dans le cadre de sa collaboration avec ISDE, le BTCN a examiné les réponses soumises par les intervenants de l'industrie des télécommunications. Ces réponses ont permis de mieux comprendre les perspectives et les positions de l'industrie, et d'orienter le développement d'un RLBSP pour le Canada[24].

Bureau temporaire de coordination nationale

En mai 2018, les ministres FPT responsables de la gestion des urgences ont tous reconnu les avantages d'un RLBSP et appuyé la mise sur pied d'un Bureau temporaire de coordination nationale (BTCN)[25] qui serait responsable de faire progresser les efforts pour mettre en place un réseau sans fil de communication de données sécurisé et interopérable[26]. Les ministres FPT ont également appuyé un ensemble de principes directeurs pour la mise en œuvre du RLBSP qu'ont élaboré conjointement les fonctionnaires FPT, les municipalités et les trois services :

- Le déploiement d'un RLBSP s'appuierait sur les pratiques exemplaires et les leçons tirées des projets pilotes et des essais;

- Les calendriers de déploiement ne seraient pas identiques dans l'ensemble du Canada, car ils seront adaptés aux priorités et aux capacités de chaque administration;

- Les réseaux de radiocommunication mobiles terrestres (RMT) coexisteraient probablement avec le RLBSP à moyen terme (10 à 15 ans);

[23] Innovation, Sciences et Développement économique Canada. 2017. Réseau à large bande de sécurité publique – Demande de renseignements.
[24] Gartner. 28 mai 2018. RLBSP – Examen de la demande de renseignements.
[25] Sécurité publique Canada. Février 2019. Bureau temporaire de coordination nationale. https://www.securitepublique.gc.ca/cnt/mrgnc-mngmnt/tnco-fr.aspx
[26] Secrétariat des conférences intergouvernementales canadiennes. Mai 2018. COMMUNIQUÉ – Réunion des ministres fédéral, provinciaux et territoriaux sécurité civile. http://www.scics.ca/fr/product-produit/communique-rencontre-des-ministres-federal-provinciaux-et-territoriaux-securite-civile/

- À court terme, l'objectif du RLBSP serait de fournir des services de communication de données sans fil sécurisés et interopérables;
- Autant que possible, on exploiterait l'infrastructure sans fil actuelle afin de réduire les coûts;
- Il faudrait établir des liens avec d'autres initiatives de communications en matière de sécurité publique (par ex. SNAP et les services 9-1-1 de PG) et des mécanismes de gouvernance;
- Les problèmes de couverture et de capacité devraient être traités au moyen de programmes de financement de tous les ordres de gouvernement.

À la lumière de ces principes directeurs, le mandat du BTCN est d'offrir une perspective stratégique consolidée à l'égard du cadre, ainsi que des considérations sur les exigences techniques, la gouvernance et les modèles opérationnels du futur RLBSP du Canada. Le BTCN a pour objectif de présenter un document de politique aux ministres FPT responsables de la gestion des urgences au début de 2020, lequel traitera des questions soumises par ISDE dans leur décision de juin 2017 au sujet de la désignation du spectre de l'utilisation de la large bande de la sécurité publique.

Le BTCN reconnaît que la mise en œuvre d'un RLBSP au Canada commandera une étroite collaboration entre les gouvernements, l'industrie et les utilisateurs finaux du réseau. Conséquemment, le bureau réunit des représentants des administrations, des associations et des ministères ci-dessous (par ordre alphabétique).

Composition du Bureau temporaire de coordination nationale

Fédéral	Provincial et territorial	Non gouvernemental
Agence des services frontaliers du Canada	Gouvernement de l'Alberta	Association canadienne des chefs de police
Centre des sciences pour la sécurité de Recherche et développement pour la défense Canada	Gouvernement de l'Ontario	Association canadienne des chefs de pompiers
Gendarmerie royale du Canada	Gouvernement de la Colombie-Britannique	Chefs paramédics du Canada
Innovation, Sciences et Développement économique Canada	Gouvernement de la Nouvelle-Écosse	Fédération canadienne des municipalités
Ministère de la Défense nationale du Canada	Gouvernement de la Saskatchewan	
Sécurité publique Canada	Gouvernement du Manitoba	
Service canadien du renseignement de sécurité	Gouvernement du Nouveau-Brunswick	
	Gouvernement du Québec	
	Gouvernement du Yukon	

Ces membres portent deux chapeaux : en plus d'être membres du BTCN, ils s'emploient également à défendre les intérêts et à communiquer les considérations de leurs organisations respectives, ce qui permet d'orienter l'élaboration des recommandations formulées dans le présent rapport d'étape et dans le document de politique à venir. Ils participent par ailleurs à ce processus d'élaboration sur une base continue.

Sensibilisation et participation des intervenants

Le BTCN reconnaît le rôle essentiel des intervenants dans le développement d'un RLBSP qui sera fonctionnel et efficace dans un contexte canadien. C'est la raison pour laquelle le BTCN a sollicité et recueilli les points de vue d'un éventail d'intervenants dans le cadre de différents forums, y compris du secteur privé, du milieu universitaire, des trois services, des administrations FPT, des exploitants d'infrastructures essentielles et des municipalités. La participation des intervenants se poursuivra jusqu'à la présentation du document de politique au début de 2020, et possiblement au-delà.

En 2017-2018, avant la création du BTCN, l'équipe de travail fédérale sur le RLBSP[27] mise sur pied par le groupe de travail FPT sur l'interopérabilité (GTI) a mené une série d'ateliers à l'intention des intervenants dans six villes du pays, ainsi qu'une séance de mobilisation en ligne. À ces ateliers ont participé plus de 200 intervenants provenant de nombreuses administrations du pays, notamment le Yukon, la Colombie-Britannique, l'Alberta, la Saskatchewan, le Manitoba, l'Ontario, le Québec, le Nouveau-Brunswick, l'Île-du-Prince-Édouard, la Nouvelle-Écosse et Terre-Neuve-et-Labrador. Sécurité publique Canada a également œuvré séparément, par l'intermédiaire du GTI et d'autres forums FPT, pour mobiliser les intervenants dans les Territoires du Nord-Ouest et le Nunavut. L'équipe de travail sur le RLBSP a consulté les gouvernements provinciaux et territoriaux, les administrations municipales, les premiers intervenants, le secteur privé et différents intervenants au sujet des modèles possibles de mise en œuvre d'un RLBSP au Canada. On compte parmi les défis en matière de communications d'urgence que l'on a le plus souvent relevés dans le cadre de ces consultations : la coordination d'un RLBSP potentiel; la couverture dans les régions rurales, éloignées et nordiques; les coûts et les calendriers possibles de mise en œuvre; l'interopérabilité entre le Canada et les États-Unis; la capacité au sein des petites collectivités et organismes bénévoles; et la relation entre un RLBSP potentiel et les réseaux de RMT existants. On a aussi fait part au BTCN de ces préoccupations dans le cadre des activités de mobilisation menées auprès des intervenants, comme expliqué ci-après.

Entre juin 2017 et janvier 2018, le CSS de RDDC, au nom de l'équipe de travail sur le RLBSP, a tenu huit ateliers un peu partout au pays dans le but de valider les cas pratiques relatifs au RLBSP et de mieux comprendre les besoins des utilisateurs de la communauté de la sécurité publique dans le contexte des communications en matière de sécurité publique. Ces séances ont accueilli un total de 131 participants, y compris des représentants de la communauté des premiers intervenants, du milieu universitaire, des secteurs de la technologie de l'information et des télécommunications,

[27] L'équipe de travail fédérale sur le RLBSP réunissait des représentants de SP, d'ISDE et du CSS de RDDC.

et des administrations municipales et provinciales. Outre ces ateliers, la Gendarmerie royale du Canada (GRC) a également soumis des commentaires consolidés à propos des 31 cas pratiques révisés. L'information recueillie, en plus de la rétroaction sur les cas pratiques relatifs au RLBSP, a permis de réaliser des analyses plus approfondies des exigences de la communauté de la sécurité publique. Ces analyses ont mené à l'élaboration du document intitulé « Les cas d'utilisation et les exigences des utilisateurs du Réseau à large bande de sécurité publique (RLBSP) » du CSS de RDDC[28]. Elles ont par ailleurs servi de document d'orientation pour créer d'autres documents scientifiques au sujet des considérations techniques relatives au RLBSP du Canada.

Le BTCN reconnaît le travail et l'apport précieux des autres ministères, des provinces, des territoires, des municipalités et des associations des trois services. Que ce soit dans le contexte des allocutions présentées lors de conférences, des séances d'information à l'intention des intervenants ou des réunions entre intervenants et utilisateurs, les activités de sensibilisation et de mobilisation menées au sein de leurs territoires de compétence respectifs sont d'une importance cruciale pour élaborer des recommandations pertinentes fondées sur des données probantes à propos de la mise en œuvre d'un RLBSP au Canada.

Ce que nous avons entendu

La rétroaction soumise de la part des intervenants était de nature positive, ces derniers étant satisfaits des progrès et du leadership démontrés dans cette initiative. Ils sont également reconnaissants d'être informés des travaux en cours et ont exprimé leur souhait d'être tenus au courant de l'évolution de la situation. Les intervenants ont hâte de prendre part à cette initiative et ont offert d'aider le BTCN.

On compte parmi les questions les plus fréquemment soulevées par les intervenants dans le cadre de ces activités de mobilisation le calendrier de mise en œuvre du RLBSP et les cycles budgétaires aux échelles fédérale, provinciale et municipale, en particulier depuis l'allocation du spectre par ISDE en 2017. Dans certains territoires de compétence, les infrastructures vieillissantes de communication et les investissements devant être réalisés dans un avenir proche sont des raisons qui sous-tendent l'accélération du lancement d'un RLBSP.

On a fait mention de l'interopérabilité à l'échelle du pays et des organismes, y compris entre les applications, à titre de considération importante pour les utilisateurs du RLBSP, ainsi que de la résilience du réseau. Les défis attribuables à la couverture ont fait l'objet d'une attention considérable, en particulier pour ce qui est des collectivités rurales, éloignées et nordiques. On a aussi souligné les questions de l'allocation de licences, de l'utilisation expérimentale de la bande 14, et de l'emploi commercial de la capacité excédentaire.

[28] Centre des sciences pour la sécurité de Recherche et développement pour la défense Canada. Non publié. Les cas d'utilisation et les exigences des utilisateurs du Réseau à large bande de sécurité publique (RLBSP).

En décembre 2018, le BTCN a tenu une séance de mobilisation à Toronto avec des intervenants du secteur privé. Au cours de l'événement, et des discussions bilatérales subséquentes, le BTCN a fait le point sur les travaux en cours, répondu aux questions des participants et sollicité leurs commentaires sur les approches proposées et les incidences possibles sur les intervenants. Le degré de participation obtenu témoigne de l'intérêt de l'industrie privée à prendre part au projet du RLBSP. Les participants souhaitaient en apprendre davantage à propos des consultations publiques d'ISDE, l'attribution des licences non standards de la bande 14, et le processus de transition. On a aussi fait mention de l'harmonisation potentielle avec les investissements commerciaux prévus comme un facteur d'efficacité potentiel dans la mise en œuvre du RLBSP.

Le BTCN a également recueilli les commentaires de fournisseurs de services de transport et de services publics, lesquels ont exprimé leur intérêt de participer et contribuer au projet du RLBSP. Powertech Labs a établi un partenariat avec de nombreux intervenants en vue de mener des essais qui permettront, entre autres choses, de démontrer, de tester et de valider la valeur du RLBSP dans le cadre des activités des services publics et des services de transport. Ces organisations disposent déjà d'une infrastructure considérable, ce qui est particulièrement important dans les régions rurales et éloignées qui sont mal desservies.

Le BTCN a aussi échangé sur une base régulière avec son homologue américain, la First Responder Network Authority qui est responsable de l'exploitation du réseau FirstNet aux États-Unis et qui de ce fait représente un intervenant international important. On a créé FirstNet en 2012 et lui a alors alloué 20 MHz de spectre, le même qui fut alloué au Canada. FirstNet a reçu 7 milliards de dollars pour établir un réseau national à large bande de la sécurité publique qui est interopérable, et s'est par ailleurs vu confier le mandat de mettre sur pied, d'exploiter et d'entretenir ce réseau[29].

Au cours de leurs réunions avec le BTCN, FirstNet a partagé de précieuses informations et leçons qu'il a tirées de son expérience de déploiement et de mise en œuvre d'un RLBSP national. Ces discussions bilatérales ont permis au BTCN de mieux comprendre les risques et les possibilités d'importance au chapitre de certains éléments, y compris l'interopérabilité du RLBSP entre le Canada et les États-Unis, la sécurité du réseau, les besoins des utilisateurs de la sécurité publique, l'évolution des technologies, ainsi que les considérations en matière de gouvernance et d'ordre opérationnel. Les échanges avec FirstNet se poursuivront sur une base continue alors que le BTCN élabore des recommandations au sujet d'un RLBSP national canadien.

