

Envoyé en préfecture le 23/12/2024

Reçu en préfecture le 23/12/2024

Publié le 23/12/2024

ID : 971-219711231-20241220-2024065CT-DE

Berser
Levisuit



RÉPUBLIQUE FRANÇAISE
**COLLECTIVITÉ
DE SAINT-BARTHÉLEMY**

SCHÉMA LOCAL DE RÉSILIENCE DE SAINT-BARTHÉLEMY

Table des matières

synthèse	4
introduction	7
1. phase 1 – phase préparatoire	8
2. phase 2 – audit territorial.....	9
2.1. Des vulnérabilités identifiées sur le territoire	9
2.2. Des dispositifs opérationnels en cas d'évènements majeurs	18
2.2.1. Un Centre Opérationnel Territorial au service de la gestion de crises	18
2.2.2. Des solutions télécom opérationnelles pour la Collectivité	19
2.3. Des réseaux résilients pour lutter contre les vulnérabilités du territoire	20
2.3.1. Des systèmes de câbles sous-marins contribuant à la résilience du territoire.....	20
2.3.2. Des réseaux de fibres optiques résilients couvrant l'intégralité du territoire... ..	25
2.3.3. Un réseau LoRaWAN en cours de déploiement.....	33
2.3.4. Des carences identifiées sur le réseau mobile	33
2.3.5. Un projet d'IXP sur Saint-Barthélemy motivé par la coopération régionale....	33
2.3.6. Un réseau électrique résilient	35
2.4. Des dispositifs de sécurité informatique de la collectivité à améliorer.....	37
2.4.1. Des risques informatiques identifiés	37
2.4.2. Une prise en considération de la sécurité des données	39
2.4.3. Des mesures de sécurité logique	40
2.4.4. Des procédures d'accès physique en place	40
2.4.5. Une absence de processus de continuité de l'activité	40
2.4.6. L'agence Caribéenne pour la Cybersécurité, une réponse au risque cyber... ..	40
3. phase 3 – des solutions et des scénarios d'intervention pour améliorer la résilience	42
3.1. Des outils numériques au service de la réduction des risques de catastrophes	42
3.1.1. Développer les systèmes d'alerte à la population	42
3.1.2. La création d'un centre de veille pour une meilleure résilience	43
3.2. Améliorer le niveau de résilience des réseaux	45
3.2.1. Le devenir et l'amélioration des systèmes de câbles sous-marins.....	45
3.2.2. L'évolution des réseaux de fibre optique	47
3.2.3. Vers un réseau mobile plus résilient.....	49
3.2.4. Le point d'échange SBH-IX à exploiter pour une meilleure résilience.....	50
3.2.5. Poursuivre l'amélioration du niveau de résilience du réseau électrique.....	51
3.3. Renforcer la sécurité informatique de la Collectivité	52
3.3.1. La construction d'un Schéma directeur des systèmes d'information - SDSI ..	52

3.3.2.	La mise en place d'un plan de reprise d'activité et plan de continuité d'activité - PRA / PCA	52
3.3.3.	Une collaboration au service de la sécurité informatique des acteurs du territoire	52
3.3.4.	Vers une amélioration du traitement des données de la Collectivité	53
3.3.5.	Des locaux accueillant les opérateurs et hébergeant les données.....	54
4.	priorisation des actions	55
	annexe 1 : liste des acteurs rencontrés.....	57
	annexe 2 : dégâts d'irma sur les infrastructures télécoms.....	58
	annexe 3 : local gcn shell beach – photos visite terrain.....	59
	annexe 4 : local gcn Police – photos visite terrain	60
	annexe 5 : nro de lorient – photos visite terrain	61
	annexe 6 : nro de gustavia – photos visite terrain.....	62
	annexe 7 : coffrets de rue– photos visite terrain	63
	glossaire	64

SYNTHÈSE

Face aux défis croissants liés au changement climatique, aux risques naturels et aux menaces technologiques, la Collectivité de Saint-Barthélemy a construit son schéma local de résilience. Les enjeux pour l'île sont d'autant plus importants que le territoire est fortement exposé à des risques naturels, industriels et technologiques.

Ce schéma local de résilience se focalise sur la résilience des réseaux, sur les dispositifs d'alerte à la population et sur le système d'information de la collectivité. En effet, les besoins en télécommunications des 10 585 habitants¹ sont en constantes augmentations et il est nécessaire de maintenir une continuité de service même en cas de survenue d'un événement majeur. De plus, un des premiers enjeux de la Collectivité est de maintenir informée la population en toute circonstance et notamment en cas de catastrophe naturelle.

Afin de fournir une connexion internet et des services à ses habitants, la Collectivité de Saint-Barthélemy dispose de plusieurs réseaux et solutions techniques : deux câbles sous-marins, deux réseaux de fibres optiques, un réseau hertzien, une liaison satellitaire et un réseau LoRaWAN. Cependant tous ces réseaux sont soumis à des risques naturels, cyber et accidentels.

Consciente de ces risques, la Collectivité s'est dotée d'un Plan Territorial de Sauvegarde. Ce plan a permis d'identifier les risques, de mettre en place une structure opérationnelle en cas d'événements majeurs et de disposer de plans préventifs et curatifs pour les différents risques identifiés. Le schéma local de résilience s'inscrit donc dans le plan territorial de sauvegarde en se focalisant uniquement sur les réseaux de télécommunications.

La Collectivité de Saint-Barthélemy est une collectivité d'outre-mer (COM), régie par l'article 74 de la Constitution, ce qui lui permet de disposer d'un statut particulier et d'une organisation institutionnelle propre. La collectivité exerce ainsi les compétences dévolues par les lois et règlements en vigueur aux communes, ainsi que celles dévolues au Département de la Guadeloupe et à la Région de la Guadeloupe. Elle dispose également de compétences propres relevant traditionnellement de l'État (fiscalité, urbanisme, environnement, énergie, etc.). Cette particularité permet à la Collectivité de Saint-Barthélemy de porter des projets d'envergure et de les mettre en œuvre de manière simplifiée.

Les objectifs clés du schéma sont les suivants :

- **Renforcer la résilience des réseaux de télécommunications** : les infrastructures numériques de l'île sont vulnérables aux risques naturels et technologiques. Le schéma prévoit des actions pour renforcer ces réseaux, comme l'enfouissement des câbles, l'arrivée d'un troisième câble sous-marin sur l'île ou encore le bouclage du réseau de collecte des NRO (deux chemins optiques différents pour acheminer le trafic) ;
- **Sécuriser l'approvisionnement en électricité et la résilience des réseaux** : Des efforts considérables ont été entrepris pour sécuriser l'alimentation en électricité, avec des câbles enterrés et des générateurs de secours pour assurer la continuité du service. Une résilience accrue du réseau électrique, crucial pour les télécommunications, a été mise en place depuis le passage de l'ouragan Irma.
- **Développer et optimiser les systèmes d'alerte à la population** : Le schéma inclut des outils numériques modernes pour alerter rapidement la population en cas de crise.

¹ Source : INSEE 2022

Un réseau de bornes wifi et de sirènes a été déployé pour améliorer la réactivité des alertes.

- **Améliorer la sécurité informatique** : L'île est de plus en plus exposée aux cybermenaces, et la collectivité travaille activement à l'amélioration de la cybersécurité à travers des audits, la mise en place de solutions techniques, et la coopération avec l'Agence Caribéenne pour la Cybersécurité (ACCYB).

Ces objectifs ont été déclinés en actions selon un degré de priorité (le niveau 1 étant le niveau de priorité le plus élevé).

PRIORITÉ 1		
SYSTÈMES D'ALERTE ET DE GESTION DE CRISE		
› Développer les systèmes d'alerte à la population.	2023-2027	1 2 3 4 5
› Créer un centre de veille territorial.	2023-2027	1 2 3 4 5
RÉSEAUX TÉLÉCOMS ET ÉLECTRIQUE		
› Assurer la continuité de fonctionnement du câble GCN.	2024 - 2034	1 2 3 4 5
› Migrer les équipements GCN, SCF, SSCS dans le futur NRO de Gustavia et engager les travaux de remise en état des locaux occupés mis à disposition de GCN.	2025	1 2 3 4 5
› Construire un troisième câble sous-marin, en collaboration avec d'autres îles caribéennes, avec un point d'atterrissage différent de Shell Beach.	2024 - 2027	1 2 3 4 5
› Lancer les réflexions, étudier et mettre en place les modalités techniques, juridiques et financières de gestion du service public industriel et commercial des réseaux Télécom	2024 - 2027	1 2 3 4 5
› Poursuivre la démarche engagée sur le réseau mobile et les sites résilients.	2024 - 2028	1 2 3 4 5
› Poursuivre les travaux d'enfouissement du réseau électrique.	2024 - 2028	1 2 3 4 5
› Renouveler les moteurs de la centrale électrique.	2024 - 2028	1 2 3 4 5
SÉCURITÉ INFORMATIQUE DE LA COLLECTIVITÉ		
› Construire le Schéma Directeur des Systèmes d'Information de la Collectivité.	2024 - 2025	1 2 3 4 5
› Mettre en place les actions d'amélioration de la sécurité de la donnée en débutant par l'audit cyber.	2024	1 2 3 4 5
› Poursuivre le projet autour de la donnée.	2024 - 2026	1 2 3 4 5

Echelle :	
1	Moins de 100 k€
2	Entre 100 k€ et 500 k€
3	Entre 500 k€ et 1 million
4	Entre 1 et 10 millions
5	Plus de 10 millions

PRIORITÉ 2

RÉSEAUX TÉLÉCOMS

- › Développer SBH-IX en collaboration avec les IXP des Îles voisines. 2024-2026 
- › Poursuivre la démarche engagée sur le réseau mobile avec la volonté de faire du RAN Sharing total. 2024-2028 

SÉCURITÉ INFORMATIQUE DE LA COLLECTIVITÉ

- › Construire le plan de reprise d'activité du SI de la Collectivité. 2024 - 2025 
- › Construire le plan de continuité d'activité du SI de la Collectivité. 2024 - 2025 
- › Collaborer avec l'ACCYB pour sensibiliser sur le sujet de la cybersécurité. 2024 - 2027 

Echelle :

1	Moins de 100 k€
2	Entre 100 k€ et 500 k€
3	Entre 500 k€ et 1 million
4	Entre 1 et 10 millions
5	Plus de 10 millions

Ce schéma vise à maintenir Saint-Barthélemy comme un territoire connecté et résilient, capable de faire face efficacement aux diverses menaces tout en assurant la continuité des services essentiels pour ses habitants.

INTRODUCTION

L'élaboration du schéma local de résilience s'est articulée autour de quatre grandes phases :

PHASE 1 - PRÉPARATOIRE

- Informations des parties prenantes (Préfecture, Banque des territoires, etc.) ;
- Communication sur la démarche de construction du schéma local de résilience auprès des acteurs du territoire.

PHASE 2 - AUDIT TERRITORIAL

- Diagnostic de vulnérabilité ;
- Dispositifs opérationnels en cas d'événements majeurs ;
- Réseaux résilients sur le territoire ;
- Dispositifs de sécurité informatique de la Collectivité.

PHASE 3 – SOLUTIONS ET SCENARIOS D'INTERVENTION

- Recommandations et actions à mettre en place des solutions d'alertes et d'améliorer la résilience des réseaux et la sécurité informatique de la Collectivité.

PHASE 4 – PLAN D' ACTIONS

- Priorisation des actions.

1. PHASE 1 – PHASE PRÉPARATOIRE

Cette première phase avait pour but d'approfondir les connaissances du territoire et d'informer les acteurs sur la démarche de la construction d'un schéma local de résilience. Elle s'est déroulée conjointement à la démarche de construction du schéma directeur des usages numériques de la collectivité.