Peu importe la manière dont le RLBSP sera mis en œuvre, la communauté de la sécurité publique souhaite garantir que le spectre serve l'intérêt du public. Parallèlement, le BTCN veut garantir que le RLBSP sera utilisé par la communauté de la sécurité publique et qu'il deviendra aussi indispensable que les systèmes de RMT qui sont actuellement utilisés par la

[29] https://firstnet.gov/about/history, consulté le 19 février 2019.

majorité des premiers intervenants et du personnel de sécurité publique. On compte parmi les autres considérations d'importance l'abordabilité, la résilience et l'interopérabilité.

À cette étape, le BTCN est en position de fournir aux intervenants des analyses et des recommandations préliminaires à des fins d'examen. Il est important de souligner que les propositions du BTCN se concentrent sur les exigences minimales d'un RLBSP interopérable au Canada. Cela permet aux entités de la sécurité publique d'adapter ou d'utiliser la capacité du réseau de manière à satisfaire leurs différents besoins.

Projets, projets pilotes et expériences touchant au RLBSP

Afin d'offrir des analyses fondées sur des données probantes et des recommandations éclairées, le BTCN a rassemblé et examiné de la documentation et des études à propos de la mise en place d'un RLBSP au Canada et à l'échelle internationale. Lorsque cela était possible, le BTCN a également collaboré directement avec des personnes et des organisations en vue de recueillir de l'information et des commentaires. L'expérience, l'expertise et les corpus d'études à la disposition du BTCN lui ont permis de dégager des leçons au chapitre de la gouvernance, de la prestation de services, de l'économie, et des technologies existantes et émergentes. Pour répondre le plus efficacement possible aux besoins de la communauté d'utilisateurs de la sécurité publique du Canada, le déploiement d'efforts pour garantir que les conclusions et les recommandations du BTCN sont soutenues par des constatations tangibles qui se fondent sur le monde réel est d'une importance centrale dans les activités que mène le bureau. De façon générale, les thèmes de recherche comprennent les projets et les exemples internationaux se rapportant au RLBSP; les projets pilotes et projets d'autre nature sur le RLBSP; et les expériences touchant aux technologies liées au RLBSP.

À l'échelle internationale, le Canada assure un rôle de leadership dans la recherche sur les technologies associées au RLBSP et dans l'élaboration de solutions novatrices. Alors que d'autres pays examinent les questions en matière de RLBSP qui leur sont propres, le Canada peut aussi apprendre de l'expérience et des difficultés associées à la large bande de sécurité publique de ces pays. Bien que l'on doive envisager les approches canadiennes possibles en fonction de notre réalité sur les plans géographique, économique, démographique et politique, la comparaison avec d'autres projets nationaux de RLBSP nous donne l'occasion d'examiner un éventail de leçons apprises. Au moment de la rédaction du présent rapport, certains pays, dont les États-Unis, le Royaume-Uni, l'Australie, la France, la Finlande, le Qatar et la République de Corée, menaient, à différentes étapes, des projets nationaux de RLBSP. Vu la proximité de FirstNet et son inclusion au principe d'interopérabilité du RLBSP, il va de soi que son expérience aux États-Unis représente actuellement un intérêt particulier pour le BTCN. Alors que ces marchés internationaux se développent et que d'autres émergent, le BTCN continuera d'assurer un suivi à cet égard et d'intégrer des analyses à ces conclusions.

Pour ce qui est des projets pilotes, des essais et des initiatives touchant au RLBSP, le BTCN s'est tenu informé des exemples qui existent au Canada et aux États-Unis afin de se pencher sur les validations de concepts pour chacun de ces pays. On mène plusieurs projets pilotes au Canada grâce aux licences temporaires expérimentales du spectre de la bande 14, et nombreux d'entre eux se concentrent sur des études pratiques dans des environnements guidés ou simulés en fonction des événements. On a conçu d'autres exemples de manière à ce qu'ils soient limités sur le plan géographique et à ce qu'ils fonctionnent selon leurs propres besoins locaux. On compte parmi ces exemples le réseau d'essai LTE (Long-Term Evolution technology) de la RCN; le LTE Project du service de police régional de Halton; le réseau d'essai à large bande mobile du service de police de Toronto; le réseau d'essai LTE du service de police de Calgary; le projet LA-RICS LTE; les réseaux d'essai LTE d'Adams County (Colorado); le RLBSP LTE de Harris County (Texas); le *JerseyNet* du New Jersey; le Public Safety LTE Network du Nouveau-Mexique; l'expérience du Service des incendies d'Ottawa sur les matières dangereuses, l'expérience sur les communications des aéroports du Service paramédic d'Ottawa; et la série d'activités de l'Expérience Canada–États-Unis de renforcement de la résilience (CAUSE).

Les considérations d'ordre technologique ont également tenu une importance particulière dans le travail du BTCN, notamment en ce qui concerne les capacités et les limites actuelles et anticipées du réseau à large bande. On suppose que le RLBSP s'appuierait sur des normes ouvertes, dans la mesure du possible, qui comprendraient des renvois particuliers à celles établies par le 3rd Generation Partnership Project (3GPP) (ainsi qu'à celles formulées par d'autres organes clés de normalisation, s'il y a lieu). Le BTCN a donc assuré un suivi des rapports d'expériences et de constatations publiés par des organisations, des institutions et des organismes clés, dont le CSS de RDDC; le Centre de recherches sur les communications d'ISDE; l'initiative Bridging Research and Interoperability Collaboration (BRiC) de l'Université de Regina; la Telematics Research Lab de l'Université Simon-Fraser; l'Office of Emergency Communications et l'Office for Interoperability and Compatibility du Department of Homeland Security; le Communications Technology Laboratory du National Institute of Standards and Technology; le Texas A&M University Internet 2 Technology Evaluation Center; le Centre for Testing and Interoperability de l'Institut européen des normes de télécommunication.

Alors que cette section ne fournit pas une liste exhaustive de documents de référence, elle a néanmoins pour objectif d'offrir un aperçu de la profondeur et de l'étendue de la recherche dont on tient compte pour formuler des conclusions et des recommandations.

Principes applicables au RLBSP

Le BTCN reconnaît que les discussions entourant la mise en place d'un RLBSP au Canada sont en cours depuis un bon moment. On a établi que l'utilisation d'un réseau à large bande dans le contexte de la sécurité publique offre des avantages considérables et qu'elle peut améliorer au bout du compte l'efficacité des efforts d'intervention. La création d'un RLBSP national contribuerait à résoudre les problèmes actuels en matière de communications d'urgence en offrant

aux intervenants un accès prioritaire aux réseaux de communication, un degré élevé d'interopérabilité avec les autres administrations, ainsi qu'une utilisation sécuritaire des données et des applications sans fil à haute vitesse. Toutefois, certains aspects importants doivent être pris en compte afin de répondre aux besoins de la communauté de la sécurité publique dans la mise en place de ce réseau. On décrit ces considérations ci-après, celles-ci étant essentielles à la réussite d'un RLBSP canadien.

On entend par « principes » les normes, les règles ou les valeurs fondamentales qui représentent ce qui est souhaitable et positif pour une personne, un groupe, une organisation ou une communauté, et qui aident à déterminer le bien-fondé ou l'inadéquation de ses actions. Ils sont de nature plus sommaire que les politiques et les objectifs – ils ont pour but de diriger et d'orienter la collectivité dans son ensemble.

Les principes applicables au RLBSP sont le fruit de projets pilotes et d'essais, d'études de cas internationales et des exigences des utilisateurs que l'on a relevées en analysant les cas pratiques relatifs au RLBSP recueillis dans le cadre de consultations avec les utilisateurs potentiels du RLBSP. Ils découlent des connaissances en matière de sécurité publique et de configuration de réseau, des études et de l'expérience, ainsi que des normes, des pratiques éthiques et des expériences culturelles partagées par les membres nationaux du BTCN.

Le RLBSP doit offrir un service équitable à l'ensemble de la communauté de la sécurité publique. La qualité de l'expérience est le fondement du RLBSP et témoigne de l'universalité de son service. Celle-ci offre un cadre aux principes qui s'appliquent aux RLBSP et constitue le fondement des principes qui le régissent, tels qu'ils sont appliqués.

On emploie le terme « utilisateurs du RLBSP » plutôt que le terme « utilisateurs de la sécurité publique ». Les « utilisateurs du RLBSP » ne comprennent pas les utilisateurs commerciaux qui ne s'inscrivent pas dans l'enveloppe de la sécurité, mais qui consomment une partie de la capacité du spectre du RLBSP lorsque celui-ci est inutilisé par les utilisateurs du RLBSP.

On présente ci-après les principes applicables au RLBSP du Canada.

Interopérabilité

Principe : *Le RLBSP permet à ses utilisateurs de communiquer et partager de l'information, conformément aux autorisations prévues, et ce, en tout temps et depuis tout lieu où celui-ci est accessible.*

Les utilisateurs des réseaux LTE commerciaux sont intrinsèquement capables de communiquer entre eux en tout temps et depuis tout endroit où s'étend la couverture grâce aux technologies mises en œuvre et aux ententes d'itinérance entre les ORM.

Le principe d'interopérabilité du RLBSP commande l'offre des services de réseau et l'application des ententes qui sont nécessaires pour assurer l'accès des utilisateurs du RLBSP aux services du RLBSP et à d'autres utilisateurs depuis tout endroit au sein du RLBSP, et ce, en tout temps.

Sous réserve d'une entente avec FirstNet, des services de réseau et des ententes supplémentaires sont nécessaires pour assurer l'accès des utilisateurs du RLBSP et de FirstNet aux services et autres utilisateurs dont ils ont besoin pour s'acquitter de leurs fonctions depuis tout endroit au sein du RLBSP ou de FirstNet, et ce, en tout temps. Comme stipulé par le plan d'action de la SICC et le GTI de CANUS, l'interopérabilité des communications entre un responsable du RLBSP du Canada et FirstNet est essentielle au partage transfrontalier d'informations stratégiques et techniques[30].

Le RLBSP doit être assujetti à des normes communes de sorte que les applications adoptées dans une région donnée du Canada fonctionnent adéquatement dans les autres régions du pays, que les applications cruciales à la mission soient pleinement interopérables, et que l'expérience des utilisateurs du RLBSP soit uniforme.

Il s'agit d'un aspect fondamental de la vision d'un RLBSP capable d'assurer l'accessibilité et le partage de l'information. Bien que les fonctions d'accessibilité et de partage de l'information puissent être lancées ou réalisées dans l'environnement sans fil du RLBSP, celles-ci sont exécutées par le biais des interactions entre les applications, les données et les serveurs de l'émetteur et du destinataire. Les lois, les règlements, les politiques et les ententes en place influenceront la disponibilité de telles transactions et pourraient commander des changements facilitant leur application. Le RLBSP nécessitera la mise en place de règles en matière d'accès et de partage.

Permanence de l'accès au réseau

Principe : *Que ce soit dans le cadre de leurs activités quotidiennes, ou encore d'événements ou d'urgences d'importance majeure, les utilisateurs du réseau doivent disposer en permanence d'un accès immédiat et ininterrompu au RLBSP, partout où celui-ci s'étend.*

Des mécanismes assurant la qualité du service, l'accès prioritaire et la préemption (QPP) au sein du RLBSP sont nécessaires pour garantir l'accès des utilisateurs du RLBSP. Les utilisateurs du RLBSP doivent toujours avoir la priorité

[30] Sécurité publique Canada. Janvier 2018. Stratégie d'interopérabilité des communications pour le Canada. https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntrprblt-strtg/index-fr.aspx

sur les utilisateurs commerciaux et doivent bénéficier d'un droit de préemption sur ces derniers. Au sein du RLBSP, il doit exister des mécanismes qui déterminent la priorité et d'autres fonctions qui assurent un contrôle adéquat des ressources du RLBSP, qui établissent la hiérarchie des commandes locales et qui sont capables de modifier de façon dynamique la « cote » QPP des utilisateurs et des applications lorsque leur rôle dans le cadre d'un événement donné est suffisamment important.

Les utilisateurs passant d'un mécanisme de prestation de services à un autre – d'un fournisseur à un autre, ou d'un site fixe à un site déployable – ne doivent pas se heurter à une interruption de session et doivent bénéficier de la cote de QPP, peu importe la manière dont ils sont branchés au RLBSP. De plus, les sessions entre le RLBSP et FirstNet ne doivent pas être interrompues.

Couverture

Principe : *Le RLBSP offrira, à tout le moins, une couverture équivalente à celle de la technologie commerciale à large bande et devra étendre sa couverture aux zones et collectivités urbaines, rurales, autochtones et éloignées qui sont mal desservies, ou améliorer sa couverture dans ces régions.*

Les événements quotidiens, d'importance majeure et d'urgence, dans le cadre desquels les utilisateurs du RLBSP interviennent ne sont pas assortis de limites sur le plan de la géographie ou de la durée, et surviennent souvent de manière inattendue dans les collectivités intérieures, rurales, éloignées, nordiques ou autochtones pour lesquelles l'analyse de rentabilisation actuelle de la couverture commerciale est faible. Une couverture permanente doit être assurée dans les endroits où les utilisateurs du RLBSP mènent fréquemment ou normalement leurs activités et celle-ci doit être complétée par une couverture déployable partout ailleurs. La couverture ne peut pas être inférieure à celle dont les utilisateurs commerciaux bénéficient et devrait, avec le temps, être supérieure.

Résilience et robustesse

Principe : *Le RLBSP doit être résilient et robuste pour répondre aux exigences en matière d'accès au réseau.*

Les services offerts par le RLBSP à ses utilisateurs, en particulier ceux jugés essentiels à la mission, sont importants dans le cadre des opérations quotidiennes et revêtent une importance particulière au cours des événements majeurs et des situations d'urgence, cas où ils sont susceptibles d'être perturbés par les conditions de l'environnement ou de faire l'objet d'une attaque. Le RLBSP doit être en mesure de fonctionner sans interruption dans un large éventail de conditions, être capable de se remettre des contretemps (ou d'un contretemps) et de s'adapter adéquatement aux changements. Les sites

de réseau d'accès radio (RAR) pourraient nécessiter un renforcement d'un degré supérieur à celui des sites commerciaux, particulièrement en ce qui concerne l'alimentation, et ce, afin de survivre aux scénarios les plus défavorables[31].

Prestation des services essentiels à la mission

Principe : *Le RLBSP permettra de fournir aux utilisateurs de la sécurité publique des services essentiels à la mission qui seront hébergés par le réseau.*

Il est largement reconnu qu'une interruption ou une perturbation des services de communication s'appuyant sur l'utilisation d'appareils dotés d'un bouton micro (PTT), peu importe le moment, entraînent une dégradation importante des opérations. Il s'agit d'un élément essentiel de communication et de sécurité des opérations de sécurité publique. Alors que l'on développe et adopte le RLBSP, en plus des normes ouvertes comme celles s'appliquant aux appareils à bouton de microphone essentiels à la mission (MCPTT), on commencera à utiliser des données essentielles à la mission (MCData) et des vidéos essentiels à la mission (MCVideo) à titre d'éléments fondamentaux et centraux de communication et de sécurité. Contrairement aux applications choisies par les organismes utilisateurs individuels, ces services essentiels à la mission qui sont hébergés par le réseau feront partie intégrante du RLBSP et permettront d'améliorer son interopérabilité nationale.

Sécurité

Principe : *Le RLBSP doit intégrer et prendre en charge des mécanismes de sécurité qui répondent aux exigences de confiance des organisations d'utilisateurs du RLBSP et de celles qui utilisent ce dernier pour échanger des données.*

Les évaluations des risques permettent d'estimer la probabilité et l'incidence des menaces potentielles. Les mécanismes de sécurité sont intégrés par couche afin d'atténuer l'incidence des menaces possibles. Les menaces potentielles au RLBSP doivent être relevées, évaluées et atténuées par une posture de sécurité suffisamment efficace pour assurer un accès continu au réseau et gagner la confiance des utilisateurs du RLBSP et de ceux disposés à échanger leurs données dans le réseau.

Durabilité

Principe : *Le RLBSP doit répondre aux besoins de la première génération d'intervenants sans compromettre sa capacité de satisfaire aux besoins des futurs intervenants*.

[31] Pour obtenir un exemple de lignes directrices en matière de renforcement, consulter le rapport sur les communications en matière de sécurité publique de 2014 du NPSTC : *Defining Public Safety Grade Systems and Facilities*. http://www.npstc.org/download.jsp?tableId=37&column=217&id=3066&file=Public_Safety_Grade_Report_140522.pdf.

Les plans environnemental, économique et social sont les trois piliers de la durabilité. Le RLBSP doit être exploité par l'entremise de mécanismes qui garantissent que l'intégrité environnementale est préservée, que les ressources requises pour assurer son intégrité ultérieure sont accessibles et que les besoins futurs des intervenants peuvent être satisfaits, qu'ils sont satisfaits et qu'ils sont respectés. Sont inhérents à ce principe la nécessité d'assurer une maintenance continue, d'évoluer, de se tenir à jour des technologies et des normes changeantes, et de veiller à ce que les fournisseurs de biens et de services du RLBSP soient durables pour un bon nombre d'années.

Abordabilité

Principe : *Le RLBSP doit être abordable pour l'ensemble de la communauté d'utilisateurs.*

L'abordabilité est mesurée en fonction du coût relativement au prix qu'un acheteur est en mesure de payer. L'interopérabilité ne peut pas être compromise en raison du manque de moyens financiers des membres de la communauté d'utilisateurs du RLBSP de souscrire aux services du RLBSP. L'abordabilité rivalisera avec d'autres priorités du RLBSP en raison du sous-financement.

Si les coûts d'adhésion aux services du RLBSP étaient prohibitifs pour certains abonnés, la solution de remplacement serait d'appliquer des tarifs subventionnés. À titre d'exemple, on pourrait tirer ces subventions des revenus générés par l'utilisation commerciale de la capacité excédentaire du spectre du RLBSP ou de frais supplémentaires semblables à ceux des services commerciaux actuellement en place dans certaines régions du Canada.

Utilisation du spectre

Principe : *Le RLBSP utilisera le spectre de manière efficace.*

Que ce soit pour soutenir les utilisateurs du RLBSP dans le cadre de leurs activités quotidiennes, d'événements majeurs ou d'urgences, ou pour générer des revenus en soutien aux autres principes du RLBSP, le spectre du RLBSP doit être utilisé aussi efficacement que possible.

Le spectre du RLBSP doit être accessible à ses utilisateurs en tout temps, et ces derniers doivent bénéficier d'un accès prioritaire et d'un droit de préemption sur les utilisateurs commerciaux. Bien que les besoins des utilisateurs du RLBSP puissent par moments excéder la capacité offerte par le spectre, la plupart du temps, le spectre alloué au RLBSP doit bénéficier d'une capacité excédentaire.

La mise à profit de la portion inutilisée du spectre par les utilisateurs commerciaux, à l'extérieur de l'enveloppe de sécurité du RLBSP, est un gage de la capacité à générer des revenus pour compenser les coûts associés au RLBSP.

Options de prestation opérationnelle

Méthodes et approches en matière de recherche

Conception de l'étude

Le BTCN a réalisé des analyses comparatives afin d'élaborer et d'orienter l'évaluation de l'utilisation du spectre, de la prestation des services et de la structure de délivrance de licences du RLBSP.

Critères et méthodes de sélection

Aux fins des analyses, on a sélectionné et évalué un éventail de modèles possibles en fonction de leur capacité à respecter pleinement les principes fondamentaux qui régissent le RLBSP. Les modèles ont été sélectionnés en consultation avec différents intervenants et experts techniques, y compris le CSS de RDDC, et ceux-ci témoignent d'un éventail raisonnable de possibilités. Lorsque cela était pertinent, le BTCN s'est appuyé sur des études de cas internationales et les premiers utilisateurs de réseaux à large bande de sécurité publique pour soutenir ses analyses comparatives et orienter l'élaboration de ses recommandations. Par exemple, les leçons apprises des États-Unis, du Royaume-Uni, de la République de Corée et de l'Australie ont servi à démontrer les avantages, les défis et les limites associés aux différents modèles.

Analyse des données

Le BTCN a attribué des cotes à chacun des principes du RLBSP en s'appuyant sur les informations et les constatations clés d'études de cas, de recherches et de consultations auprès d'experts techniques. L'attribution des cotes s'est faite en fonction des catégories suivantes :

- Vert – Probabilité élevée de satisfaction du principe (E)
- Orange – Probabilité modérée de satisfaction (M)
- Rouge – Probabilité faible de satisfaction (F)

Chaque cote a été attribuée sur une base relative et avait pour but de mettre en évidence les différences entre les modèles. Il est important de noter qu'il est possible que l'ampleur des différences ne soit pas uniforme. À titre d'exemple, la différence entre les cotes rouges et orange pourrait différer de la différence entre les cotes orange et vertes. Rien n'a été tenté jusqu'ici pour déterminer si certaines exigences sont plus ou moins importantes que d'autres, il ne faut donc pas les comparer les unes aux autres. Le BTCN reconnaît aussi l'importance de la souplesse au chapitre des options de prestation opérationnelle et déploie tous les efforts qui soient pour relever les possibilités supplémentaires qui pourraient déborder du cadre d'une analyse donnée.

Analyse

Modèles d'utilisation du spectre

Contexte

Dans le cadre du budget de 2015, le gouvernement du Canada a reconnu que la création d'un RLBSP à l'aide de la bande 14 serait une étape essentielle pour améliorer « la collaboration entre les organismes de sécurité publique afin qu'ils puissent sauver des vies et assurer la sécurité de nos collectivités»[32] . Comme le soutient la communauté de la sécurité publique, cette désignation du spectre est nécessaire pour répondre à la demande actuelle et à long terme des premiers intervenants en matière de communication de données mobiles[33].

À la lumière de ces décisions, le RLBSP devrait, à son lancement, être un réseau cellulaire à large bande de quatrième génération (4G) semblable aux réseaux commerciaux qui desservent actuellement les appareils intelligents utilisés par la population générale[34]. Conformément à la décision d'ISDE, celui-ci utiliserait la bande 14 et permettrait aux premiers intervenants et à d'autres utilisateurs de la sécurité publique de communiquer et de partager de l'information riche en contenu les uns avec les autres dans le cadre d'opérations quotidiennes et d'événements majeurs et d'incidents[35].

Bien qu'il existe de nombreuses façons possibles de mettre en œuvre un RLBSP national, les approches relatives à l'utilisation du spectre de la bande 14 peuvent varier considérablement et représenter différents coûts et risques[36]. Afin de soumettre des recommandations sur la mise en œuvre du RLBSP au Canada, le BTCN a envisagé trois modèles généraux d'utilisation du spectre, lesquels s'harmonisent avec les objectifs et les besoins fonctionnels actuels de la communauté de la sécurité du Canada. Les modèles sont définis dans le tableau 1 ci-dessous.

[32] Chapitre 4.3, sous-section *Améliorer les communications relatives à la sécurité publique :* https://www.budget.gc.ca/2015/docs/plan/toc-tdm-fra.html.
[33] Innovation, Sciences et Développement économique Canada. Juin 2017. Décisions se rapportant au cadre politique, technique et de délivrance de licences pour l'utilisation du spectre à large bande destiné à la sécurité publique, et ce, dans les bandes de 758 à 763 MHz et de 788 à 793 MHz (bloc D), ainsi que de 763 à 768 MHz et de 793 à 798 MHz (bloc SPLB), p. 6.
[34] Recherche et développement pour la défense Canada. Avril 2017. Implementation models for a public safety broadband network, p. 1
[35] Innovation, Sciences et Développement économique Canada. Juin 2017. Décisions se rapportant au cadre politique, technique et de délivrance de licences pour l'utilisation du spectre à large bande destiné à la sécurité publique, et ce, dans les bandes de 758 à 763 MHz et de 788 à 793 MHz (bloc D), ainsi que de 763 à 768 MHz et de 793 à 798 MHz (bloc SPLB).
[36] Recherche et développement pour la défense Canada. Avril 2017. Implementation models for a public safety broadband network, p. 2

Tableau 1 : Modèles d'utilisation du spectre

Modèles d'utilisation du spectre		
Modèle no 1 **Réseau exclusivement consacré à la sécurité publique** (Réseau spécialisé)	Modèle no 2 **Réseau partagé à des fins de sécurité publique et commerciales** (Réseau partagé)	Modèle no 3 **Réseau commercial** (Réseau commercial)
Il s'agit d'un réseau consacré à la sécurité publique, dont le spectre est exclusivement utilisé par les utilisateurs de la sécurité publique (utilisation des blocs SPLB et D) (p. ex. la Corée du Sud – SafeNet).	Il s'agit d'un réseau qui soutient l'utilisation à des fins de sécurité publique et des fins commerciales (avec réseaux de base distincts), qui offre un accès prioritaire et des droits de préemption aux utilisateurs de la sécurité publique lors d'urgences et autres situations de nécessité (p. ex. États-Unis – FirstNet).	La communauté de la sécurité publique obtient des services d'un ou de plusieurs fournisseurs de services commerciaux, qui utilisent leur spectre existant ou leur spectre de la bande 14 acquise (p. ex. le Royaume-Uni).

Bien que l'on ait soumis trois modèles distincts à des fins d'examen, il convient de noter qu'à la lumière des *Décisions se rapportant au cadre politique, technique et de délivrance de licences pour l'utilisation du spectre à large bande destiné à la sécurité publique* d'ISDE (juin 2017), le modèle n^{o} 3 – réseau commercial – n'est plus pertinent et ne fait plus l'objet d'un examen. Dans le cadre de ces décisions, comme susmentionné, ISDE a alloué 20 MHz de spectre aux fins d'un RLBSP national. Conséquemment, le modèle n^{o} 3, selon lequel le RLBSP obtiendrait des services de fournisseurs commerciaux qui utilisent le spectre commercial actuel ou nouvellement acquis, ne fait plus l'objet d'un examen du fait qu'un RLBSP national ne serait pas uniquement exploité par l'entremise des réseaux commerciaux existants.