La phase préparatoire s'est déroulée du 27 février au 23 mai 2024. Durant cette période, une trentaine d'acteurs ont été interrogés. La liste des personnes, entités et partenaires rencontrés est annexée au présent rapport ([annexe 1 : listes des acteurs rencontrés](#)).

Lors de ces rencontres, la méthodologie de construction et l'organisation du schéma de résilience ont été abordées.



Figure 1 : Hôtel de la Collectivité de Saint-Barthélemy

2. PHASE 2 – AUDIT TERRITORIAL

Un audit territorial a permis de dresser un état des lieux du territoire en s'appuyant sur les éléments suivants :

- Le diagnostic de vulnérabilité qui permet d'identifier les aléas spécifiques au contexte de l'île et d'identifier leurs impacts potentiels sur la résilience des réseaux télécoms ;
- L'organisation mise en place au sein du Centre Opérationnel Territorial pour la gestion de crise ;
- L'état des lieux des réseaux sur le territoire, et en particulier les réseaux de télécommunications et le réseau électrique ;
- Le système d'information de la Collectivité.

En complément, une visite terrain des infrastructures a été réalisée le 19 avril 2024 afin de dresser un état des lieux complet. Les photos de cette visite sont disponibles de [l'annexe 3 à 7](#).

2.1. Des vulnérabilités identifiées sur le territoire

Ce diagnostic s'appuie sur le Plan Territorial de Sauvegarde de Saint-Barthélemy réalisé dans le cadre du projet SAFE St Barth² et sur le site gouvernemental Géorisques :

- Un plan de sauvegarde a pour but de permettre à une collectivité de disposer de plans d'actions lors de la survenance d'événements naturels, sanitaires et technologiques ;
- Le site Géorisques³ fournit des compléments d'information sur les risques naturels auxquels Saint-Barthélemy est exposé.

Dans le cadre de la construction du plan territorial de sauvegarde, une étude des aléas a été réalisée. Pour chaque aléa identifié, un plan d'intervention gradué a été rédigé.

Les aléas sont classés selon les catégories suivantes :

- Aléas naturels ;
- Aléas technologiques ;
- Aléas de ruptures d'approvisionnement ;
- Aléas sanitaires ;
- Aléa terroriste ;
- Aléa cybersécurité.

Pour chacune de ces catégories, des risques précis sont rattachés.

² <https://safestbarth.fr>

³ <https://www.georisques.gouv.fr/>

2.1.1.1. Des aléas naturels divers

2.1.1.1.1. Les aléas d'inondation

Saint-Barthélemy est exposé à des risques d'inondations liés aux ruissellements des eaux pluviales. Toutes les zones urbanisées sont exposées à cet aléa.

Les inondations peuvent impacter certains éléments des réseaux présents sur le territoire. C'est certainement le réseau de distribution d'électricité qui est le plus sensible à cet aléa. Une inondation se caractérise par une submersion, ou une crue rapide ou lente, d'une zone habituellement hors d'eau. Cet aléa est déterminé sur Saint-Barthélemy par une topographie marquée, essentiellement composée de ravines réactives aux fortes pluies, lorsque les sols sont saturés en eau. De fait, les zones inondables sont importantes dans les plaines littorales qui malgré leur petite taille, comportent quelques dépressions lagunaires (comme Grande Saline).

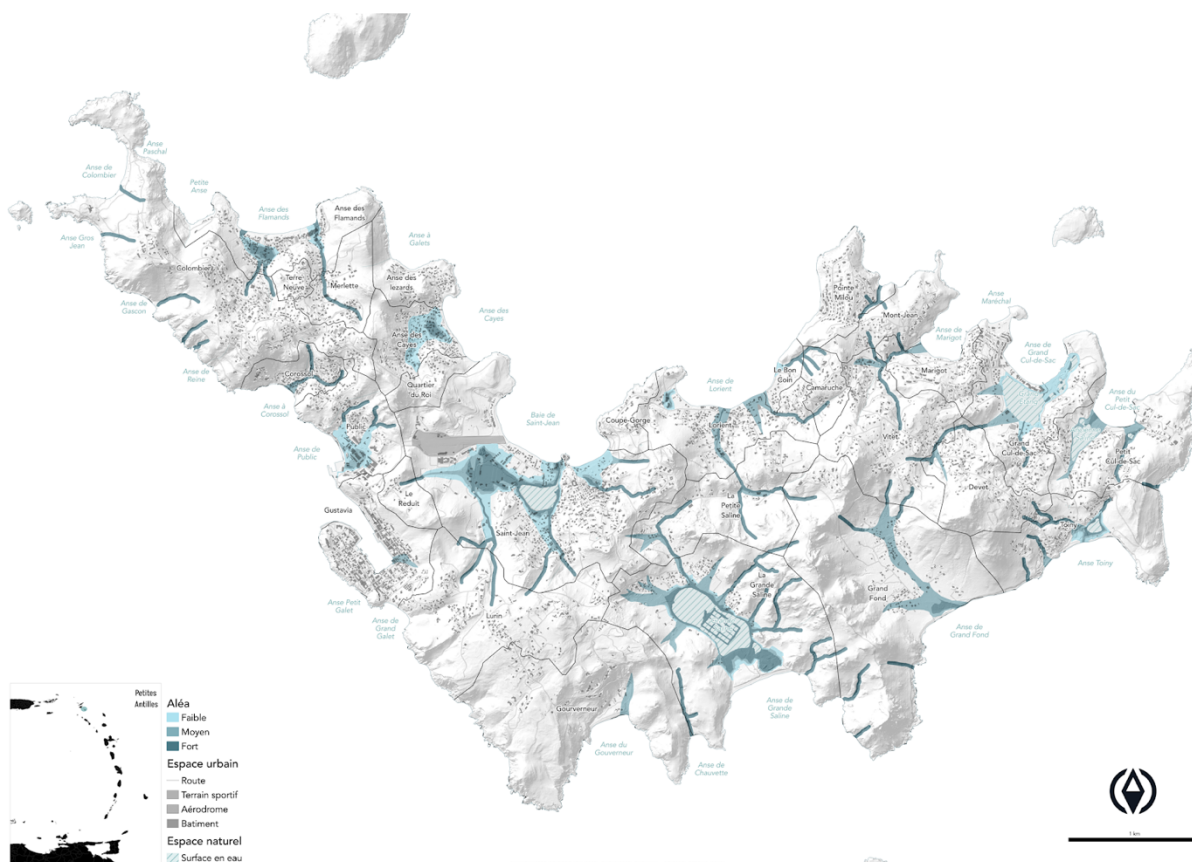


Figure 2 : carte des aléas d'inondation

2.1.1.1.2. Les aléas cycloniques

L'apparition de cyclone représente un risque pour une partie des infrastructures télécoms.

Les dégâts peuvent être plus ou moins importants et différents selon l'intensité du cyclone et son type (vents violents, houle, pluies, etc.) ; les risques auxquels est exposé Saint-Barthélemy sont donc dépendants des caractéristiques du cyclone.

Les cyclones peuvent notamment entraîner des submersions marines en raison de la baisse de la pression atmosphérique et peuvent encore être accentuées par la forte houle. Dans ce cas, les dégâts sont comparables à ceux occasionnés par des inondations. L'île, composée

de nombreuses anses, est exposée à ce phénomène susceptible de toucher de nombreuses zones habitées. Par ailleurs, le ruissellement pluvial, conséquence de fortes pluies, associé à une faible capacité d'infiltration des sols, soit en raison de leur saturation, soit en raison de leur imperméabilisation (développement urbain) peut être un facteur aggravant. De ce fait, toute zone urbanisée est soumise à ce risque, avec des conséquences comme l'isolement ou la noyade. D'autres phénomènes indirects peuvent être causés par de fortes pluies comme les coulées de boue ou encore les mouvements de terrain.

À noter, que l'intensité des phénomènes cycloniques est définie selon la classification Saffir-Simpson :

Catégorie	Vents soutenus	Impacts potentiels
D - Dépression	0-63 km/h	Pluies intenses
T - Tempête tropicale	64-118km/h	Pluies intenses / dommages négligeables
1 - Cyclone de catégorie 1	119-153km/h	Pluies intenses / forts vents / dommages négligeables aux habitations légères, la végétation et le mobilier urbain / dommages importants sur les quais et les jetées
2 - Cyclone de catégorie 2	154-177km/h	Pluies intenses / forts vents / dommages structurels aux habitations (important sur les habitations légères), la végétation et le mobilier urbain / dommages importants sur les quais et les jetées
3 - Cyclone de catégorie 3	178-210km/h	Pluies intenses / forts vents / dommages structurels aux petites résidences et habitations (important voir destruction des habitations légères, sans fondations), la végétation et le mobilier urbain / dommages importants sur les quais et les jetées / Inondation côtière et possible glissement de terrain
4 - Cyclone de catégorie 4	211-251km/h	Pluies intenses / forts vents / dommages structurels aux bâtiments (dommages irréparables voir destruction des habitations légères, sans fondations et petites habitations), la végétation et le mobilier urbain / dommages importants sur les quais et les jetées / Inondation côtière et possible glissement de terrain et érosion des plages
5 - Cyclone de catégorie 5	Plus de 251km/h	Pluies intenses / forts vents / dommages considérables bâtiments (dommages irréparables voir destruction), la végétation et le mobilier urbain / dommages considérables sur les infrastructures côtières et les bâtiments sur le littoral / fortes crues et inondation côtière et possible glissement de terrain et érosion des plages

Figure 3 : Échelle de classification Saffir-Simpson

La saison cyclonique s'étend de juin à novembre avec un risque accru entre mi-août et mi-octobre.

Selon l'outil Géorisques un vent est estimé violent lorsque sa vitesse atteint 80 km/h en vent moyen et 100 km/h en rafale à l'intérieur des terres. À titre d'exemple, les vents de l'ouragan IRMA ont atteint des vitesses allant jusqu'à 360km/h.

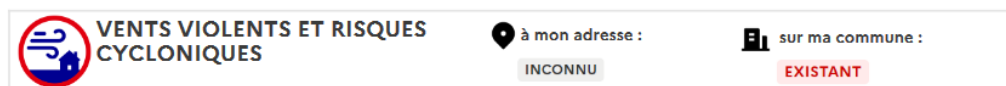


Figure 4 : Extrait de l'aléa Cyclone - Géorisques

Des mesures collectives (entretien des réseaux, etc.) et individuelles (adaptation des constructions, etc.), prises et recommandées, permettent la réduction considérable des dommages causés par les inondations.

À la suite de l'ouragan IRMA, la Collectivité de Saint-Barthélemy a pris la décision d'enterrer 100% des réseaux fixes (cuivre, fibre optique et distribution d'électricité), ce qui la différencie

des autres territoires. L'enfouissement de la boucle locale cuivre, encore partiellement en aérien, suit progressivement le rythme des travaux de mise en souterrain du réseau électrique sur le domaine public routier. Les armoires de sous-répartition réparties sur le bord des routes sont également exposées à des risques d'endommagement. L'[annexe 2](#) montre les dégâts causés par IRMA sur ces armoires extérieures.

Par ailleurs, le réseau mobile (pylônes) est, par nature, le plus exposé aux risques cycloniques.

2.1.1.1.3. Les aléas de mouvements de terrain

Les mouvements de terrain peuvent être de différentes sources : glissements de terrain, ravinements et chutes de blocs. Une des principales conséquences est l'affaissement des infrastructures routières ce qui peut entraîner d'importants dégâts sur les réseaux souterrains (électrique, télécom, eau potable, etc.). Ces dommages peuvent ainsi conduire à des coupures électriques. Ceci a une conséquence directe sur les réseaux télécoms puisqu'ils sont alimentés électriquement.