Dans ces mêmes décisions, ISDE accepte que l'utilisation commerciale de la capacité excédentaire soit permise pourvu que les utilisateurs de la sécurité publique aient la priorité et des droits de préemption sur toute forme d'utilisation commerciale[37]. Celui-ci encourage les discussions continues à ce chapitre et au sujet d'autres questions afin de formuler des recommandations éclairées qui se fondent sur un point de vue consolidé.

[37] Innovation, Sciences et Développement économique Canada. Juin 2017. Décisions se rapportant au cadre politique, technique et de délivrance de licences pour l'utilisation du spectre à large bande destiné à la sécurité publique, et ce, dans les bandes de 758 à 763 MHz et de 788 à 793 MHz (bloc D), ainsi que de 763 à 768 MHz et de 793 à 798 MHz (bloc SPLB).

Considérations

Le BTCN a appliqué les hypothèses retrouvées dans le tableau 2 dans le cadre de son analyse afin de formuler des recommandations au sujet de l'utilisation du spectre du RLBSP du Canada. L'apport de modifications aux hypothèses fondamentales présentées ci-après pourrait avoir une incidence sur l'analyse et les recommandations qui en découlent.

Tableau 2 : Hypothèses concernant l'utilisation du spectre

Légende	Oui (O)	Non (N)

Hypothèses concernant l'utilisation du spectre		
Hypothèses	**Spécialisé**	**Partagé**
On mettrait en œuvre un RLBSP en tirant profit de l'infrastructure physique, comme les stations de base, des ORM commerciaux et de l'infrastructure de communication du gouvernement et de la sécurité publique, dans la mesure du possible.	O	O
Des mécanismes de QPP seraient mis en place, car il s'agit d'un critère très important pour les utilisateurs.	O	O
Le réseau de base de la sécurité publique serait distinct du réseau de base commercial.	O	O
Les organismes de sécurité publique ne sont pas obligés d'adhérer au RLBSP.	O	O
Un spectre est alloué à la sécurité publique.	O	O

Analyse, risques et possibilités

Tout en tenant compte des considérations susmentionnées, le BTCN a mené une évaluation qualitative de chacun des modèles d'utilisation du spectre à l'examen en fonction de leur capacité à satisfaire aux principes applicables au RLBSP, et ce, en leur attribuant une cote de probabilité de satisfaction faible, modérée ou élevée.

Les possibilités et les défis associés à chacun des modèles sont présentés de façon sommaire dans le tableau 3 : *Résumé de l'analyse des modèles d'utilisation du spectre*, et sont expliqués en détail ci-après.

Tableau 3 : Résumé de l'analyse des modèles d'utilisation du spectre

Légende	Probabilité élevée de satisfaction du principe (E)	Probabilité modérée de satisfaction (M)	Probabilité faible de satisfaction (F)

Résumé de l'analyse des modèles d'utilisation du spectre		
Principes évalués du RLBSP	**Réseau spécialisé**	**Réseau partagé**
Interopérabilité	M	M
Permanence de l'accès au réseau	E	E
Couverture	F	E
Résilience et robustesse	M	E
Prestation des services essentiels à la mission	E	E
Sécurité	E	E
Durabilité	F	E
Abordabilité	F	E
Utilisation du spectre	F	E

Interopérabilité : Pour chacun des modèles examinés, l'interopérabilité est assurée par la coordination centrale des politiques relatives aux opérations du réseau, l'adoption de normes nationales en matière d'interopérabilité et un régime solide de surveillance et d'application de ces politiques et normes.

On estime que les modèles de réseaux spécialisé et partagé présentent une probabilité modérée d'assurer l'interopérabilité. Le principal risque menaçant l'interopérabilité d'un réseau spécialisé ou partagé tient de l'hypothèse selon laquelle les organismes de sécurité publique n'auraient pas l'obligation d'adhérer au RLBSP. Conséquemment, il

est possible que certains utilisateurs de la sécurité publique ne migrent pas de leurs services commerciaux actuels et donc qu'ils ne soient pas interopérables avec les utilisateurs du RLBSP qui accèdent à des services et des applications hébergés par le réseau du RLBSP.

Permanence de l'accès au réseau : On estime que les deux modèles présentent une probabilité élevée d'offrir un accès permanent au réseau. Un réseau spécialisé pourrait ne compter qu'un nombre relativement faible d'utilisateurs – sécurité publique seulement – et donc disposer de bande excédentaire, de sorte que les droits d'accès prioritaires et de préemption ne seraient que rarement utilisés. Un réseau partagé garantirait l'accès prioritaire des utilisateurs de la sécurité publique sur les utilisateurs commerciaux au moyen de droits de priorité et de préemption.

Couverture : On estime que le réseau partagé présente la probabilité la plus élevée de satisfaire au principe de la couverture. Comme c'est le cas pour les nombreux systèmes de RMT du Canada[38], ce modèle peut tirer profit d'un éventail de ressources afin d'étendre la couverture du réseau au-delà de la couverture des réseaux commerciaux en place, soit jusqu'aux régions rurales, éloignées ou autrement mal desservies. Ce modèle permettrait aussi d'offrir une couverture d'itinérance au sein des réseaux commerciaux en place et de tirer profit des relations existantes avec les organismes du secteur public et les infrastructures essentielles afin de promouvoir le partage de l'infrastructure et d'augmenter la couverture.

On estime qu'un réseau spécialisé présente une probabilité moindre de satisfaire au principe de couverture en raison des risques associés à la nécessité de mettre à profit les infrastructures existantes et d'établir de nouvelles infrastructures. Bien qu'un réseau spécialisé puisse être en mesure de tirer profit de l'infrastructure existante des réseaux commerciaux (comme les sites mobiles et les liaisons de raccordement), un tel réseau pourrait avoir de la difficulté à tirer profit de l'infrastructure du secteur public et d'autres infrastructures essentielles. L'atteinte des objectifs de couverture de réseau, en particulier dans les régions mal desservies, commandera des dépenses d'immobilisation considérables qui seront exclusivement assumées par le bassin d'utilisateurs de la sécurité publique. Les considérations en matière d'abordabilité et de durabilité du RLBSP tiennent compte des coûts supplémentaires.

Résilience et robustesse : Chacun des modèles d'utilisation du spectre commandera différents degrés d'investissement dans les infrastructures (p. ex. alimentation secours supplémentaire, redondance des liaisons terrestres) afin de répondre aux exigences en matière de résilience et de robustesse du RLBSP. On estime qu'un réseau partagé présente une probabilité élevée de satisfaire aux exigences en matière de résilience et de robustesse, car les ORM seraient en mesure de tirer profit des investissements de résilience et de robustesse pour améliorer parallèlement la résilience des réseaux commerciaux.

[38] Nouvelle-Écosse. 2019. Network Information. https://novascotia.ca/is/programs-and-services/psfc/network-information.asp.

Prestation des services essentiels à la mission : Comme tous les modèles s'appuieraient probablement sur des technologies et des architectures semblables, ils posséderaient tous une capacité semblable à en prendre en charge les applications et les services hébergés dans le réseau, comme les services essentiels à la mission. Il est donc fortement probable que les deux modèles soient en mesure d'assurer de tels services.

Sécurité : On tient pour acquis que les deux modèles posséderaient un réseau de base consacré à la sécurité publique, dont le trafic entrant et sortant pourrait potentiellement passer par Internet. Conséquemment, les mécanismes de sécurité physiques seraient semblables pour tous les modèles, car l'on tirerait probablement profit de différents volumes de l'infrastructure commerciale et de l'infrastructure de RMT de la sécurité publique. Le réseau spécialisé et le réseau partagé seraient tous deux en mesure d'assurer le chiffrement radio du trafic des utilisateurs.

Durabilité : La durabilité du RLBSP se caractérise par la capacité du réseau à soutenir un modèle opérationnel solide, à maintenir un bassin suffisant d'abonnés, à se tenir à la page des technologies et normes changeantes, et à assurer un accès continu à long terme à l'équipement et aux services essentiels au réseau. Au bout du compte, la durabilité du RLBSP dépendra largement de sa capacité à répondre aux besoins des utilisateurs de la sécurité publique sur une longue période et à sa capacité de le faire à des coûts économiques, sociaux et environnementaux acceptables. L'application d'une approche flexible qui permet d'effectuer des changements rapidement lorsque de nouvelles informations ou technologies sont disponibles, ou lorsque les conditions du marché changent, donnera lieu à la création d'un nombre accru de solutions durables pour les utilisateurs du RLBSP.

On estime donc que le réseau partagé est le modèle de mise en œuvre le plus durable si le spectre est alloué à un coût négligeable, car celui-ci offre des économies importantes dans les modèles opérationnels des ORM[39]. Les ORM pourraient à la fois tirer des revenus des utilisateurs de la sécurité publique et des utilisateurs commerciaux du spectre de la bande 14. De telles économies pourraient être utilisées pour diminuer les frais d'utilisateurs de la sécurité publique ou pour réaliser des investissements dans la QPP, la couverture, la robustesse, la recherche et le développement, ou pour une combinaison de ces éléments. Un réseau partagé pourrait également tirer profit des économies de gamme et des partenariats afin de réduire les coûts financiers et environnementaux du chevauchement inutile des infrastructures, comme les pylônes et les liaisons terrestres.

Le réseau spécialisé est le modèle le moins durable, car celui-ci nécessiterait de nouveaux investissements pour obtenir les mêmes résultats, sans offrir la capacité de tirer des revenus des utilisations commerciales. En 2013, on estimait que le degré d'investissement en capitaux se situait entre quatre et sept milliards de dollars[40]. De plus, des flux de revenus

[39] Innovation, Sciences et Développement économique Canada. 2014. Mise aux enchères dans la bande de 700 MHz. https://www.ic.gc.ca/eic/site/smt-gst.nsf/fra/h_sf10598.html
[40] KPMG/RedMobile. 2013.

seraient requis pour couvrir les dépenses opérationnelles, ce qui laisserait peu de fonds à réinvestir. Un réseau spécialisé ferait également concurrence aux fournisseurs commerciaux.

Abordabilité : On définit l'abordabilité du RLBSP comme la capacité du réseau à offrir un barème tarifaire soutenable pour tous les utilisateurs du RLBSP, ce qui permettrait de maximiser le nombre d'adhésions d'utilisateurs tout en répondant aux exigences d'un modèle opérationnel durable.

On estime que le réseau partagé est le modèle d'utilisation du spectre le plus abordable, car celui-ci peut tirer profit de la valeur commerciale du spectre inutilisé à des fins d'investissement, maximiser l'utilisation de l'infrastructure en place, et permettre une utilisation souple et efficace du spectre. Ces facteurs entraînent une diminution des frais pour les utilisateurs de la sécurité publique en comparaison avec le modèle de réseau spécialisé.

On estime que le réseau spécialisé est le modèle le moins abordable, car ses coûts opérationnels seraient financés exclusivement par le bassin d'utilisateurs du RLBSP, dont le nombre se situerait à environ 350 000[41]. Comme susmentionné, il est possible que le réseau spécialisé ne soit pas capable de tirer profit de l'infrastructure commerciale aussi facilement que le réseau partagé, ce qui pourrait avoir pour effet d'augmenter les tarifs des utilisateurs ou de commander l'obtention de subventions.

Utilisation du spectre : On estime que le réseau partagé présente une probabilité élevée de satisfaction en ce qui concerne l'utilisation efficace du spectre, car celui-ci serait utilisé par des utilisateurs commerciaux et des utilisateurs de la sécurité publique. Comme susmentionné, une telle utilisation partagée de la capacité inutilisée par les utilisateurs commerciaux est conforme aux décisions d'ISDE de 2017[42].

On estime que le réseau spécialisé présente une faible probabilité de permettre une utilisation efficace du spectre. Wells Fargo a estimé que dans le contexte américain, les premiers intervenants sont susceptibles d'utiliser moins de 1 % du spectre de 20 MHz qui est disponible[43]. De même, RDDC estime que les utilisateurs de la sécurité publique occupent

[41] Innovation, Sciences et Développement économique Canada. Demande de renseignements – Réseau à large bande de sécurité publique. Novembre 2017.
[42] Décisions se rapportant au cadre politique, technique et de délivrance de licences pour l'utilisation du spectre à large bande destiné à la sécurité publique, et ce, dans les bandes de 758 à 763 MHz et de 788 à 793 MHz (bloc D), ainsi que de 763 à 768 MHz et de 793 à 798 MHz (bloc SPLB). Juin 2017. Innovation, Sciences et Développement économique Canada.
[43] Forbes. 12 décembre 2017. How Much Does AT&T Stand To Gain From FirstNet? https://www.forbes.com/sites/greatspeculations/2017/12/12/how-much-does-att-stand-to-gain-from-firstnet/#164ddf672997

moins de 10 % du spectre sur une base quotidienne[44], ce qui laisse un volume considérable du spectre aux utilisations commerciales.

Recommandations à l'égard de l'utilisation du spectre

Bien qu'il soit techniquement possible de mettre en œuvre un RLBSP en appliquant une approche de réseau spécialisé ou partagé, l'analyse comparative démontre que chacun des modèles est assorti de risques et de possibilités très différents. Suivant la prise en compte de ces risques et possibilités, le BTCN recommande que l'on mette en œuvre le futur RLBSP selon une approche de réseau partagé.