Le Bureau de recherches géologiques et minières (ci-après « BRGM ») a fourni en 2024 à la Collectivité des cartographies, d'une précision au 1/10000^{ème} et au 1/5000^{ème}, pointant les zones géographiques soumises aux mouvements de terrain. Deux cartographies complémentaires ont été fournies en détaillant les zones exposées aux aléas de chutes de blocs et aux glissements de terrain.

2.1.1.1.4. Les aléas sismiques

Tout comme les mouvements de terrain, les séismes peuvent entraîner la destruction de bâtiments et l'affaissement des infrastructures routières. Ces conséquences sont de nature à impacter les réseaux souterrains (électrique, télécom, eau potable, etc.). Le système électrique peut donc être affecté (production et distribution) et ainsi entraîner des coupures électriques. Ceci a une conséquence directe sur les réseaux télécoms puisqu'ils sont alimentés électriquement.

Les dégâts engendrés dépendent de l'intensité du séisme et de sa durée. L'échelle de Richter permet de classer l'intensité des séismes selon leur magnitude :

Magnitude	Effets engendrés
9	Destruction totale à l'épicentre, et possible sur plusieurs milliers de km
8	Dégâts majeurs à l'épicentre, et sur plusieurs centaines de km
7	Importants dégâts à l'épicentre, secousse ressentie à plusieurs centaines de km
6	Dégâts à l'épicentre dont l'ampleur dépend de la qualité des constructions
5	Tremblement fortement ressenti, dommages mineurs près de l'épicentre
4	Secousse sensible, mais pas de dégâts
3	Seuil à partir duquel la secousse devient sensible pour la plupart des gens
2	Secousse ressentie uniquement par des gens au repos
1	Secousse imperceptible

Figure 5 : Echelle de Richter

2.1.1.1.5. Les aléas de volcanisme

Si localement, il n'y a pas de risque direct, l'île n'en reste pas moins exposée aux effets des volcans de l'arc volcanique des petites Antilles situé à proximité. Cela peut par exemple se traduire par des nuages de cendres dont les retombées peuvent toucher Saint-Barthélemy (Soufrière de Montserrat, 1997). Au plus près il y a Saba, surveillé par le KNMI (Royal Netherlands Meteorological Institute pour le volcan Saba). Au plus loin, la Soufrière de Saint-Vincent, surveillé par l'UWI et le SRC.

Les infrastructures télécoms ne sont donc pas directement menacées par ce risque. Cependant, l'entrée en éruption d'un des volcans dans la zone peut entraîner un tsunami pouvant toucher les côtes et donc engendrer d'importants dégâts sur les infrastructures.

Une éruption volcanique peut également isoler l'île en bloquant notamment le trafic aérien pendant plusieurs jours ou semaines, limitant les déplacements de passagers entre les îles et pouvant perturber les activités de maintenance des infrastructures et de livraison de matériels.

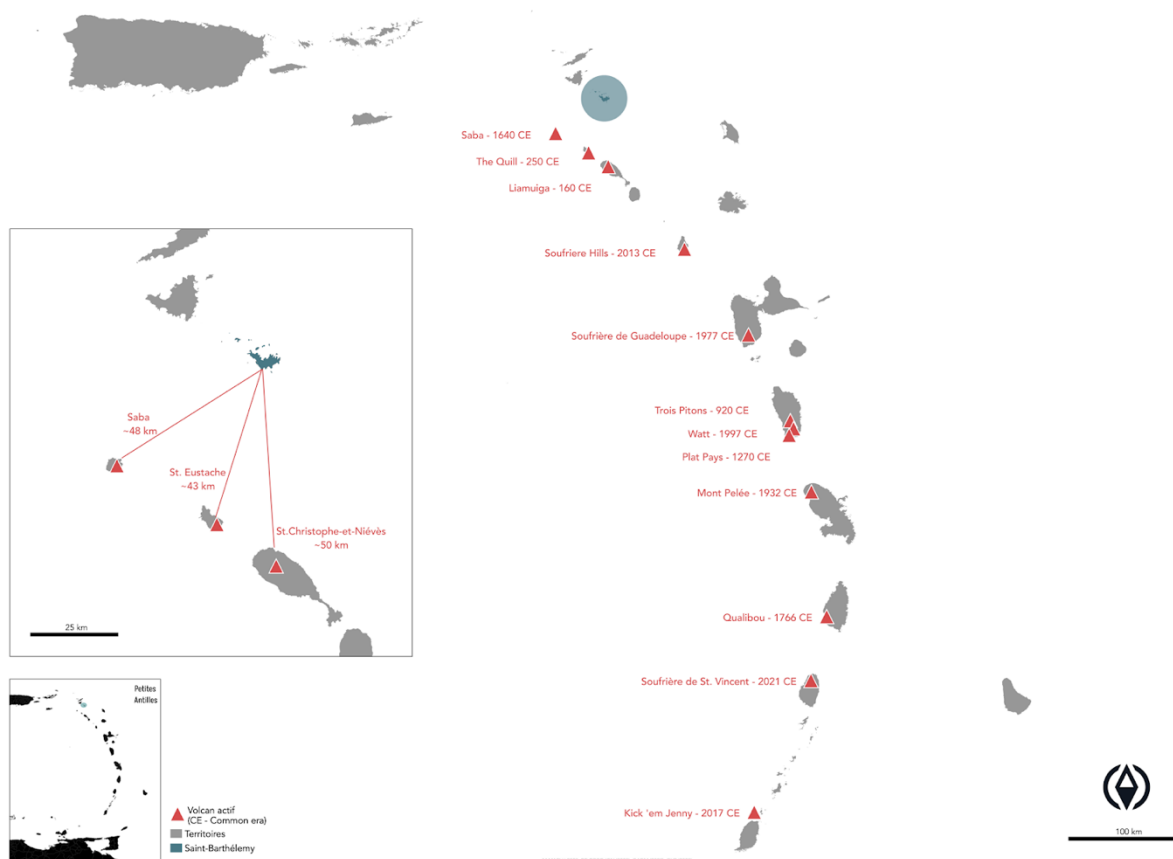


Figure 6 : carte des volcans des Antilles

2.1.1.1.6. Les aléas de tsunami

Ce phénomène peut causer de nombreux dégâts notamment sur les bâtiments et infrastructures situés sur la frange littorale. Ainsi, toutes les zones de l'île dont l'altitude est inférieure ou égale à 10 mètres ont de fortes probabilités d'être soumises à cet aléa

Les tsunamis peuvent être générés par des séismes, des glissements de terrain et des éruptions volcaniques sous-marines.

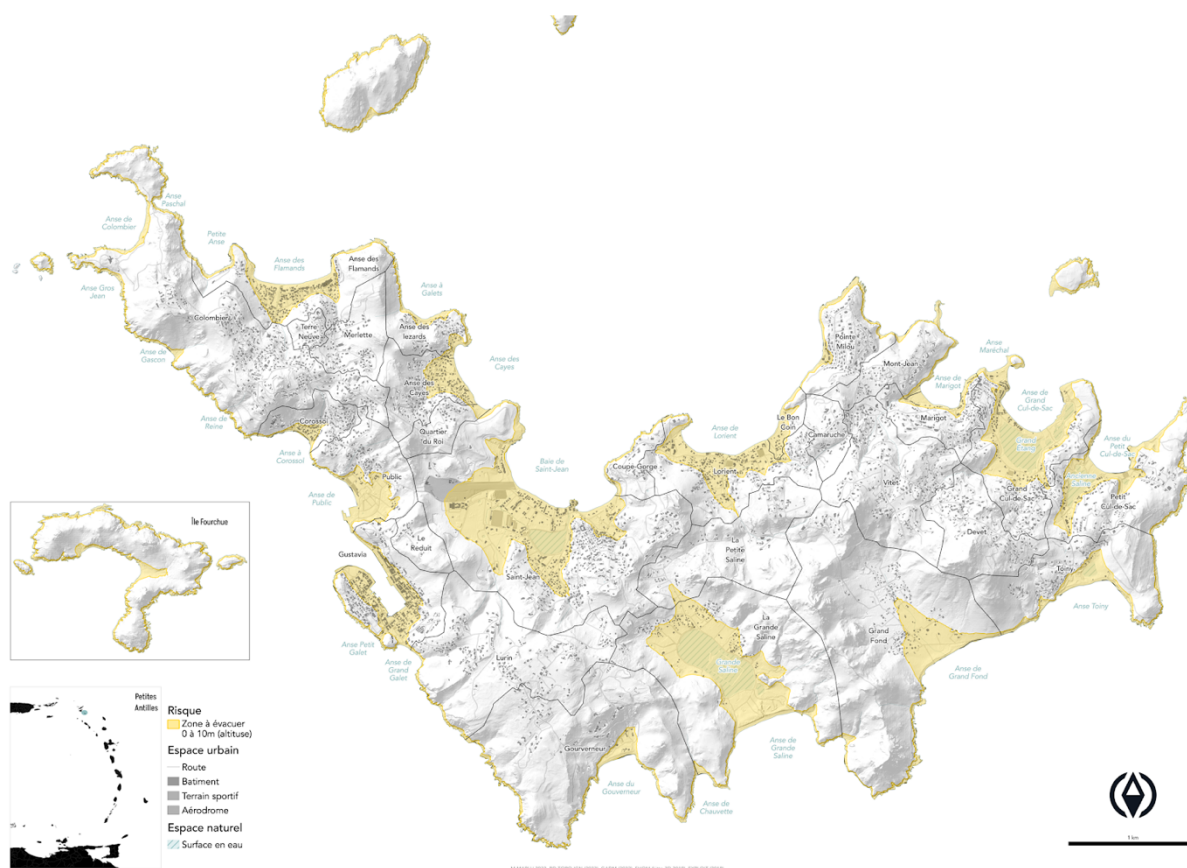


Figure 7 : carte des aléas de tsunami

2.1.1.2. Des aléas liés à l'énergie

En cas de coupure électrique, de nombreux réseaux sont impactés dont les réseaux télécoms qu'ils soient mobiles ou fixes. En effet, ces réseaux présentent une grande dépendance vis-à-vis du réseau de distribution électrique, comme l'atteste le graphe ci-dessous :

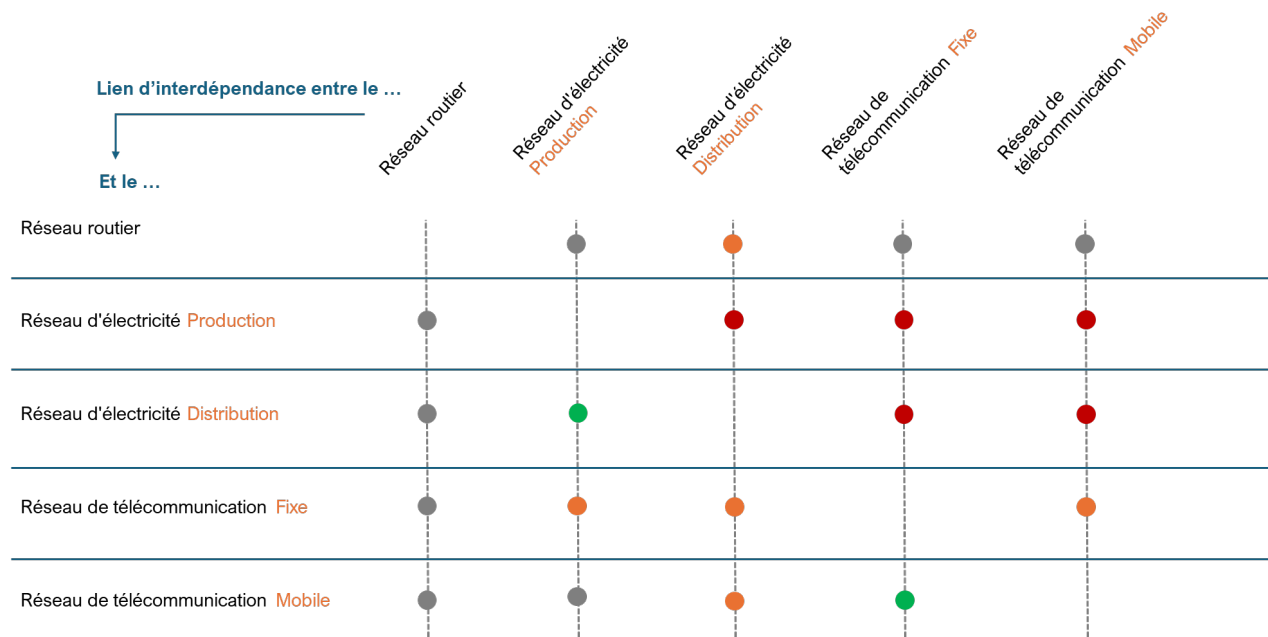


Figure 8 : Interdépendance des réseaux

La couleur indique le degré du lien de dépendance du réseau en colonne vis-à-vis de celui en ligne ; le lien de dépendance est plus fort dans le cas d'une pastille rouge que d'une pastille verte.