Selon l'analyse comparative, le réseau partagé présente la probabilité la plus élevée de satisfaire aux principes fondamentaux du RLBSP, ce qui est largement attribuable à sa capacité de maximiser la valeur du spectre de la bande 14. Cette valeur pourrait stimuler les investissements en matière de couverture, et de résilience et robustesse, tout en assurant l'abordabilité et la durabilité du réseau au fil du temps. De plus, le modèle de réseau partagé présente une capacité supérieure d'assurer l'utilisation efficace du spectre, car il permet une meilleure utilisation commerciale de la bande 14 tout en garantissant l'accès prioritaire et la préemption des utilisateurs de la sécurité publique, à l'endroit et au moment requis.

Le réseau spécialisé n'est pas le modèle privilégié, car celui-ci présente une faible probabilité de satisfaire aux principes de la couverture, de la durabilité, de l'abordabilité et de l'utilisation efficace du spectre. Le réseau spécialisé commanderait de réaliser des dépenses en immobilisation considérables ainsi que des dépenses opérationnelles continues, et dépendrait exclusivement à cette fin des tarifs payés par les utilisateurs du RLBSP, lesquels ne seraient pas complétés par un bassin beaucoup plus important d'utilisateurs payants du secteur commercial. Comme les organismes de sécurité publique ne seraient pas tenus d'adhérer au RLBSP, les coûts assumés par ces derniers seraient probablement élevés et pourraient nécessiter le subventionnement des frais d'utilisateurs afin d'assurer la migration des utilisateurs des réseaux existants. Au bout du compte, un faible taux d'adhésion au RLBSP compromettrait son interopérabilité, soit le principal objectif du futur RLBSP. De plus, le réseau spécialisé offrirait l'utilisation la moins efficace du spectre, alors qu'entre 90 % et 95 % de la capacité de ce dernier demeurerait inutilisée sur une base quotidienne, exception faite des cas d'urgences et d'événements d'importance majeure[45].

Bien que la recommandation du BTCN de mettre en œuvre un réseau partagé corresponde aux conclusions tirées dans le cadre de travaux semblables qu'a réalisés la communauté de la sécurité publique, il pourrait être pertinent d'examiner les

[44] Recherche et développement pour la défense Canada. Mai 2017. Bandwidth Requirements for Day-to-Day Operations on Canada's 700 MHz Public Safety Broadband, p. 7. http://cradpdf.drdc-rddc.gc.ca/PDFS/unc273/p805324_A1b.pdf
[45] Ibidem

conséquences qui s'ensuivraient si les régions adoptaient différentes approches d'utilisation du spectre[46]. Dans un second temps, on a entrepris des analyses supplémentaires afin de déterminer si une combinaison d'approches permettrait d'assurer le respect des principes du RLBSP, ainsi que d'offrir des niveaux équivalents de services et de qualité d'expérience à tous les utilisateurs du RLBSP. Si une telle approche donnait lieu à des iniquités, celle-ci pourrait compromettre la mise en œuvre nationale du RLBSP.

Modèles de prestation de services

Contexte

Il existe de nombreuses façons de mettre en œuvre le RLBSP, chacune des approches possibles étant associée à un ensemble d'acteurs et à une distribution des fonctions qui lui sont propres. Le BTCN a envisagé quatre approches de prestation de services pour le RLBSP du Canada, en comparant celles-ci en fonction de leur capacité à satisfaire aux principes du RLBSP. Les approches présentées ci-après sont de nature notionnelle, l'objectif n'étant pas de déterminer l'approche de prestation de services ou le cadre de gouvernance du RLBSP que l'on adoptera au bout du compte. À l'origine, ces modèles hypothétiques ont été élaborés par le CSS de RDDC et on les a choisis pour représenter un large éventail d'options de prestation de services.

Chaque modèle est associé à une unique entité nationale et/ou plusieurs entités régionales. Aux fins du présent rapport, les entités du réseau s'acquittent de certaines fonctions opérationnelles de réseau et pourraient aussi assumer des fonctions de gouvernance. Bien que chacun des modèles précise de quelles entités les fonctions de réseau pourraient relever, aucun d'eux ne formule de recommandations quant à la composition ou la structure de l'entité nationale et des entités régionales. De plus, même si ces entités pourraient s'acquitter de différentes fonctions de réseau selon l'un ou l'autre des modèles, rien n'empêcherait ces dernières de sous-traiter leurs opérations à un tiers.

Pour obtenir des descriptions détaillées des modèles de prestation de services, voir la figure 2 : Options des modèles de prestation de services ci-dessous ou le rapport scientifique *Implications of Service Delivery Model Options on Interoperability and Operational Efficiency in a Public Safety Mobile Broadband Network* élaboré par le CSS de RDDC[47].

Modèle A : Un réseau de la sécurité publique/un ORM national
(Ci-après appelé le « modèle A ») : Un réseau national qui serait exploité dans l'ensemble du Canada (un identifiant de

[46] Recherche et développement pour la défense Canada. Implementation models for a public safety broadband network. Avril 2017; TETRA and Critical Communications Association. A discussion on the use of commercial and dedicated networks for delivering Mission Critical Mobile Broadband Services. Février 2017; TETRA and Critical Communications Association. Mobile Broadband for Critical Communications Users – A review of options for delivering Mission Critical solutions. Décembre 2013.
[47] Recherche et développement pour la défense Canada. Mars 2017. Implications of Service Delivery Model Options on Interoperability and Operational Efficiency in a PSBN. DRDC-RDDC-2017-R038.

réseau mobile terrestre public [RMTP][48]) et qui desservirait tous les utilisateurs du RLBSP du Canada. L'ORM national pourrait être un ORM unique qui assure une couverture nationale, ou un ORM unique qui tire profit de l'infrastructure des réseaux d'accès radio (RAR) d'autres ORM afin d'offrir une couverture nationale. L'option de groupe nécessiterait la conclusion d'une entente avec tous les ORM du pays qui régirait la manière dont ils collaborent à titre de réseau unique capable d'offrir une couverture uniforme à l'échelle nationale. L'ORM national interagirait avec tous les réseaux externes et les réseaux itinérants partenaires. Il serait responsable de se conformer aux conditions de licence (CDL) d'ISDE, aux normes sur les réseaux et aux principes du RLBSP.

Modèle B : Réseaux régionaux multiples de la sécurité publique/ORM régionaux multiples
(Ci-après appelés le « modèle B ») : Les entités régionales se verraient allouer un spectre délimité par un secteur géographique particulier et chacune d'elles aurait son propre n° de RMTP. Chaque entité régionale serait responsable d'interagir avec des réseaux externes, disposerait d'ententes d'itinérance nationales et internationales, et serait tenue de se conformer aux CDL. Dans un premier temps, des normes devraient être mises en place, mais il n'y aurait pas d'organe central responsable de les gérer alors que celles-ci évoluent ou de veiller à leur application uniforme ou leur respect. Chaque entité régionale serait tenue de s'acquitter de toutes les fonctions de réseau.

Modèle C : Réseau unique de la sécurité publique/ORM régionaux multiples
(Ci-après appelé le « modèle C ») : Chaque entité régionale se verrait allouer un spectre et l'ensemble d'entre elles se partageraient un n° de RMTP. L'entité de coordination nationale serait responsable de présenter la demande de n° de RMTP. À l'instar du modèle B, les entités régionales seraient responsables d'interagir avec des réseaux externes, disposeraient d'ententes d'itinérance et seraient tenues de se conformer aux CDL et aux normes sur les réseaux. L'entité de coordination nationale serait appelée à gérer les normes alors qu'elles évoluent. Chaque entité régionale serait tenue de s'acquitter de la majorité, voire de la totalité, des fonctions de réseau.

Modèle D : Réseau unique de la sécurité publique/ORM régionaux multiples (avec opérations nationales centralisée)
(Ci-après appelé le « modèle D ») : Une entité nationale serait responsable des normes sur les réseaux, des liaisons avec les réseaux externes, des ententes d'itinérance et de certaines fonctionnalités opérationnelles de réseau. Les fonctions de réseau pourraient être consolidées au sein de l'entité nationale à des fins d'efficacité. Le spectre pourrait être alloué à l'entité nationale ou aux entités régionales.

[48] L'identifiant de RMTP est un numéro universel unique de six chiffres qui permet de distinguer un réseau mobile public d'un autre réseau mobile public dans le monde. Le n° de RMTP comprend un indicatif de pays de la station mobile (IPSM) à trois chiffres et un code de réseau mobile (CRM) à trois chiffres. Au Canada, le CRM est géré par l'Administrateur de la numérotation canadienne (ACN), sous l'autorité du CRTC. Au moment de la rédaction du présent rapport, on ne savait si l'ACN attribuerait de multiples n°s de RMTP aux entités régionales. (European Telecommunications Standards Institute [ETSI]. Technical Specification 122-101, version 15.6.0. Octobre 2018.

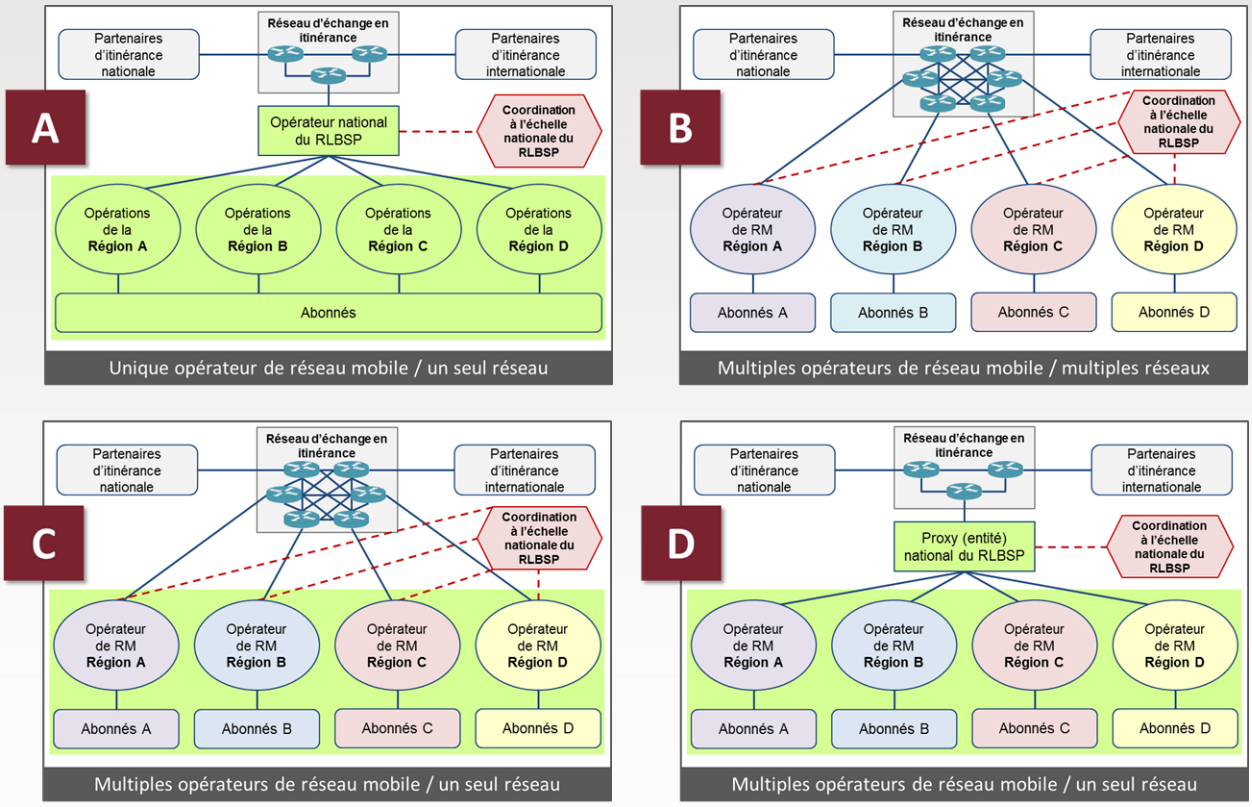

Figure 2 : Options des modèles de prestation de services[49]

Considérations

Le CSS de RDDC a élaboré les modèles A, B, C et D et les a évalués dans son rapport de 2017[50] en fonction des différences importantes qui existent entre chacun d'eux. On les a examinés dans le contexte d'un réseau partagé, comme recommandé précédemment.

Selon le modèle de réseau partagé, les utilisateurs commerciaux pourraient accéder au spectre du RLBSP, mais seuls les utilisateurs du RLBSP autorisés seraient présents sur le RLBSP. Dans les cas où le RAR serait partagé entre les utilisateurs commerciaux et les utilisateurs du RLBSP, chacun d'eux disposant de leur réseau de base, on pourrait appliquer l'architecture de réseau central multi-opérateurs.

[49] Ibidem, p. 6 à 8
[50] Recherche et développement pour la défense Canada. Mars 2017. Implications of Service Delivery Model Options on Interoperability and Operational Efficiency in a PSBN. DRDC-RDDC-2017-R038.

Analyse, risques et possibilités

Tout en tenant compte des considérations susmentionnées, le BTCN a mené une évaluation qualitative des quatre modèles possibles de prestation en fonction de leur capacité à satisfaire aux principes du RLBSP, et ce, en leur attribuant une cote de probabilité de satisfaction faible, modérée ou élevée.

Les possibilités et les défis associés à chacun des modèles sont présentés de façon de sommaire dans le tableau 4 : *Résumé de l'analyse des modèles de prestation de services*, et sont expliqués en détail ci-après.

Tableau 4 : Résumé de l'analyse des modèles de prestation de service

Légende	Probabilité élevée de satisfaction du principe (E)	Probabilité modérée de satisfaction (M)	Probabilité faible de satisfaction (F)

Modèles de prestation de services				
Principes du RLBSP évalués	**Modèle A :** Un ORM national/un réseau	**Modèle B :** PRM régionaux multiples/ réseaux régionaux multiples	**Modèle C :** ORM régionaux multiples/ un réseau unique *(aucun organe national responsable des fonctions)*	**Modèle D :** ORM régionaux multiples/ un réseau unique *(avec organe national responsable des fonctions)*
Interopérabilité	M*	F	F	E
Permanence de l'accès au réseau	E	E	E	E
Couverture	M*	E	E	E
Résilience et robustesse	M*	M	M	E
Prestation des services essentiels à la mission	E	M	M	E
Sécurité	E	M	M	E
Durabilité	M*	F	F	E
Abordabilité	M*	F	F	E

Utilisation efficace du spectre	E	E	E	E

* La cote fournie s'appuie sur l'hypothèse selon laquelle un ORM est embauché sur une base contractuelle pour offrir une couverture à l'échelle nationale. Dans les cas où l'ORM du RLBSP tire profit du RAR d'autres ORM, lorsque cela est nécessaire, la cote « modérée » (orange) passerait à une probabilité « élevée » de satisfaction (vert).

Interopérabilité : La capacité des utilisateurs d'accéder au RLBSP est essentielle à l'interopérabilité et c'est pourquoi l'accessibilité du réseau est nécessaire à l'adhésion des utilisateurs. On estime que le modèle A présente une probabilité modérée de satisfaction, car actuellement, aucun ORM n'offre une couverture nationale adéquate. Conséquemment, un ORM unique du RLBSP serait tenu d'étendre suffisamment sa propre couverture pour répondre aux besoins du RLBSP. En revanche, un ORM unique du RLBSP pourrait augmenter la couverture du RLBSP en concluant des ententes avec d'autres ORM qui disposent d'une couverture de RAR dans les endroits non couverts par l'ORM du RLBSP. Cette deuxième approche présente tout de même un risque que la couverture nationale ne soit pas assurée si aucune entente ne peut être conclue. Les deux options susmentionnées présentent un risque que les organismes de sécurité publique continuent de recourir aux services de leurs réseaux commerciaux locaux pour une multitude de raisons opérationnelles, ce qui compromettrait l'interopérabilité nationale, car les utilisateurs du RLBSP ne seraient pas en mesure d'échanger facilement des données avec les intervenants qui se servent toujours de leurs réseaux commerciaux.

Si les ORM ne pouvaient pas coopérer pour assurer une couverture à l'échelle nationale, le modèle D présenterait la probabilité la plus élevée de satisfaire au principe d'interopérabilité. Les capacités de gestion centrale des normes d'interopérabilité et d'harmonisation avec l'ORM régional le mieux outillé pour répondre aux besoins de la sécurité publique ont pour effet d'accroître la probabilité que la majorité des utilisateurs de la sécurité publique soient sur le même réseau.

Les modèles B et C présentent la plus faible probabilité de satisfaire au principe d'interopérabilité. L'utilisation de plateformes et de services propres aux ORM régionaux entraînerait des défis au chapitre de l'interopérabilité des applications et des services hébergés par le réseau si les normes ne sont pas mises en œuvre de la même manière et si les opérateurs n'acceptent pas de raccorder leurs réseaux de base. Un groupe d'ORM régionaux multiples serait par ailleurs moins apte à soutenir les utilisateurs fédéraux de l'ensemble du pays sans que la qualité intégrale et le rendement des services ne soient exposés à des complexités et des risques accrus[51]. Les modèles B et C proposent aussi des exigences supplémentaires en matière d'ententes d'itinérance nationales et internationales (p. ex. on devrait conclure et gérer jusqu'à 210 ententes en comparaison avec 36 pour les modèles A et D).

[51] Ibidem, p. 19

Permanence de l'accès au réseau : On estime que tous les modèles présentent une probabilité élevée de satisfaction, car le modèle de prestation de services n'a pas d'incidence sur la capacité d'accès au réseau.

Couverture : On estime que les modèles B, C et D présentent une probabilité élevée d'assurer la couverture maximale possible, car la ou les relations avec le ou les ORM seraient établies à l'échelle régionale, ce qui offrirait davantage de souplesse régionale. Les modèles B, C et D pourraient aussi permettre de tirer profit plus facilement des relations contractuelles ou organisationnelles en place en vue d'accéder aux infrastructures provinciales, régionales ou municipales, et ce, dans le but d'étendre la couverture du RLBSP aux ORM.

Le modèle A présente une probabilité modérée de satisfaction, car un réseau national unique n'aurait pas les relations avec les organismes provinciaux, régionaux et municipaux qui sont requises pour facilement tirer profit des infrastructures et augmenter la couverture. De plus, actuellement, aucun ORM n'assure une couverture nationale adéquate, ce qui signifie que certaines régions du pays n'auraient pas accès aux services du RLBSP, à moins que les ORM coopèrent pour offrir une couverture uniforme à l'échelle nationale ou que de nouveaux investissements soient réalisés afin de pallier les lacunes dans les régions pour lesquelles l'analyse de rentabilisation a généré des résultats jugés faibles par le passé.

Résilience et robustesse : On estime que le modèle D présente la capacité de résilience et de robustesse la plus élevée. Celui-ci commande une coordination nationale hautement efficace en vue d'offrir un réseau national résilient tout en ayant certaines redondances à l'échelle régionale afin de limiter les incidences sur le réseau.
On estime que les modèles B et C présentent la probabilité la plus faible de répondre aux exigences de résilience nationale, bien que leur résilience locale ou régionale puisse être acceptable. Vu l'absence de coordination nationale dans les modèles B et C, ces derniers présentent un risque plus élevé que le réseau national ne soit pas suffisamment résilient en comparaison avec les modèles A et D. On estime que le modèle A, à titre de réseau unique, offre moins de résilience. Les incidences sur le réseau pourraient se faire sentir plus facilement dans l'ensemble du réseau national et nécessiteraient des investissements dans les capacités redondantes en comparaison avec les modèles B, C et D qui ont certaines redondances à l'échelle régionale.

Prestation des services essentiels à la mission : Les modèles A et D présentent une probabilité élevée de satisfaction, car la présence d'une entité de coordination à l'échelle nationale favoriserait l'évolution de la technologie et garantirait la prestation uniforme des services essentiels à la mission. Dans les cas où de multiples réseaux existent, comme dans les modèles B et C, on se heurte à un degré accru de complexité au chapitre de la coordination de la technologie et des normes relatives au réseau.

Sécurité : Les modèles A et D présentent la probabilité la plus élevée de répondre aux normes de sécurité, car il est plus facile de mettre en œuvre des normes de réseau et de sécurité au sein d'un réseau unique.

Les modèles B et C auraient davantage de difficulté à soutenir les utilisateurs fédéraux ou tous autres utilisateurs qui mènent leurs activités dans différentes régions. Ceci s'appliquerait particulièrement aux solutions de réseaux privés virtuels (RPV) mobiles que les réseaux multiples des modèles B et C auraient beaucoup de difficulté à soutenir.

Durabilité : De façon générale, la complexité et les coûts associés à l'établissement et au maintien de l'interopérabilité durant le cycle de vie d'un RLBSP sont fonction du nombre d'acteurs dans la sphère de prestation de services et du nombre de fournisseurs au sein du RLBSP[52]. On estime que le modèle D présente la probabilité la plus élevée d'assurer la durabilité du réseau en raison de la souplesse offerte dans la manière dont il peut être mis en œuvre. À titre d'exemple, les régions pourraient travailler de concert pour partager les ressources et certaines fonctions de réseau pourraient être centralisées, si possible, afin de réduire les coûts. On pourrait aussi atténuer les coûts et la complexité associés à l'itinérance si les régions agissaient en tant que réseau unique. On reconnaît que le marché du RLBSP n'est pas uniforme à l'échelle du pays et, conséquemment, les entités régionales indépendantes pourraient disposer de capacités variées au chapitre de la durabilité.

On estime que le modèle A présente une probabilité modérée de satisfaction. Celui-ci commanderait un investissement de capitaux en vue d'étendre la couverture aux régions où la couverture de l'ORM est déficiente. Cela dit, si un groupe d'ORM pouvait coopérer pour offrir une meilleure couverture nationale, le modèle A offrirait plus de durabilité que le modèle D.

On estime que les modèles B et C offrent les moyens les moins durables d'assurer la prestation de services mobiles à large bande. Ils commanderaient des dépenses considérables d'exploitation et d'immobilisations en raison des nombreux cas où les mêmes ressources de réseaux seraient requises pour créer et maintenir plusieurs différents réseaux de sécurité publique. Comme susmentionné, la nécessité de mettre en place et de gérer un nombre exponentiel d'ententes d'itinérances aurait pour effet d'augmenter la complexité et les risques. Le modèle C présente aussi une complexité accrue du fait qu'il nécessiterait la conclusion d'une entente d'itinérance hors-norme qui entraînerait des coûts initiaux supplémentaires et potentiellement des coûts continus. Toutefois, certains coûts et éléments de complexité seraient atténués si plusieurs régions travaillaient ensemble afin d'agir en tant que réseau unique.

Abordabilité : Les modèles A et D présentent une probabilité élevée de satisfaire au principe de l'abordabilité, car leurs structures plus centralisées permettraient de réduire les coûts qui ne peuvent être atténués de façon semblable dans les

[52] Centre des sciences pour la sécurité de Recherche et développement pour la défense Canada. Avril 2017. Implementation models for a public safety broadband network, p. 8.

modèles B et C. Conséquemment, on estime que les modèles B et C sont les moins abordables, ceux-ci présentant des degrés élevés de chevauchement et de complexité, dont les coûts associés devront être assumés au bout du compte par les utilisateurs de la sécurité publique.

Utilisation efficace du spectre : Selon l'hypothèse voulant que le RLBSP s'appuie sur une approche de spectre partagé, les modèles A à D présenteraient une probabilité élevée d'assurer une utilisation efficace du spectre.

Approches des modèles de prestation de services

Bien qu'il soit possible de mettre en œuvre un RLBSP en appliquant chacun des modèles de prestation de services évalués, l'analyse comparative démontre que chacun d'entre eux présente différents risques et différentes possibilités, notamment en ce qui concerne le respect des principes du RLBSP. À la lumière de ces risques et possibilités, le BTCN estime que l'approche des modèles A et D représente la meilleure solution d'exploitation du futur RLBSP.

La principale faiblesse du modèle A est l'absence d'un ORM bien établi qui assure une couverture nationale adéquate pour les utilisateurs du RLBSP de l'ensemble du pays. Pour combler les lacunes en matière de couverture, il faudra réaliser des investissements qui au bout du compte auront une incidence sur la durabilité et l'abordabilité. L'option selon laquelle l'ORM du RLBSP assurerait une couverture dans les régions mal desservies par l'entremise d'ententes d'accès à l'infrastructure de RAR d'autres ORM dépend de la disposition des ORM de RAR à conclure des accords avec l'ORM du RLBSP. Il n'y a aucune certitude à ce chapitre. Le modèle D devient le meilleur modèle en l'absence de la capacité à réunir un groupe d'ORM pour former le modèle A.

Le modèle D est celui à privilégier, car il permet d'offrir la meilleure zone de couverture régionale tout en fonctionnant à titre de réseau national unique. Cette approche permettrait d'assurer une interopérabilité nationale et la conformité aux autres principes du RLBSP tout en offrant un réseau durable et abordable.

L'analyse comparative démontre que les modèles B et C ne seraient pas en mesure de satisfaire aux principes du RLBSP. La structure de réseaux multiples dotée de peu de structures nationales de coordination et de soutien, voire aucune, pose un risque relativement à l'interopérabilité et la capacité à soutenir les utilisateurs fédéraux. De plus, une structure plus complexe entraîne des coûts supplémentaires pour les intervenants participants.

Évaluations des approches de mise en œuvre mixte

Une mise en œuvre mixte du RLBSP présente les risques supplémentaires décrits ci-après.

Mise en œuvre des principes et des normes applicables au RLBSP : Des normes devraient être élaborées à partir des principes du RLBSP. Dans le cas où coexistent de multiples RLBSP indépendants, et qu'il n'y a aucune coordination ou

direction globale, il est probable que des normes (identiques ou différentes) seraient mises en œuvre de différentes façons dans l'ensemble du pays. Cela aurait pour effet d'accroître le risque de non-satisfaction des principes, comme l'interopérabilité et la sécurité, et présenterait des défis considérables pour les utilisateurs (les utilisateurs fédéraux en particulier) qui, conséquemment, ne peuvent ou ne veulent pas adhérer au RLBSP.