En cas de survenue d'une coupure électrique, le réseau mobile peut cesser de fonctionner dans l'heure qui suit. Sur l'île, seuls 3 sites mobiles sont équipés de générateurs électriques (TDF Lurin, Aéroport, NRA Gustavia Orange).

2.1.1.3. Des aléas de cybersécurité

Le risque cyber ne fait que s'accroître avec le développement constant du numérique. Ces risques peuvent être de différentes natures pour Saint-Barthélemy : cyberattaque, coupure des câbles sous-marins, défaillance des équipements et des infrastructures des opérateurs privés situés sur d'autres îles, etc.

L'apparition de l'un de ces risques entraînerait potentiellement le vol et/ou la perte de données, un isolement de l'île, des pertes financières, des atteintes au système d'information de la Collectivité et un impact négatif sur la réputation de l'île.

Malgré la mise en place de mesures préventives ou correctives, ces événements peuvent impacter plus ou moins les utilisateurs. Une échelle d'urgence et de temps d'intervention a été définie par l'ACCYB :

NIVEAU D'URGENCE	RÉACTION
CRITIQUE	IMMÉDIATE
IMPORTANT	72 HEURES
PRÉOCCUPANT	5 JOURS
SIGNIFICATIF	15 JOURS
NON SIGNIFICATIF	30 JOURS

Figure 9 : Échelle de niveau d'urgence pour les risques cyber

Les enjeux de cybersécurité sont donc essentiels pour la Collectivité et tous les usagers. La Collectivité s'est saisie de ces enjeux en étant à l'initiative au côté de la Guadeloupe et de la Guyane de la création de [l'Agence Caribéenne de la Cybersécurité](#) et de la mise en place prochaine du CSIRT ATLANTIC (Computer Security Incident Response Team).

2.1.1.4. Aléas liés à l'architecture des réseaux des opérateurs de télécommunication

Le risque lié à l'architecture des réseaux des opérateurs de télécommunication est un facteur externe à l'île, mais néanmoins à prendre en compte.

En effet, les cœurs de réseau des opérateurs télécoms intervenant à Saint-Barthélemy se trouvent sur d'autres îles des Antilles. Ainsi, si l'un des risques mentionnés précédemment affecte une autre île que Saint-Barthélemy (notamment la Guadeloupe ou Saint-Martin), Saint-Barthélemy en subira immédiatement les conséquences.

Cela justifie que la Collectivité exploite son propre réseau et motive sa demande de soutien de l'État, depuis l'Ouragan Irma, d'imposer une obligation de routage local des télécommunications aux opérateurs.

2.2. Des dispositifs opérationnels en cas d'évènements majeurs

2.2.1. Un Centre Opérationnel Territorial au service de la gestion de crises

La Collectivité dispose d'un Centre Opérationnel Territorial (ci-après « COT »). Ce centre est placé sous l'autorité du Président de la Collectivité ou du Préfet, qui est le Directeur des Opérations de Secours (DOS) et du Commandant des Opérations de secours (COS) ou Responsable du Service territorial d'incendie et de secours (ci-après « STIS »). À noter que le COT sera prochainement situé au sein de la nouvelle caserne du STIS hébergeant également le centre de veille.

Le COT est outil au service de la gestion des crises sur le territoire. L'ensemble des outils du centre de veille seront mis au service du COT lorsqu'il sera activé.

Le COT est en charge, en cas de crise ou d'événement majeur, de :

- Analyser la crise : sources, enjeux et actions en cours ;
- Mettre en place une stratégie d'action : prioriser, anticiper et évaluer les besoins ;
- Alerter et informer : la population, les équipes terrain et les services de l'État ;
- Agir : en communiquant, en engageant les actions et en s'adaptant au contexte de la crise.

L'organisation type du COT est définie selon le schéma ci-dessous.

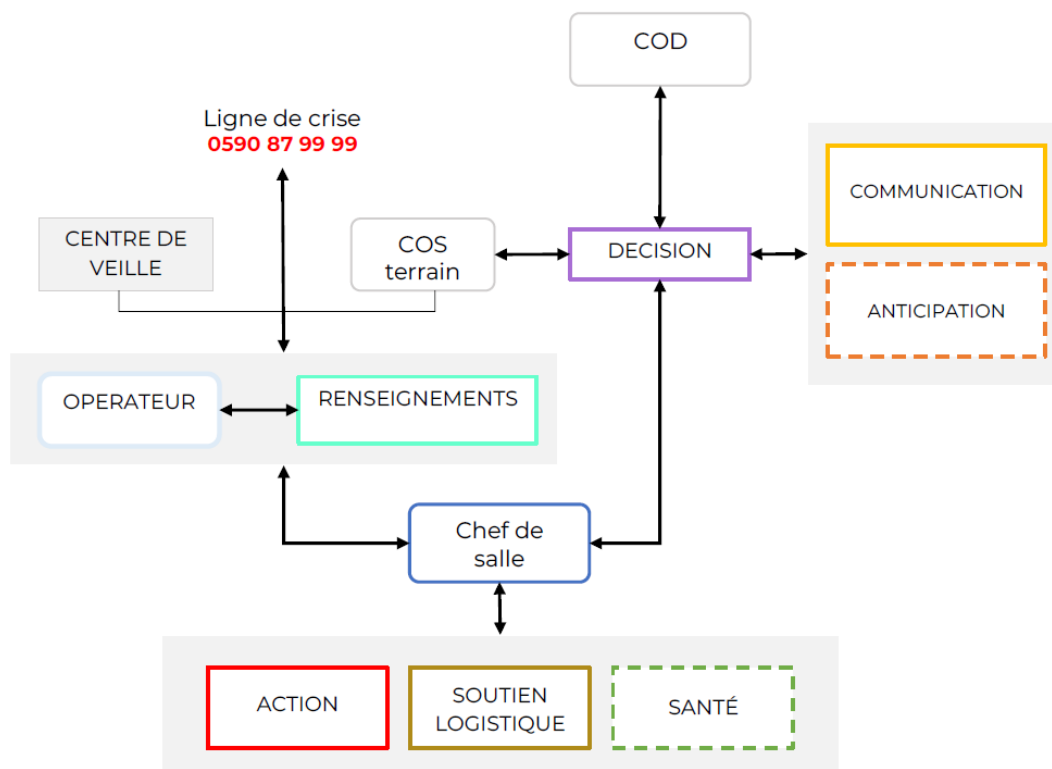


Figure 10 : Schéma d'organisation du COT

Les cellules Renseignements, Anticipation et Santé sont présentes pour répondre à des besoins spécifiques. Leur existence et leur la taille peuvent donc varier en fonction des événements et des besoins à traiter.

Le COT organise également des exercices réguliers de crise afin de tester et d'améliorer son fonctionnement. À l'issue de chaque exercice, un compte rendu est réalisé pour évaluer l'organisation du COT, et identifier les points forts et les axes d'amélioration pour chaque composante (humaine, organisationnelle et technique).

2.2.2. Des solutions télécom opérationnelles pour la Collectivité

La collectivité a mis en place un certain nombre d'actions dans le cas de la survenance d'un événement. En effet, des solutions sont mises en place pour pallier les défaillances des opérateurs privés et répondre aux besoins de communication et d'accès à internet de la Collectivité et des services de secours :

- Un réseau téléphonique VOIP local (3CX) capable de fonctionner sans accès internet :
 - La solution avec des postes fixes équipant tous les agents de la collectivité dans les différents bâtiments de la collectivité est également déployée auprès des partenaires publics et privés ayant un rôle à jouer en cas d'évènement majeur (préfecture, hôpital, gendarmerie, EDF, SAUR, SIDEM, etc.). Il y a un annuaire avec les numéros de téléphone des différents services directement sur le poste téléphonique mis en place ;
 - La solution Soft phone 3CX sur téléphone portable permet d'accéder à ce réseau interne via le réseau de bornes wifi de la collectivité grâce à des Domain Name System (ci-après « DNS ») internes ;
 - Ce réseau de téléphones a donc la capacité de fonctionner sans internet ce qui permet d'assurer la communication entre les acteurs majeurs du territoire en cas de défaillance des opérateurs de télécommunication ;
- Un réseau de bornes wifi déployé au sein des bâtiments de la collectivité (pour les agents) et sur certains points du domaine public : en cas de catastrophes naturelles, certains points d'accès répartis deviennent accessibles au public ;
- Deux abonnements FttO à débit garanti et un accès internet directement sur le câble sous-marin SSCS ;
- Un abonnement FttH supplémentaire chez différents opérateurs pour certains bâtiments de la Collectivité, y compris au sein des NRO dans lesquels sont installés les équipements actifs du système d'information de la Collectivité ;
- Un abonnement Starlink sur un des trois NRO ;
- Un réseau radio opéré par la Collectivité et destiné aux services de secours (Police, Pompiers, Sécurité Civile) dont les baies sont connectées au réseau FttO et interconnectées entre elles. Les baies sont équipées de batteries permettant d'assurer la continuité de service en cas de coupure électrique temporaire (le site de TDF Lurin qui couvre la quasi-totalité du territoire est secouru par un groupe électrogène) ;
- Un réseau de coffrets de rue connecté au réseau privé de la Collectivité permettant d'y brancher simplement sur un switch en PoE n'importe quel objet connecté (caméra, point wifi, haut-parleur, sirène d'alerte, téléphone IP, gateways LoRaWAN, ...).

2.3. Des réseaux résilients pour lutter contre les vulnérabilités du territoire

2.3.1. Des systèmes de câbles sous-marins contribuant à la résilience du territoire

Les Caraïbes sont connectés à internet via de nombreux câbles sous-marins. Cependant chaque île ne dispose que d'un ou deux points d'interconnexion (point de défaillance unique).

Concernant l'île de Saint-Barthélemy, elle dispose d'un accès internet via deux systèmes de câbles sous-marins :

- Global Caribbean Network (ci-après « GCN ») ;
- Saba, Statia Cable System (ci-après « SSCS »).

Ces deux systèmes de câbles sous-marins ont été cofinancés par l'Union européenne (ci-après « UE ») et par les gouvernements locaux.

Les principaux fournisseurs d'accès à Internet de Saint-Barthélemy disposent d'un accès à ces deux systèmes de câbles.

2.3.1.1. Le câble Global Caribbean Network (GCN)

La région de Guadeloupe a conclu, en novembre 2004 et pour une durée de 20 ans, un contrat de délégation de service public avec la société Global Caribbean Network. Ce contrat a pour objet la conception, la réalisation, le financement, la pose et l'exploitation d'un câble sous-marin dédié à la communication à haut débit.

Ce câble sous-marin, baptisé « Guadeloupe Numérique », permet de relier les îles de Guadeloupe, de Saint-Martin et de Saint-Barthélemy en fibres optiques. Le câble représente une longueur totale de 890 km et a été mis en service en octobre 2006.