Expérience commune des utilisateurs : On tient pour acquis que les utilisateurs et les organismes du RLBSP présenteront des capacités variées de mise en œuvre du RLBSP au sein de leurs administrations respectives. Certaines municipalités et organisations régionales seront disposées et aptes à investir le capital et les fonds opérationnels requis pour mettre en place un RLBSP spécialisé ou partagé, par l'entremise de la bande 14, à l'échelle locale ou régionale. Les administrations qui ne sont pas en mesure d'engager les ressources financières requises seront désavantagées, ce qui accentuera les inégalités entre les utilisateurs et les prestataires potentiels du RLBSP national.

Interopérabilité : Certains utilisateurs de la sécurité publique continueront de faire appel à des fournisseurs commerciaux pour les raisons suivantes : aucun service du RLBSP n'est accessible, ils préfèrent leurs fournisseurs de services actuels ou ont des obligations envers eux, ou les services RLBSP sont pour eux inabordables. Les ORM en concurrence pourraient offrir des services semblables à ceux du RLBSP, comme l'accès prioritaire et les droits de préemption, et ce, moyennant des frais supplémentaires afin de rivaliser avec le RLBSP dans certaines régions. L'interopérabilité des communications vocales demeurerait la même dans les régions qui bénéficient d'une interopérabilité des communications vocales de RMT. L'interopérabilité des données varierait selon les administrations ou les disciplines (p. ex. services de police, d'incendie ou d'ambulanciers, infrastructures essentielles, etc.), selon l'accessibilité des services du RLBSP, et les organismes qui utilisent les services du RLBSP relativement à ceux qui utilisent des services commerciaux.

Durabilité et abordabilité : La durabilité et l'abordabilité globales du RLBSP seraient compromises si différents îlots du RLBSP étaient mis en œuvre un peu partout au pays. Dans les régions où le spectre de la bande 14 est largement prisé sur le plan commercial, le RLBSP sera plus durable et pourrait ne nécessiter que peu de financement public supplémentaire, voire aucun. Cela dit, dans les régions où le spectre de la bande 14 n'est pas aussi prisé, on pourrait être tenu de s'appuyer sur un financement public à long terme. De plus, un manque de coordination pourrait entraîner un chevauchement des infrastructures de réseau et du capital humain qui sont nécessaires pour exploiter et gérer le réseau.

Utilisation du spectre : On estime que dans les réseaux spécialisés, les utilisateurs du RLBSP n'utiliseraient qu'un maximum de 10 % du spectre de 20 MHz dans le cadre de leurs opérations quotidiennes[53]. Ainsi, si l'on appliquait une

[53] Centre des sciences pour la sécurité de Recherche et développement pour la défense Canada. Mai 2017. Bandwidth Requirements for Day-to-Day Operations on Canada's 700 MHz Public Safety Broadband, p. 7. http://cradpdf.drdc-rddc.gc.ca/PDFS/unc273/p805324_A1b.pdf

approche de mise en œuvre fragmentée, il est possible que le spectre soit utilisé de manière inefficace dans certaines régions du pays en comparaison avec d'autres qui soutiennent l'usage commercial et celui de la sécurité publique.

Structure de délivrance de licences

Contexte

Tel qu'il a été mentionné précédemment dans le présent rapport, ISDE a rendu les décisions suivantes au sujet de la délivrance de licences d'utilisation du spectre à large bande de la sécurité publique de 700 MHz[54].

D-1	Le spectre dans les bandes de 758 à 763 MHz et de 788 à 793 MHz (bloc D) est désigné aux fins d'utilisation de la large bande par la sécurité publique.
D-2	Le spectre dans ces bandes ne sera pas mis aux enchères.
D-3	Les licences de spectre seront délivrées soit directement à une ou à plusieurs ERSP; cet aspect est à déterminer à une date ultérieure.
D-4	L'utilisation commerciale de la capacité inutilisée sera permise pourvu que les utilisateurs de la sécurité publique aient la priorité et des droits de préemption sur toute forme d'utilisation commerciale.
D-5	ISDE n'imposera pas de technologie particulière, toutefois, toute technologie employée pour le spectre à large bande destiné à la sécurité publique dans la bande de 700 MHz doit assurer une interopérabilité nationale et transfrontalière, garantir la priorité et la préemption pour les services de sécurité publique, et se conformer à la solution d'interopérabilité relative au « partage des systèmes fondés sur les normes ».

ISDE devrait mener des consultations supplémentaires à propos du cadre de délivrance de licences d'utilisation de la bande 14 avant de délivrer de telles licences.

Hypothèses

Outre les décisions présentées ci-haut, les hypothèses qui suivent s'appliquent à l'analyse de la structure de délivrance de licences d'utilisation du futur RLBSP :

- On mettra en place des normes nationales qui se fondent sur les principes du RLBSP afin d'assurer une expérience uniforme et équitable des utilisateurs à l'échelle du pays;

[54] Innovation, Sciences et Développement économique Canada. Juin 2017. Décisions se rapportant au cadre politique, technique et de délivrance de licences pour l'utilisation du spectre à large bande destiné à la sécurité publique, et ce, dans les bandes de 758 à 763 MHz et de 788 à 793 MHz (bloc D), ainsi que de 763 à 768 MHz et de 793 à 798 MHz (bloc SPLB). https://www.ic.gc.ca/eic/site/smt-gst.nsf/fra/sf11289.html

- Le réseau s'appuiera sur approche d'utilisation de spectre partagé;
- On utiliserait une combinaison d'ententes de délivrance de licences et d'ententes contractuelles pour garantir la satisfaction des principes du RLBSP.

Considérant ces hypothèses, le BTCN envisage les approches de délivrance de licences présentées ci-après.

Licence octroyée à l'échelle nationale et aucune sous-licence : Le titulaire de licence nationale serait l'unique responsable de la prestation des services du RLBSP et pourrait conclure des contrats de sous-traitance, au besoin. Cette structure de délivrance de licences correspond au modèle A de prestation de services : Un réseau de la sécurité publique/un ORM national commercial.

Licence principale octroyée à l'échelle nationale et sous-licences à l'échelle régionale : Le titulaire de licence nationale pourrait conclure des ententes avec des sous-titulaires de licence, lesquels seraient tous tenus de servir la communauté de la sécurité publique. Les ententes contractuelles seraient appliquées parallèlement aux CDL afin de garantir le respect des principes et des normes applicables au RLBSP. Une telle structure de délivrance de licences correspond au modèle D de prestation de services : ORM régionaux multiples/un réseau unique.

Multiples licences octroyées à l'échelle régionale : Les titulaires de licences régionales seraient responsables de la prestation des services du RLBSP dans leurs régions respectives et devraient adhérer aux normes nationales qui s'appliquent au RLBSP. La structure de délivrance de licences est applicable dans le cas des modèles de prestation de services B, C et D, lesquels prévoient de multiples ORM régionaux.

ISDE est l'autorité suprême en ce qui concerne le régime de délivrance de licences et l'on mènera un processus distinct pour élaborer un cadre de délivrance de licences de la bande 14. Le BTCN se penche donc sur les incidences que les approches de délivrance de licences pourraient avoir sur la satisfaction des principes du RLBSP et traitera de ce sujet de manière plus approfondie dans le document de politique.

Utilisation commerciale de la capacité excédentaire

Dans son document de décisions de 2017, ISDE affirmait ce qui suit : « L'utilisation commerciale de la capacité inutilisée sera permise pourvu que les utilisateurs de la sécurité publique aient la priorité et des droits de préemption sur toute forme d'utilisation commerciale[55] ». Par l'entremise de consultations continues avec les fournisseurs de service et les

[55] Ibidem

fabricants, le BTCN poursuit l'élaboration de ses recommandations à l'égard du partage de la capacité inutilisée du spectre de la bande 14 avec les utilisateurs commerciaux.

Comme on le précise dans le document « Description de l'architecture du RLBSP » publié par le CSS de RDDC en 2019, le trafic commercial de la bande 14 passerait exclusivement par le réseau de base commercial. Cela signifie que le trafic commercial et le trafic de la sécurité publique seraient distincts l'un de l'autre lorsque tous les deux utilisent le spectre de la bande 14. Cette approche a pour effet de dissiper les inquiétudes en matière de sécurité et de confidentialité de la communauté de la sécurité publique pour ce qui est d'assurer la protection et la sécurité des données et des informations qui sont transportées par l'entremise du réseau.

Aux États-Unis, la First Responder Network Authority a conclu un contrat de location avec leur partenaire de réseau commercial, lequel permet la commercialisation du spectre désigné avec accès prioritaire et droits de préemption. Cette entente n'a pas eu d'incidences négatives sur l'expérience des utilisateurs de FirstNet. Selon certaines estimations, exception faite des cas d'urgence, l'utilisation quotidienne des organismes de sécurité publique permettra l'utilisation à des fins commerciales d'une portion importante (inutilisée) du spectre[56].

Certaines régions rurales et éloignées continuent de se heurter à un accès limité à la large bande en raison de l'analyse de rentabilisation peu concluante sur le déploiement du secteur privé dans ces régions. L'utilisation partagée du spectre de la bande 14 dans les collectivités rurales et éloignées pourrait offrir une meilleure couverture du RLBSP, et ce, tout en favorisant l'amélioration de l'accès au dernier kilomètre à la large bande des utilisateurs des collectivités rurales et éloignées.

Les exploitants de services publics utilitaires et d'autres infrastructures ont également relevé des synergies supplémentaires avec le RLBSP et ont exprimé leur intérêt à tirer profit du spectre de la bande 14 en vue de soutenir des exigences de communications essentielles à la mission. Ces partenaires potentiels du RLBSP pourraient offrir une précieuse infrastructure de communication, et ainsi accélérer le déploiement et augmenter la zone de couverture du RLBSP.

Le BTCN continuera donc d'évaluer la possibilité que le spectre de la bande 14 soit mis à profit à titre de contribution en nature en vue de subventionner les investissements dans le RLBSP, particulièrement en ce qui concerne l'établissement et l'amélioration de la couverture, le renforcement de la résilience du réseau ou la réduction des obstacles financiers potentiels qui pourraient compromettre l'adoption répandue des utilisateurs de la sécurité publique.

[56] Trefis Team. How Much Does AT&T Stand to Gain from FirstNet? Forbes. 12 décembre 2017. https://www.forbes.com/sites/greatspeculations/2017/12/12/how-much-does-att-stand-to-gain-from-firstnet/#78dae0772997

Le BTCN continuera également d'examiner les possibilités qui se dégagent de l'élaboration de nouvelles utilisations du spectre et façons de gérer la bande 14 qui permettent de satisfaire le plus efficacement aux principes du RLBSP. Alors que se poursuit l'analyse du document de politique, le BTCN évaluera l'incidence de ses propositions sur la valeur commerciale du spectre de la bande 14, lesquelles pourraient soutenir ou limiter les analyses de rentabilisation potentielle.

Prochaines étapes

Le présent rapport d'étape peut servir de document de référence, de sorte que les propositions avancées par le BTCN s'harmonisent avec les besoins des utilisateurs de l'ensemble du pays, tout en étant viables pour tous les intervenants. L'objectif est de veiller à ce que les intervenants soient en mesure d'utiliser le RLBSP pour améliorer leurs capacités de communication dès que possible. Les intervenants sont encouragés à examiner les recommandations ci-incluses et à soumettre leurs points de vue et commentaires au BTCN.

Le BTCN continuera de solliciter la participation des partenaires, des intervenants, des experts et des utilisateurs FPT afin d'améliorer les options qu'il formule à propos des principes, de la mise en œuvre et de la prestation de service. Un document de politique sera présenté au début 2020 aux ministres FPT responsables de la gestion des urgences. Le BTCN continuera également de se pencher sur les considérations supplémentaires suivantes :

- Examiner et définir de façon plus approfondie les objectifs associés aux principes du RLBSP;
- Décrire le marché potentiel du RLBSP au Canada;
- Déterminer les besoins des utilisateurs fédéraux;
- Analyser les modèles de financement potentiel du RLBSP en vue d'évaluer la viabilité pour tous les intervenants et déterminer la ou les offres les plus susceptibles de satisfaire aux principes du RLBSP;
- Définir les exigences en matière de gouvernance, ainsi que proposer des rôles et des relations s'inscrivant dans le déploiement, les opérations et l'évolution du réseau en se penchant sur les divers intérêts des intervenants du RLBSP.

Importance des actions coordonnées

Le RLBSP se veut une solution technologique qui permettra d'atténuer les silos de communication des données par l'entremise d'un réseau canadien sécurisé qui est accessible à tous les premiers intervenants. Si un RLBSP était mis en œuvre de manière non coordonnée, le BTCN estime que cela entraînerait des répercussions négatives sur les premiers intervenants et les citoyens du Canada. D'abord et avant tout, une approche fragmentée ou mal coordonnée aurait pour

effet d'accentuer le risque d'iniquités au sein et entre les groupes d'intervenants. De telles iniquités vont à l'encontre des principes fondamentaux du RLBSP et pourraient conséquemment compromettre l'intégrité et la réussite du réseau à l'échelle nationale.

Priorités du gouvernement relatives à la large bande en milieu rural

Des annonces budgétaires récentes du gouvernement du Canada et d'un certain nombre de provinces et territoires comprennent des propositions d'investissements considérables dans l'expansion des services Internet à haute vitesse et des services mobiles. À titre d'exemple, le budget fédéral de 2019 proposait un investissement de 1,7 milliard de dollars sur 13 ans afin de « compléter » le financement du programme *Brancher pour innover*; d'établir le *Fonds pour la large bande universelle*; et de garantir la capacité de pointe des satellites en orbite basse afin de desservir les régions les plus rurales et les plus éloignées du Canada. *L'incitatif à l'investissement accéléré* aura aussi pour effet d'encourager des investissements accrus de la part du secteur privé dans l'Internet haute vitesse des régions rurales et éloignées, alors que jusqu'à maintenant, des entreprises de télécommunications ont signalé plus de 1 milliard de dollars en activité du secteur privé. Cet incitatif devrait favoriser la concurrence dans le secteur des télécommunications en ce qui concerne les technologies actuelles et émergentes. Les investissements dans la large bande en milieu rural soutiendront l'amélioration des communications à large bande sans fil, ce qui facilitera le déploiement du RLBSP.

À l'échelle provinciale, la Saskatchewan a proposé un investissement de capitaux de 321 millions de dollars en vue de moderniser les réseaux de SaskTel, et le Québec a proposé un investissement de 400 millions de dollars sur 7 ans pour améliorer l'Internet à haute vitesse et l'accès cellulaire dans les régions éloignées. De même, dans son discours du Trône de 2019, l'Alberta a promis d'investir dans une stratégie sur la large bande dans les milieux ruraux.

Ces annonces sont des signes positifs comme quoi la connectivité à large bande à l'échelle nationale est une priorité à de nombreux degrés dans l'ensemble du pays, ce qui pourrait contribuer à rehausser le positionnement d'un RLBSP au Canada. De plus, il pourrait y avoir des liaisons possibles à d'autres secteurs qui devraient faire l'objet de l'évaluation du RLBSP national. Le BTCN continuera donc d'assurer un suivi des progrès accomplis dans le cadre des initiatives existantes et proposées afin de tirer profit des possibilités offertes par les investissements complémentaires.

Définitions

Terme	Définition
Accès au réseau	Capacité à accéder directement au RLBSP des services essentiels à la mission.
Bande 14	Un bloc de fréquences apparié de 10 +10 MHz dans les bandes 758-763 MHz et 788-793 MHz (bloc D) et 763-768 MHz et 793-798 MHz (bloc PSBB).
Bureau national de coordination temporaire	Bureau mis sur pied par le gouvernement du Canada et ayant pour mandat d'assurer un rôle de leadership dans l'avancement d'un RLBSP national et interopérable au Canada.
Capacité du réseau	La quantité maximale de données qui peuvent être transmises entre différents points du réseau par l'entremise d'un circuit de liaison ou d'un chemin du réseau.[57]
Conditions de licence	Les conditions qu'impose ISDE aux titulaires de licences en échange du droit d'utilisation du spectre.
Couverture	La couverture réseau peut être établie en ciblant un pourcentage de la population qui réside dans la zone de couverture ou en fixant un objectif de couverture d'une superficie terrestre ou d'une longueur de route couverte par le réseau. La couverture réseau sans fil peut être étendue de façon temporaire en utilisant des capacités pouvant être déployées dans une zone d'incident localisée ou en ayant recours à l'itinérance à l'échelle de plusieurs réseaux.
Durcissement	Collection d'outils, de techniques et de pratiques exemplaires que l'on utilise pour atténuer la vulnérabilité à une ou plusieurs menaces.
Entité nationale	Entité juridique qui appliquera les principes du RLBSP et qui sera responsable des fonctions opérationnelles de réseau ou des fonctions de gouvernance, selon le modèle de prestation de services choisi.
Entité régionale	Entité juridique qui représentera directement le RLBSP auprès des organismes de sécurité publique des régions ou des administrations municipales et assurera les fonctions de gouvernance et les fonctions opérationnelles de réseau que n'assume par l'entité nationale.
Infrastructures	On entend par infrastructures essentielles l'ensemble des processus, des

[57] https://www.techopedia.com/definition/18179/capacity-network (uniquement en anglais)

essentielles	systèmes, des installations, des technologies, des réseaux, des biens et des services nécessaires pour assurer la santé, la sûreté, la sécurité ou le bien-être économique des Canadiens et des Canadiennes ainsi que le bon fonctionnement des gouvernements. Les infrastructures essentielles peuvent être autonomes ou interconnectées et interdépendantes dans les administrations provinciales, territoriales ou nationales ou entre celles-ci. Les perturbations des infrastructures essentielles peuvent entraîner des pertes de vie catastrophiques et avoir des effets néfastes sur l'économie.[58]
Interopérabilité	Capacité du personnel d'urgence de communiquer entre les administrations, les disciplines et les ordres de gouvernement au moyen de systèmes divers, au besoin et en fonction des autorisations. Cela inclut l'atteinte d'une opérabilité nationale totale au moyen d'identifiants d'utilisateur courants sans égard au mode de déploiement du réseau ainsi qu'à l'interopérabilité du RLBSP avec les services de radio mobile à court et à moyen terme. On peut également assurer l'interopérabilité des données à l'échelle de l'application.
Itinérance	Capacité d'un utilisateur du RLBSP à recevoir automatiquement des services, y compris des services de données, lorsqu'il se déplace à l'extérieur de la zone géographique de son réseau à domicile, au moyen d'un réseau de déplacement.
Numéro d'identification de réseau mobile terrestre public (no de RMTP)	Code universel unique d'identification (3GPP – Globally unique network identification code)
Opérateur de réseau mobile	Les fournisseurs de service sans fil et de réseaux sans fil, ainsi que les entreprises de communication sans fil et de téléphonie cellulaire sont des fournisseurs de services de communication sans fil qui possèdent ou qui contrôlent tous les éléments nécessaires pour vendre ou offrir des services à un utilisateur final : une infrastructure de réseau sans fil, une infrastructure de liaisons terrestres, des services de facturation, des services à la clientèle, des systèmes informatiques, et des organisations de marketing et de réparation.
Préemption	Droit utilisé en combinaison avec le droit d'accès prioritaire pour contrôler l'utilisation des ressources en annulant les sessions actives d'utilisateurs de priorité moindre et permettre l'allocation des ressources à des utilisateurs de priorité supérieure, et ce, lorsque les ressources d'un réseau sont rares ou utilisées à plein rendement.

[58] Sécurité publique Canada. 2009. Stratégie nationale sur les infrastructures essentielles.

Prestation de services	Approche de prestation de services mobiles à large bande aux utilisateurs du RLBSP.
Priorité	Mécanisme par lequel les utilisateurs, les applications, les flux de trafic ou les paquets individuels ont préséance sur d'autres pour assurer un service ou envoyer des paquets de données lors de périodes de congestion du réseau.
Qualité de service	Mécanismes de hiérarchisation du trafic et de contrôle des ressources utilisés pour atteindre les degrés souhaités de rendement en matière de flux de données.
Radio mobile terrestre	Systèmes de communication sans fil communément utilisé par les premiers intervenants d'urgence pour soutenir la communication de données vocales et de données en faible débit.
Réseau d'accès radio	Technologie qui permet de connecter des appareils individuels à d'autres parties d'un réseau au moyen de connexions radio.
Résilience	Capacité du réseau à fournir et à maintenir un niveau de service acceptable compte tenu des diverses défectuosités et difficultés liées à l'exploitation normale d'un réseau. L'infrastructure résiliente du RLBSP serait consolidée pour faire face aux menaces telles que les pannes de courant, les inondations, les secousses sismiques, le terrorisme et le vandalisme et, en cas de panne, pour rétablir rapidement les capacités de communication.
Sécurité	Capacité de protéger et de sécuriser l'infrastructure physique du réseau et de prévenir les actes malveillants tels que les cyberattaques au niveau du serveur ou des applications.
Services essentiels à la mission (MC Services)	Les services essentiels à la mission (MC Services) renvoient aux normes définies dans le 3GPP, y compris celles s'appliquant aux appareils à bouton de microphone essentiels à la mission (MCPTT), aux données essentielles à la mission (MCData) et aux vidéos essentiels à la mission (MCVideo). On décrit ces normes et leur évolution dans les publications Rel-13, Rel-14 et Rel-15 du 3GPP.
Services essentiels à la mission	L'ensemble des activités, des appareils, des services et des systèmes dont la défaillance ou l'interruption entraînera un arrêt ou une dégradation sévère des opérations peuvent être qualifiés d'essentiels à la mission. Dans le contexte de la communauté de la sécurité publique et du RLBSP, il s'agirait de tous les aspects des services de communication essentiels dont dépend un utilisateur donné dans le cadre de ses activités quotidiennes, de situations d'urgence et

	d'événements planifiés.
Spectre	Fréquences radio par l'entremise desquelles les données sans fil sont transmises. Le spectre utilisé à des fins de communication est réglementé par des organismes nationaux qui déterminent quelles plages de fréquences peuvent être utilisées, et ce, par qui et dans quel but.
Systèmes déployables	Systèmes portatifs qui sont temporairement installés dans la nature et qui fournissent des services sans fil au moyen d'équipement LTE. Plusieurs systèmes déployables peuvent être liés les uns aux autres pour desservir une région plus grande. Les systèmes déployables peuvent avoir ou non des liaisons terrestres. Ces systèmes peuvent être de taille suffisamment petite pour être transportés par une personne ou remorqués par un véhicule, ou il peut s'agir de systèmes montés ou même aéroportés.
Technologie d'évolution à long terme (LTE)	Norme de communication sans fil à haute vitesse applicable aux appareils et terminaux de données mobiles.
Trois services	Toutes les organisations du Canada qui fournissent des services de police, de protection et de lutte contre les incendies et d'ambulancier paramédical, ceux-ci étant représentés par l'Association canadienne des chefs de police (ACCP), l'Association canadienne des chefs de pompiers (ACCP) et Chefs paramédics du Canada (CPC).
Utilisateurs	Les utilisateurs du RLBSP peuvent être des organismes d'utilisateurs finaux de sécurité publique, des gouvernements ou des ministères, ou des personnes.
Utilisateurs commerciaux	Utilisateurs des ORM qui n'assument pas de rôle en matière de sécurité publique.
Utilisateurs du RLBSP	Personnes, entités ou organismes, et leurs appareils, qui assument un rôle ou une responsabilité au chapitre de la santé, de la sûreté et de la sécurité du public et ses infrastructures qui accèdent au réseau.

Acronymes

Acronyme	Définition
3GPP	Projet de partenariat de 3e génération (Third Generation Partnership Project)
4G	Quatrième génération
5G	Cinquième génération
9-1-1 de PG	Services 9-1-1 de prochaine génération
ANC	Administrateur de la numérotation canadienne
BTCN	Bureau temporaire de coordination nationale
CANUS	Canada – États-Unis
CDL	Conditions de licence
CRM	Code de réseau mobile
CRTC	Conseil de la radiodiffusion et des télécommunications canadiennes
CSS de RDDC	Centre des sciences pour la sécurité de Recherche et développement pour la défense Canada
DHS	Department of Homeland Security
DR	Demande de renseignements
EN	Entité nationale
ER	Entité régionale
ERMV	Exploitant de réseaux mobiles virtuels
ERSP	Entité du réseau de sécurité publique
EU	Équipement de l'utilisateur
FPT	Fédéral-provincial-territorial

GC	Gouvernement du Canada
GE	Gestion des urgences
GTI	Groupe de travail sur l'interopérabilité
IoPST	Internet des objets de la sécurité publique
IPSM	Indicatif de pays de la station mobile
ISDE	Innovation, Sciences et Développement économique Canada
LTE	Technologie d'évolution à long terme
MHz	Mégahertz
MIA	Module d'identification d'abonné
MOCN	Réseau de base partagé par plusieurs opérateurs (Multi-Operator Core Network)
MSIN	Numéros d'identification d'abonnement mobile (Mobile Subscription Identification Numbers)
No de RMTP	Numéro d'identification de réseau mobile terrestre public
ORM	Opérateur de réseau mobile
QPP	Qualité du service, accès prioritaire et préemption
QS	Qualité du service
RAR	Réseau d'accès radio
RB	Réseau de base
RLBSP	Réseau à large bande pour la sécurité publique
RPV	Réseau privé virtuel
RTM	Radio mobile terrestre
SEM	Services essentiels à la mission

SICC	Stratégie d’interopérabilité des communications pour le Canada
SNAP	Système national d’alertes au public
SPLB	Large bande destinée à la sécurité publique
SPSF	Service prioritaire sans fil
TIC	Technologies de l’information et de la communication
UIT	Union internationale des télécommunications