L'investissement initial s'élève à 25,3 millions d'euros. La Collectivité de Saint-Barthélemy a contribué à hauteur d'un million d'euros pour l'établissement de sa branche dont le point d'atterrissage est situé à Gustavia (Shell Beach).⁴

La branche « Saint-Barthélemy » du câble GCN a permis le désenclavement de l'île grâce à sa capacité maximale de 5 Gbit/s.⁵

La DSP arrivant à son terme en mars 2025, des réflexions sont actuellement menées sur le renouvellement de ce contrat.

⁴ Sources : <https://www.submarinecablemap.com/submarine-cable/global-caribbean-network-gcn>
Schéma Directeur Territorial d'aménagement Numérique de Saint-Barthélemy de Décembre 2013

⁵ SDTAN

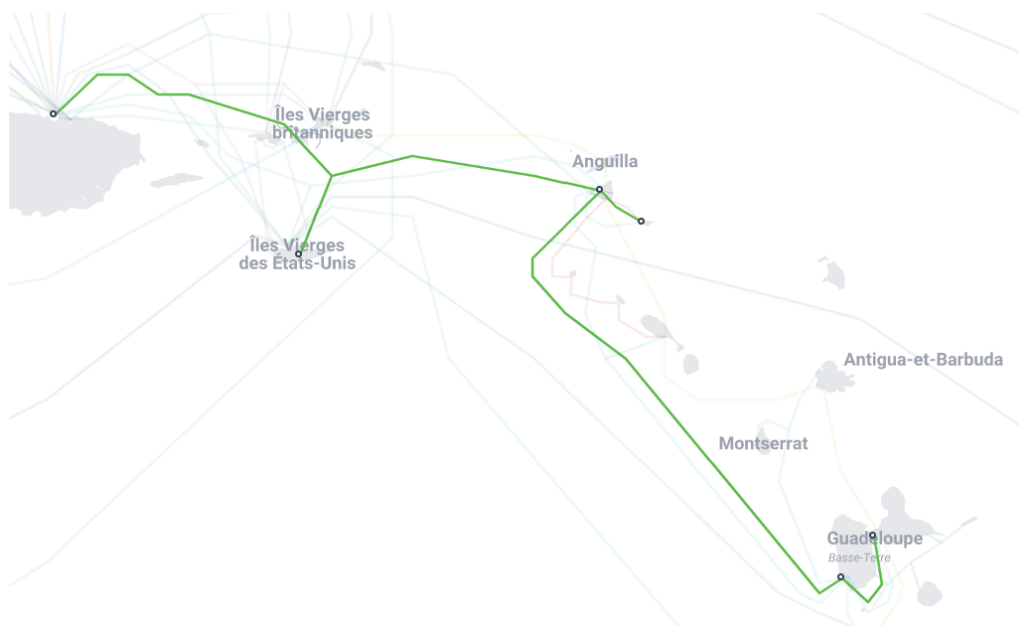


Figure 11: <https://www.submarinecablemap.com/submarine-cable/global-caribbean-network-gcn>

Sur l'île, GCN dispose de deux bâtiments avec un local réservé à GCN et un local de colocalisation pour les opérateurs tiers, y compris les opérateurs de câbles sous-marins tels que SSCS et SCF (Southern Caribbean Fiber). Ces locaux appartiennent à la collectivité et sont loués par la collectivité pour un loyer très largement inférieur au marché (9 000 €/an). L'état de leur maintenance laisse à désirer (les systèmes de climatisation et d'incendie sont défectueux) et se doit d'être revu ([voir photos](#)).

2.3.1.2. Le câble Saba, Statia Cable System (SSCS)

Saint-Barthélemy est relié par un deuxième câble sous-marin à l'internet mondial. Le câble Saba, Statia Cable System d'une longueur totale de 198 km, connecte les îles de Saba, Statia, Saint-Kitts et Sint-Maarten.

Ce câble a été mis en service en 2012 à l'initiative du gouvernement néerlandais pour permettre la création d'une infrastructure de communication et ainsi faciliter la transmission de données entre ses îles. En 2013, une extension vers l'île de Saint-Barthélemy a été réalisée. Comme pour le câble GCN, le point d'atterrissage est situé à Gustavia (Shell Beach), ce qui est problématique dans une optique de résilience des réseaux.

Le système de câbles est détenu par les Pays-Bas et exploité par la société SSCS BV pour le compte du Ministère de l'Intérieur et des Relations du Royaume des Pays-Bas (Ministry of the Interior and Kingdom Relations - BZK).



Figure 12 : <https://www.submarinecablemap.com/submarine-cable/saba-statia-cable-system-sscs>

À noter qu'il existe une branching unit entre Saint-Martin et Saba à laquelle Saint-Barthélemy est raccordée. Saint-Barthélemy peut donc sortir son trafic vers Saint-Kitts sans passer par Saint-Martin.

Le câble SSCS arrive dans le « local police ». Le « local police » est dans un état critique avec notamment des infiltrations d'eau. Par ailleurs, alors que ce local est censé être exclusivement un local télécom, il sert également d'espace de stockage de matériel. Il est nécessaire de refaire entièrement le local ([voir photos](#)).

2.3.1.3. Un projet de nouveau câble sous-marin pour renforcer la résilience du territoire

L'état actuel de la connexion externe à l'île à travers les câbles GCN et SSCS n'est pas satisfaisant pour les acteurs du territoire qui constatent qu'il existe un point de défaillance unique.

En effet, ces câbles ont le même point d'atterrissage (à Gustavia, Shell Beach). Dans une optique de résilience des réseaux, il serait préférable que ces câbles arrivent à deux endroits différents sur l'île.

Deuxièmement, ces câbles posent des limites et sont source de mécontentements sur les prix pour les plus petits opérateurs, la disponibilité et la qualité des réseaux. La bande passante sur les câbles supporte les coûts de maintenance du système de câble. Le marché est relativement opaque et les prix observés sont de 10 à 50 fois supérieurs à ceux pratiqués dans l'UE continentale, en partie à cause d'une mauvaise efficacité opérationnelle.

Un troisième câble serait nécessaire pour pallier les limites identifiées. Un point d'atterrissage différent de Gustavia, avec une localisation à Saint-Jean semble préférable. Ceci permettrait de réduire une partie des risques tout en dédoublant les accès à l'internet mondial.

Une structure de portage commune avec les îles voisines ayant des besoins communs serait pertinente sur ce sujet.

Plusieurs projets de nouveaux câbles sous-marins sont actuellement à l'étude dans la région.

2.3.1.3.1. Le projet EU Project Fusion

Le projet vise à interconnecter la zone Antilles-Guyane au continent européen en passant par le nord de l'océan Atlantique. Actuellement, aucun câble ne relie directement cette zone à l'Europe. Les Antilles sont reliées au continent Américain qui lui est connecté au continent européen.

Dans ce contexte, une extension de câble sous-marin, entre la Guyane et l'Europe, est prévue à horizon 2025. Cette extension passera par la zone sud de l'océan Atlantique. Mais ce chemin doit être redondé par la zone nord.

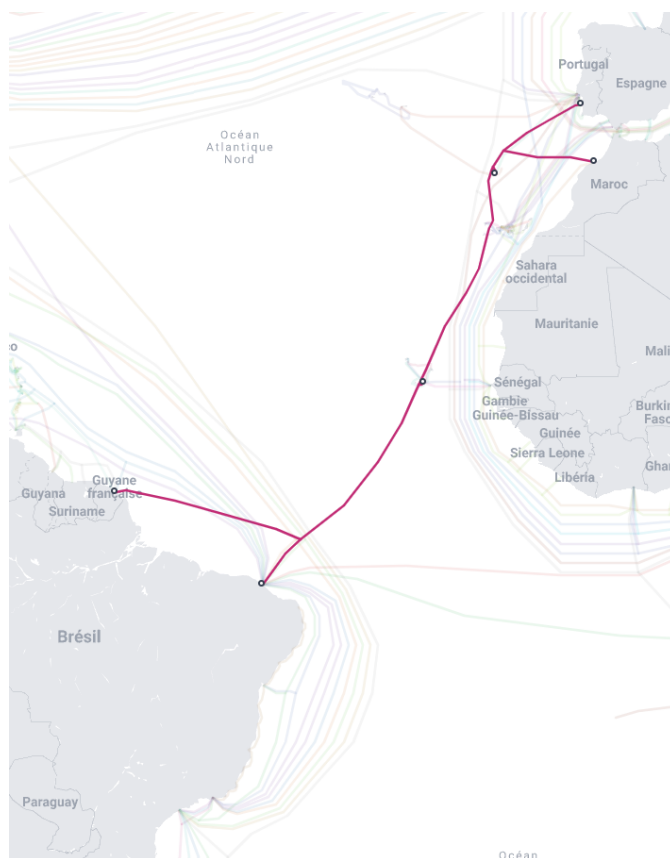


Figure 13 : <https://www.submarinecablemap.com/submarine-cable/ellalink>

Le raccordement de la Guyane au réseau EllaLink est prévu à horizon 2026. La Société Publique Locale pour l'Aménagement Numérique de la Guyane (ci-après « SPLANG ») a commandé et financé ce raccordement.

La collectivité de Saint-Barthélemy pourrait y voir une opportunité de raccordement à un réseau transatlantique. Ce câble d'une longueur de 6 200 km relie le Brésil, le Maroc et le Portugal.⁶

Pour cela, il serait nécessaire d'interconnecter les îles antillaises en mutualisant les opérateurs sur les différents câbles sous-marins. Un des opérateurs propose de mettre en place une solution de backbone Multiprotocol Label Switching (ci-après « MPLS ») afin de fournir des offres redondées de bout en bout aux utilisateurs sans passer par de nombreux intermédiaires.

Ce projet apporterait une meilleure résilience et faciliterait les connexions avec l'Europe.

⁶ Source : <https://www.submarinecablemap.com/submarine-cable/ellalink>

2.3.1.3.2. Le projet BELLA II

Le projet de câble nommé BELLA II vise à remplacer le câble Americas-II. Le futur câble aurait deux routes : une vers la Martinique et une vers Miami. Altice (SFR) et Telxius (Telefonica) sont présents dans le consortium.

Avec ce câble, Saint-Barthélemy pourrait devenir un « Hub » sur la Caraïbe en tant que véritable route alternative et résiliente vers la Martinique et les USA (à Miami).

2.3.1.3.3. Deep Blue One

Dans le cadre d'un projet visant à accroître la capacité sous-marine internationale des Caraïbes et de l'Amérique latine, Orange a signé un accord de partenariat avec Digicel en septembre 2021 pour prolonger le câble Deep Blue One jusqu'à Cayenne.

Deep Blue One est un câble de 2 000 km reliant la Guyane française, le Suriname, le Guyana et Trinidad & Tobago.

Ce nouveau système offre une solution sécurisée et adaptative dans la région pour répondre aux besoins croissants en bande passante. Le projet de câble Deep Blue One a été mis en service en mai 2024.

Une interconnexion à ce câble pourrait être envisagée. Par ailleurs, si Deep Blue One envisageait de remonter vers le nord des Antilles un prolongement pourrait être envisagé vers Saint-Barthélemy.

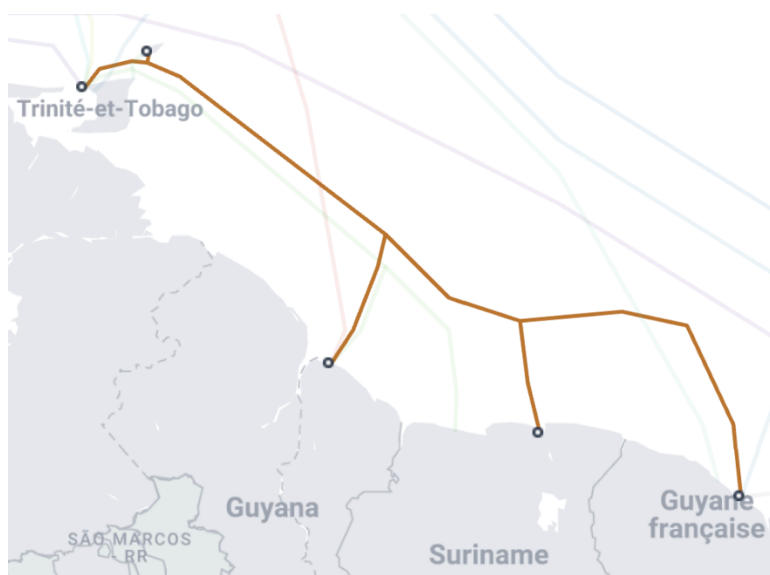


Figure 14 : <https://www.submarinecablemap.com/submarine-cable/deep-blue-one>

2.3.2. Des réseaux de fibres optiques résilients couvrant l'intégralité du territoire

Saint-Barthélemy compte sur son île un certain nombre de réseaux, dont deux réseaux d'initiative publique exploités directement par la Collectivité. Afin d'assurer un certain niveau de résilience, la Collectivité a pris le parti d'appliquer des mesures de construction sur les infrastructures :

- Un réseau FttH 100% enterré jusqu'aux raccordements : à la suite du passage de l'ouragan IRMA, qui a notamment engendré d'importants dégâts sur les réseaux aériens, la Collectivité a accéléré les chantiers de mise en souterrain. L'enfouissement des réseaux permet de les protéger face au risque récurrent, notamment le risque cyclonique ;
- Des Nœuds de Raccordements Optiques (ci-après « NRO ») construits en béton et surélevés en zones submersibles : ceci permet de renforcer la résistance des NRO face aux aléas climatiques (tsunami, cyclone, etc.) ;
- Les armoires des points de mutualisation (ci-après « PM »), les points de raccordements distants mutualisés (ci-après « PRDM ») et les répartiteurs techniques optiques (ci-après « RTO ») sont hébergés dans les NRO.

Au-delà des règles de construction, la Collectivité a pensé son architecture sur des modèles participant à la résilience des réseaux avec :

- Deux réseaux distincts :
 - Un réseau Fiber to the Home (ci-après « FttH ») nommé St Barth Digital sur lequel les opérateurs commerciaux peuvent fournir des offres de services internet aux habitants de l'île. Il supporte également les offres du réseau FttE (Fiber to the Entreprise) ;
 - Un réseau Fiber to the Office (ci-après « FttO ») nommé Smartfibre. Ce réseau de fibre noire permet aux opérateurs commerciaux de fournir des offres uniquement à destination des professionnels. La collectivité interconnecte ses bâtiments sur ce réseau et les systèmes d'alerte y sont connectés.
- Des liens de transport NRO-PM dimensionnés afin de généraliser les connexions de type point à point : L'avantage de ces connexions est que l'utilisateur bénéficie de sa propre fibre jusqu'au NRO et non jusqu'au PM. Cela permet d'éviter les saturations de débit. Le point à point est également un avantage pour l'opérateur commercial en particulier pour les offres dédiées aux professionnels ;
- Un réseau FttO intégralement bouclé. Cette configuration permet d'assurer une continuité d'accès internet pour les éléments du réseau ;
- Des liens de collecte entre les NRO, les nœuds de raccordement d'abonnés (ci-après « NRA »), et les points d'accès (y compris station d'atterrissage) dimensionnés avec des routes disponibles et activables par simple jarretièrage (mise en place d'une jarretière) au niveau des RTO. En effet, des RTO appartenant à la Collectivité sont installés dans tous les locaux techniques télécom.

2.3.2.1. Le réseau FTTO – Fiber to the Office

La mise en œuvre du réseau FttO, nommé Smartfibre, ouvert à tous les opérateurs a joué un rôle essentiel dans la réduction de la fracture numérique sur le territoire à partir de 2015. En plus de favoriser la concurrence au profit des entreprises locales, cette initiative a renforcé l'attractivité globale de l'île. Le réseau FttO a été conçu dès son origine pour être résilient, avec

2.3.2.2. Le réseau FTTH – Fiber to the Home

La Collectivité est également propriétaire à 100% du seul réseau FttH présent sur l'île. Il couvre tout le territoire et fournit un accès internet à très haut débit à tous les habitants et entreprises. De ce fait, la concurrence entre les fournisseurs d'accès à internet (ci-après « FAI ») permet à la population de bénéficier de prix attractifs et d'un certain niveau de qualité de service.

La collectivité de Saint-Barthélemy a contractualisé avec le groupement Dauphin Telecom et Les Courants Faibles, un marché global de performance (ci-après « MGP ») pour la conception, la réalisation et l'exploitation (maintenance et assistance à la commercialisation comprises) du réseau de desserte FttH. Les parties prenantes de ce contrat sont :

- La collectivité de Saint-Barthélemy : maître d'ouvrage ;
- Le groupement : titulaire du MGP.

À mi-2024, sur un total de 14 zones, 12 sont déjà déployées, une est en cours de déploiement et une est en attente de la finalisation de travaux de génie civil. Le nombre de prises déployées s'élève à 4 831 sur un total de 7 281. La fin du déploiement est prévue dans le courant du premier semestre 2025.

Le taux de disponibilité du réseau est supérieur à 99,9%.

Le réseau est ouvert à tous les opérateurs commerciaux afin de garantir une concurrence au bénéfice de l'utilisateur final.

Sur le réseau FttH, 6 opérateurs télécoms sont présents dont 5 actifs :

- Dauphin Télécom ;
- Igwan.net ;
- Orange ;
- Saint-Barh Telecom ;
- Solutech ;
- Xiwo (inactif à date).

D'un point de vue technique, le réseau optique de la collectivité est 100% souterrain afin de le protéger au mieux des phénomènes cycloniques qui constituent un risque périodique. Ce point marque une différence majeure avec la majorité des réseaux FttH français. De plus, le réseau FttH est conçu de manière à disposer de 100% de réserve (y compris dans les SRO, qui sont des PM1000) jusqu'aux boîtiers situés à l'entrée des poches de 72 locaux afin d'anticiper les nouvelles constructions.

La Collectivité a également fait le choix de localiser ses armoires de sous-répartition dans ses NRO. Le réseau est constitué de 3 NRO situés respectivement à Gustavia, Lorient et Saint-Jean, desservant chacun plusieurs ZAPM. Les 3 NRO seront d'ici à 2025 interconnectés avec des routes dissociées ce qui en fait une infrastructure résiliente.

2.3.2.2.1. Les éléments contractuels résilients

Dans le cadre de ce marché, plusieurs éléments participant à la résilience ont été exigés dans le cahier des charges. Les éléments indiqués ci-dessous sont spécifiques au réseau FttH.

Concernant la maintenance, on distingue :

- La maintenance préventive du Réseau :
 - Contrôles périodiques de l'état du Réseau, notamment selon les prescriptions des équipementiers ;

- Programmation et exécution d'opérations de maintenance préventive : remplacement de câbles et de tout autre équipement optique sans travaux de génie civil, remplacement d'appui, élagage ;
- Analyse d'impact sur les Usagers et information préalable des Usagers impactés pour toute opération de maintenance programmée ;
- Gestion des déclarations de travaux ;
- Analyse a posteriori des incidents pour identifier des mesures de prévention pertinentes.
- La maintenance curative du réseau :
 - Enregistrement des signalisations d'incidents de la part des opérateurs commerciaux (ci-après « OC ») à toute heure, 7 jours sur 7 ;
 - Mise en œuvre des actions correctives avec intervention terrain si nécessaire ;
 - Information des OC sur la gestion des incidents les concernant ;
 - Mise en œuvre d'un processus d'escalade ;
 - Gestion des lots de maintenance ;
 - Analyse a posteriori des performances de traitement des incidents et mise en œuvre de mesures d'amélioration.

Les engagements de GTR sur le réseau FttH et FttE intégrés dans l'offre de référence sont rédigés comme suit :

« Une option de GTR en Heures et Jours Ouvrés peut être souscrite pour chaque Ligne FTTH, soit lors de la Commande de cette Ligne soit ultérieurement sur une Ligne déjà en service.

Toute Ligne FTTE comprend une Garantie de Temps de Rétablissement de 48h, en Heures et Jours Ouvrés. Des options supplémentaires peuvent être souscrites pour chaque Ligne FTTE lors de la commande de la Ligne FTTE ou ultérieurement.

En cas de commande simultanée d'une Ligne FTTH ou FTTE et d'une option GTR, la mise en service de l'option en question est concomitante à la mise en service de la Ligne FTTH ou FTTE. La date de début du Service de la Ligne FTTH ou FTTE vaut également date de début du Service pour l'option.

En cas d'ajout de l'option GTR sur une Ligne FTTH ou FTTE déjà en service, le délai d'activation de l'option est de dix (10) Jours Ouvrés. Un avis de mise à disposition du Service est envoyé sous format électronique par l'OI à l'OC confirmant l'activation de ladite option.

En cas de souscription de cette option, l'OI s'engage, en cas d'interruption totale du service sur cette Ligne, à rétablir le service dans un délai correspondant à l'option souscrite (Annexe 1) :

- *Pour l'option GTR 48h : rétablissement du Service dans un délai de quarante-huit (48) Heures Ouvrées, du lundi au vendredi inclus entre 7h00 et 17h00, hors jours fériés ;*
- *Pour l'option GTR 24h : rétablissement du Service dans un délai de vingt-quatre (24) Heures Ouvrées, du lundi au vendredi inclus entre 7h00 et 17h00, hors jours fériés ;*
- *Pour l'option GTR 10h : rétablissement du Service dans un délai de dix (10) Heures Ouvrées, du lundi au vendredi inclus entre 7h00 et 17h00, hors jours fériés.*

Le délai est comptabilisé de l'ouverture du ticket d'incident complet, dans les conditions de l'article 12.1 ci-avant, et jusqu'à la fermeture par l'OI.

Le délai est suspendu pendant les Heures Non Ouvrées et les Jours Non Ouvrés, ainsi qu'entre les demandes d'informations de l'OI et les réponses de l'OC.

Le dépassement du délai donnera lieu à l'application de pénalités selon l'article 2.4.4 de l'Annexe 1 des présentes.

La GTR individuelle s'applique à l'exclusion des cas suivants :

- *Cas de Force majeure, ayant un impact direct ou indirect sur la durée de réparation ;*
- *Fait d'un tiers ;*
- *Incident sur un équipement sous la responsabilité de l'OC ou du Client Final (SAV ouvert à tort) ;*
- *En d'interruption de Service résultant de Travaux Programmés ;*
- *Nécessité pour l'OI d'obtenir l'autorisation d'un tiers avant intervention sur un domaine public ou privé ;*
- *Erreur de pré-localisation de l'incident par l'OC auteur de la signalisation SAV ;*
- *Infrastructure d'accueil du Câblage Client Final non réutilisable ;*
- *Responsable technique de l'OC injoignable, si l'OI a besoin de précisions indispensables avant intervention ou d'un accès au domaine privé du Client Final.*

L'OC peut résilier à tout moment l'option de GTR souscrite sur une Ligne FTTH ou FTTE, sous réserve du respect d'un délai de préavis de dix (10) Jours Ouvrés. »

Les engagements de GTR sur le réseau FttH et FttE sont les suivants :

« Une option de GTI en huit (8) Heures et Jours Ouvrés peut être souscrite pour chaque Ligne FTTH, soit lors de la Commande de cette Ligne soit ultérieurement sur une Ligne déjà en service. Cette option est incluse pour toute Ligne FTTE.

Les dispositions relatives à la commande, la mise en service et la résiliation de l'option GTI sont identiques à celles des options GTR.

En cas de souscription de cette option GTI, l'OI s'engage, en cas d'interruption totale du service sur la Ligne concernée, à débiter l'intervention en vue de rétablir le Service dans un délai de huit (8) Heures Ouvrées entre 7h00 et 17h00, du lundi au vendredi inclus, hors jours fériés.

Le délai est décompté comme pour les options GTR.

Les cas d'exclusion de la GTI sont identiques à ceux de la GTR.

Le dépassement du délai donnera lieu à l'application de pénalités selon l'article 2.4.4 de l'annexe 1 des présentes. »

À noter que les heures ouvrées (HO) sont comprises entre 7h00 et 17h00, du Lundi au Vendredi.

Tous ces engagements sont disponibles sur le site internet de Saint-Barth Digital (<https://www.stbarthdigital.fr/je-suis-un-operateur#ancrer1>).

Concernant l'accès physique au NRO ([annexe 3 et 4](#)), les locaux, les compartiments en baie, et les SRO sont accessibles 24h/24h, 7j/7j au moyen d'une carte d'accès sans-contact que la COM remet à ses sous-traitants et aux opérateurs clients du réseau.

2.3.2.2.2. Les modalités d'interaction entre la Collectivité et le Titulaire

La résilience est également liée aux modalités d'interaction des différents acteurs.

Au titre du SI permettant la gestion technique du réseau en interne, le Titulaire doit rendre consultables les données pour la Collectivité et permettre le transfert du système d'information FttH et des données au terme de l'accord-cadre.

Au titre de l'exploitation, le Titulaire est en charge de :

- Communiquer aux OC les informations sur le réseau (fichier d'informations préalables enrichies (IPE)) ;
- Contrôler la qualité des raccordements finals établis, le cas échéant, par les éventuels sous-traitants ;
- Assurer la maintenance préventive et curative et reporter sur la qualité de service.

2.3.2.2.3. Les nœuds de raccordement optique permettant l'accès internet

À terme, trois nœuds de raccordements optiques seront mis en place pour l'activation du réseau.

NRO de Lorient

Le NRO de Lorient a été pensé avec des règles d'architecture résilientes :

- Poste électrique présent à moins de 50m ;
- Surélévation de 1 mètre du poste électrique et du NRO pour limiter les risques de submersion marine ;
- Local attenant hébergeant un groupe électrogène de secours avec plusieurs jours d'autonomie.

Le passage de l'ouragan IRMA a confirmé ces choix de construction puisque le NRO de Lorient n'a pas été impacté. Il a permis à la population de disposer de Wifi alors que l'ensemble des réseaux de télécommunications étaient hors services.

À noter que le NRO héberge 5 points de mutualisation et le point d'échange internet (ci-après « IXP »). Il offre également la possibilité aux opérateurs commerciaux de proposer des offres FttE en point à point pour les entreprises.

Bien que de taille réduite (16m² de surface intérieure), ce NRO est un modèle du genre. Son aménagement intérieur lui permet d'accueillir au sein d'une seule salle l'atelier énergie, les SRO, les RTO FttH et FttO, les baies hébergeant les équipements actifs des opérateurs et celles hébergeant le SI de la Collectivité. En service depuis 2015, il est très bien entretenu. Même si certains raccordements sont sous-traités, notamment ceux d'Orange avec un mode STOC (sous-traitance opérateur commercial) limité aux PM, la présence d'un contrôle d'accès à l'entrée et au niveau de chaque compartiment de baie et de caméras de vidéoprotection permet de le conserver dans un très bon état ([voir photos](#)).

Enfin, il est équipé d'un système de GTB et de dispositifs de prévenance en cas d'alerte de dysfonctionnement. Ce système permet de remonter des données de consommation électrique, de température, d'humidité, d'état d'usure des batteries ou d'état de fonctionnement du groupe électrogène et du système de sécurité incendie à gaz.

NRO de Gustavia

Le NRO de Gustavia sera livré d'ici la fin de l'année 2024. Sa livraison a été retardée de 1 an en raison de la survenance d'un incendie d'origine électrique peu de temps avant sa réception en 2023.

Il répond aux mêmes exigences de construction et d'équipements que celui de Lorient (bâtiment en béton armé, présence d'un poste de transformation à moins de 50m, présence d'un groupe électrogène de secours et d'un atelier énergie, GTB, vidéoprotection, contrôle d'accès). En revanche, sa superficie est nettement plus importante que celle du NRO de Lorient ([voir photos](#)). En effet, il s'étend sur une superficie de 100m² sur deux niveaux et propose des salles distinctes, chacune équipées de contrôle d'accès :

- Une salle PM ;
- Une salle opérateurs ;
- Une salle SI COM ;
- Une salle serveurs tiers ;
- Deux salles avec ateliers énergie redondants.

NRO de Saint-Jean

Actuellement en construction, il devrait être livré dans le courant du premier semestre 2025. Inspiré des retours d'expérience et donc des principes de construction et d'équipement des NRO de Lorient et de Gustavia, il sera doté d'une salle de stockage au premier étage. Afin de pallier les difficultés d'approvisionnement dans des délais raisonnables et de pouvoir disposer d'emplacement sécurisé pour y installer le matériel extérieur en cas d'alerte cyclonique, la collectivité a fait le choix de doter ce NRO d'un espace de stockage dédié.

La salle serveurs tiers sera en mesure d'accueillir la station d'atterrissage d'un futur câble sous-marin ayant son point d'arrivée au Nord de l'île.

2.3.2.2.4. Les modalités particulières de commercialisation du réseau FttH

Afin de faciliter le parcours du client final, mais également de s'assurer de la qualité de construction et d'exploitation de son réseau, la collectivité a fait le choix de promouvoir le pré-raccordement comme mode privilégié de construction du câblage client final malgré le risque de non-commercialisation de la prise optique. Laissé au départ à la discrétion des premiers opérateurs clients du réseau entre mode OI, pré-racco ou mode STOC, le mode de commercialisation sur prise pré-raccordée a été très rapidement plébiscité par ces derniers. Il est aujourd'hui adopté par tous les opérateurs commerciaux et le mode STOC, qui ne concerne qu'un seul opérateur, se limite aux seules actions de « jarretière » au PM et s'apparente donc plutôt à une simple opération de churn (ou changement d'opérateur). L'offre de référence de St Barth Digital propose également les prestations de pose et de dépose de jarretière au PM. En cas de résiliation d'un client final, l'opérateur doit impérativement commander la prestation de dépose de jarretière ou la réaliser lui-même dans un délai fixé dans l'offre de référence, faute de quoi la Collectivité la dépose aux frais de l'opérateur défaillant. Cela permet de conserver une armoire SRO dans un état favorable à une bonne exploitation du réseau.

La partie câblage client final est, comme le reste du réseau exclusivement réalisée en souterrain. A l'exception de ceux situés dans les locaux techniques des immeubles, tous les PBO sont positionnés dans des chambres télécom sous voirie ou trottoir. Les administrés sont accompagnés par St Barth Digital en ingénierie pour la pose des fourreaux en domaine privé. Si la réalisation du pré-raccordement est réalisée sans frais, les travaux de pose ou de préparation des infrastructures d'accueil des câbles optique sont à la charge des propriétaires.

Cette approche pragmatique, en application depuis 2021, laisse aujourd'hui penser qu'elle est de nature à accroître la résilience des réseaux FttH en conservant un niveau de qualité du réseau dans un contexte de dynamique commerciale soutenue.

Le nombre de SAV est d'ailleurs éloquent puisque sur 118 incidents déclarés depuis 2021, seuls 66 concernaient des pannes relevant de la responsabilité de St Barth Digital et ont tous été résolus dans un délai de moins de 48h.

La Collectivité a également créé une offre d'accès à la boucle de collecte inter-NRO à tarif préférentiel et attractif pour les opérateurs clients du réseau StBarth Digital afin d'inciter ces derniers à colocaliser leurs équipements dans les NRO et à boucler leur réseau.

2.3.3. Un réseau LoRaWAN en cours de déploiement

La Collectivité a lancé un projet de déploiement de réseau LoRaWAN s'appuyant sur son réseau FttO. Le déploiement a été confié à l'entreprise Solutech.

Ce réseau couvre l'ensemble de l'île avec environ 25 antennes pour offrir une pénétration en « deep indoor ». Ce réseau pourra être renforcé en tant que de besoin. Le réseau est conçu pour être entièrement redondé afin que chaque capteur soit connecté, à minima, à deux antennes.

Le réseau est opérationnel depuis fin juin 2024. Un proof of concept a été lancé depuis début décembre 2023, afin de tester un cas d'usage IoT avec l'installation de 10 compteurs d'eau communicants en partenariat avec la SAUR (pour disposer d'une remontée d'informations deux fois par jour avec des alertes de seuil).

L'objectif, pour ce qui concerne la distribution d'eau potable, est ensuite de généraliser le déploiement de ces compteurs communicants pour tous les abonnés (5 000) et de multiplier les cas d'usage pour l'exploitant du réseau et pour ses clients.

Plusieurs autres cas d'usage sont déjà envisagés à court terme pour répondre aux ambitions de la Collectivité : mesure de la qualité de l'air, mesure du bruit, efficacité énergétique des bâtiments, etc.

2.3.4. Des carences identifiées sur le réseau mobile

La Collectivité de Saint-Barthélemy a fait le choix de raccorder tous les points hauts du réseau mobile en fibre optique. Cette mesure permet d'assurer un certain niveau qualité de service et de résilience. Actuellement, seuls 3 sites mobiles sont équipés de générateurs électriques (TDF Lurin, Aéroport, NRA Gustavia Orange).

De plus, la Collectivité a dressé une liste de contraintes aux opérateurs souhaitant s'installer sur les sites résilients (Pylônes, Shelter, groupes électrogènes).

Cependant, la couverture réseau et le débit ne sont pas suffisants. De plus, les sites mobiles actuels sont encore en majorité mono opérateurs. C'est pourquoi un projet est en cours afin de pallier les carences constatées et de regrouper les opérateurs sur des sites communs. Ce projet vise à créer des sites mutualisés, résilients et intégrés sur les points hauts identifiés collectivement entre les opérateurs mobiles et la Collectivité. Le cahier des charges à respecter pour ces sites intègre les prescriptions suivantes : existence d'un Shelter en béton, présence d'un groupe électrogène, supports d'antennes sur bâti ou sur mâts de moins de 4 mètres. Dans ce contexte, la Collectivité met à disposition le foncier nécessaire pour le déploiement du projet ([lien vers le chapitre](#)).

2.3.5. Un projet d'IXP sur Saint-Barthélemy motivé par la coopération régionale

2.3.5.1. Un projet coconstruit dans une démarche de résilience

Le projet CaribIX consistait à construire et à mettre en réseau les îles de la Guadeloupe, de Saint-Martin et de Saint-Barthélemy en construisant des Points d'échange Internet (ci-après

« IXP ») afin d'améliorer la qualité du réseau internet et donc de participer à l'attractivité de ces territoires.

Un IXP est un point d'échange internet physique. Il permet aux différents opérateurs et réseaux privés de se connecter entre eux pour échanger directement de la donnée. Grâce à cette infrastructure, les communications sont plus rapides et plus efficaces. Cela permet également d'éviter de passer par des intermédiaires et donc de réduire les coûts.

L'arrivée de l'IXP permet de réduire les coûts liés au trafic internet. En effet, un territoire sans IXP doit échanger via un lien international (États-Unis ou Europe) ce qui engendre des frais élevés. De plus, les IXP renforcent la résilience des territoires en garantissant un certain niveau de sécurité en cas de coupure de câbles.

Ce projet a été cofinancé par le programme INTERREG Caraïbes et par le Fonds Européen de Développement (FED) de l'Union européenne. Il regroupait les acteurs suivants :

- L'Union des télécommunications des Caraïbes (ci-après « CTU »). Son rôle est d'assurer la supervision du programme, de fournir des conseils techniques et des conseils sur tous les aspects liés à la mise en place et la croissance des IXP. Il s'agit d'une organisation intergouvernementale à but non lucratif créée par les chefs de gouvernement des Caraïbes (traité avril 1989). Elle est actuellement composée de 20 pays membres. Ses missions portent sur la promotion et le développement des technologies de l'information et de la communication (ci-après « TIC ») des Caraïbes afin d'assurer le développement socio-économique de la région.
- Caribbean Network Operators Group (ci-après « CaribNOG ») : il s'agit d'un groupe d'opérateurs de réseaux qui échangent des informations techniques et réalisent des retours d'expériences liées à la gestion des réseaux IP dans la région des Caraïbes.
- Dauphin Telecom qui a pour rôle de coordonner les différents acteurs du projet ;
- Les Collectivités de Saint-Barthélemy et de Saint-Martin et la Région Guadeloupe qui sont les trois collectivités ayant mis en place un IXP sur leur territoire.
 - Saint-Martin avec Smart-IX : le point d'échange est actif depuis le 25 octobre 2022 ;
 - La Guadeloupe avec GUAD-IX : projet prêt à être déployé (dans le cadre de la DSP sur le câble sous-marin GCN) ;
 - Saint-Barthélemy avec SBH-IX : le point d'échange est actif depuis le 30 juin 2022.

Malgré le déploiement de ces IXP, ces derniers ne fonctionnent pas encore comme prévu en raison de contraintes liées au personnel et à la taille du marché. Ils ne sont pas encore interconnectés et opèrent donc indépendamment sur les sujets de gouvernance, d'offres de services et de solutions techniques.

Une structure commune pour gérer ces IXP serait pertinente à mettre en place. La structure pourrait récupérer les points d'échange Internet existants et créer ceux qui manquent afin de développer une offre commerciale autonome sur le marché de gros.

En interconnectant les IXP de chaque île, cela permettrait de créer un marché plus vaste pour attirer de nouveaux fournisseurs de services en Cloud et de contenu avec des normes de performance et de qualité adéquates, comparables à celles de l'hexagone.

Pour porter ce projet, la cible est d'avoir un partenaire de confiance : sans but commercial, qui offre de la disponibilité et des services aux territoires, de manière indépendante et neutre.

2.3.5.2. SBH-IX, le point d'échange de Saint-Barthélemy

Le point d'échange de l'île a été mis en place en juin 2022 dans le cadre du projet CaribIX. Il a pour objectif d'améliorer la fiabilité du réseau de télécommunication et l'expérience de services des opérateurs et utilisateurs. Cet IXP va permettre de faciliter l'interconnexion des réseaux des différents FAI présents sur le territoire. La mise en place de SBH-IX participe également à la résilience des réseaux puisqu'il garantit une continuité d'accès aux services locaux en cas de coupure du câble sous-marin.

Actuellement, seuls les opérateurs Canal+ Télécom, Igwan.net, Solutech et Dauphin Telecom, ainsi que la Collectivité, sont présents dans SBH-IX. Le projet SBH-IX en est donc encore à ses prémices en termes de fonctionnement.

Il est nécessaire de développer cet IX afin d'accroître la résilience du territoire, de réduire les coûts de l'internet local et d'améliorer le service rendu aux usagers du réseau. L'objectif serait notamment que des grandes entreprises du numérique puissent proposer des services personnalisés avec des temps de latence réduits.

Pour pouvoir se connecter à SBH-IX, les opérateurs doivent avoir un routeur Internet sur l'île ou une connexion dédiée entre un routeur d'une île voisine et SBH-IX (ce qui n'assure pas la résilience en cas de perte d'un ou plusieurs câbles).

Dauphin Telecom et St-Barth Telecom sont techniquement capables de se raccorder, Orange, Free Caraïbes et Digicel ne disposent pas actuellement des équipements nécessaires sur place.

2.3.6. Un réseau électrique résilient

Les réseaux de télécommunications présentent une forte dépendance avec le réseau électrique. Sans alimentation, les infrastructures télécoms ne peuvent assurer une continuité de service.

Sur l'île, la Collectivité est propriétaire du réseau électrique. Cependant, la gestion et l'exploitation du réseau de distribution (postes de transformation, réseaux moyenne et basse tension) ont été confiées à EDF SEI via un contrat de concession.

Suite au passage de l'ouragan IRMA, des travaux ont été effectués sur le réseau électrique afin de renforcer sa résilience. À date :

- 100% des câbles moyennes tensions (HTA) sont enterrés ;
- 90% des réseaux basse tension sont enterrés ;
- ¼ des postes ont moins de 5 ans.

Dans les zones submersibles, les postes de transformation et les coffrets (Raccordement Emergent Modulaire Basse Tension, ci-après « RMBT » et comptages) sont surélevés de 1 m et ils sont renforcés avec du béton ([voir photo](#)).

Sur toute l'île, la plupart des coffrets sont encastrés dans des murs en béton.

Les travaux de reconstruction sont en cours de finalisation. Ils ont été cofinancés par l'Etat à hauteur de 80% dans le cadre du FACE⁷. La maîtrise d'ouvrage a été partagée entre la Collectivité et le concessionnaire EDF SEI.

⁷ Initialement nommé Fonds d'amortissement des charges d'électrification et rebaptisé Financement des aides aux collectivités pour l'électrification, le FACE est une aide de l'Etat qui permet notamment la prise en compte des conséquences des aléas climatiques

2.4. Des dispositifs de sécurité informatique de la collectivité à améliorer

La collectivité va réaliser dans le courant de l'année 2024 un audit cybersécurité, selon les recommandations de l'Agence nationale de la sécurité des systèmes d'information (ci-après « ANSSI »). Cet audit permettra de compléter les constatations effectuées par la collectivité, décrites ci-dessous.

2.4.1. Des risques informatiques identifiés⁸

Au travers d'une carte des risques, la collectivité a identifié 16 menaces avec un risque élevé. Pour chaque menace, il a été précisé les impacts sur le système et les actifs, la probabilité d'apparition, le niveau de risque, les contrôles et mesures préventives et les recommandations de contrôles.

Parmi ces risques, on retrouve les risques liés à des :

- Catastrophes naturelles : inondation et submersion marine ;
- Défaillances techniques : système de climatisation, fournisseur d'électricité, incendie ;
- Défaillances des systèmes de télécommunications : les réseaux internet, les réseaux téléphoniques, les réseaux de fibres optiques de la collectivité, défaillances des matériels serveurs ou DNS ;
- Défaillances logicielles ;
- Cyberattaques : déni de service (DDoS), virus ;
- Actions humaines : volontaires ou accidentelles.

2.4.1.1. Les défaillances techniques – Mesures préventives en place

Dans une démarche de lutte contre les défaillances techniques, la Collectivité a mis en place des actions correctives pour :

- Les défaillances liées aux systèmes de climatisation :
 - Mise en place systématique de deux climatisations indépendantes ;
 - Mise en place de groupe électrogène pour secourir les locaux critiques.
- Les défaillances liées au réseau électrique :
 - Mise en place d'onduleurs généraux / bâtiments ;
 - Mise en place de Groupe électrogène pour secourir les locaux critiques ;
 - Sauvegardes quotidiennes sur un site distant ;
 - Mise en place d'onduleur de baies pour les différents bâtiments (baies NRO/cœurs de réseaux, baies bâtiments Collectivité).

2.4.1.2. Les défaillances matérielles – Mesures préventives en place

Afin de lutter contre le risque de défaillance du serveur ou du NAS, la Collectivité effectue :

⁸ Cartes_Risques_SI_2024

- Le réapprovisionnement progressif de disques durs de secours pour les serveurs et NAS ;
- Le choix d'un système RAID 1 + 0 pour les disques durs et NAS ;
- La mise en place progressive de serveurs avec double alimentation ;
- Le remplacement progressif des serveurs vieillissants et/ou obsolètes par de nouveaux serveurs ou par virtualisation ;
- Des sauvegardes quotidiennes sur un site distant.

2.4.1.3. Les défaillances logicielles – Mesures préventives en place

Dans le cas de défaillances logicielles liées aux applications métiers, il est mis en place des mesures consistant à :

- Effectuer et suivre la maintenance préventive ;
- Analyser le problème et effectuer la maintenance corrective le plus rapidement possible ;
- Sauvegarder quotidiennement les données sur un site distant.

2.4.1.4. Les risques de cyberattaque- Mesures préventives en place

Des mesures préventives sont en place pour deux types de cyberattaques :

- Attaques par Déni de Service (DDoS) :
 - Configuration correcte du pare-feu (limitations des droits d'accès, règles de filtrage) ;
 - Segmentation en sous-réseau / VLANs ;
 - Choix d'hébergeur de qualité.
- Attaque par virus :
 - Antivirus à jour mis à jour régulièrement ;
 - Analyses antivirus régulières des postes clients, des serveurs, des médias lors de leur insertion ;
 - Antispam Cloud en amont du serveur de messagerie, mis à jour régulièrement
 - Configuration correcte pare-feu (limitations des droits d'accès, règles de filtrage) ;
 - Segmentation en sous-réseaux / VLANs ;
 - Sauvegardes quotidiennes sur un site distant ;
 - Mise à jour régulière des systèmes d'exploitation ;
 - Mise à jour régulière des firmwares équipements réseaux.

La Collectivité a mis en place des mesures préventives afin de lutter contre les actions humaines. Elles sont détaillées ci-dessous.

Actions humaines accidentelles

- Suppression de fichiers :
 - Surveiller et configurer les autorisations et limitations d'accès aux ressources et règles de filtrage, les utilisateurs privilégiés et les sauvegardes ;
 - Sauvegardes quotidiennes sur un site distant ;

- Système de cliché instantané en place sur les serveurs de données permettant une restauration à 2 points par jours.

Actions humaines volontaires

- Tentative d'intrusion sur le réseau du Système d'information de la Collectivité :
 - Antivirus à jour mis à jour régulièrement ;
 - Analyses antivirus régulières des postes clients, des serveurs, des médias lors de leur insertion ;
 - Antispam Cloud en amont du serveur de messagerie, mis à jour régulièrement ;
 - Configuration correcte pare-feu (limitations des droits d'accès, règles de filtrage) ;
 - Segmentation en sous-réseaux / VLANs ;
 - Liens VPNs inter-sites ;
 - Complexité mot de passe équipements réseau ;
 - Politique de mot de passe / accès utilisateur poste de travail ;
 - Sauvegardes quotidiennes sur un site distant ;
 - Mise à jour régulière des systèmes d'exploitation ;
 - Mise à jour régulière des firmwares.
- Tentative de piratage :
 - Antivirus à jour mis à jour régulièrement ;
 - Analyses antivirus régulières des postes clients, des serveurs, des médias lors de leur insertion ;
 - Antispam Cloud en amont du serveur de messagerie, mis à jour régulièrement ;
 - Surveiller et configurer les autorisations et limitations d'accès aux ressources et règles de filtrage, les utilisateurs privilégiés et les sauvegardes ;
 - Sauvegardes quotidiennes sur un site distant ;
 - Mise à jour régulière des systèmes d'exploitation.
- Vol ou dégradation de matériel à disposition des utilisateurs :
 - Le service informatique dispose du listing du matériel mis à disposition des utilisateurs, ainsi que des affectations ;
 - Les responsables de service ont la responsabilité de leurs agents ;
 - Sauvegardes quotidiennes sur un site distant.
- Vol ou dégradation de matériel réseau ou serveur :
 - Les matériels réseaux et serveurs sont dans des zones sécurisées, et il faut avoir une autorisation d'accès au préalable, permettant de savoir qui est intervenu dans ces zones.

2.4.2. Une prise en considération de la sécurité des données

Concernant la sécurité des données, la collectivité dispose d'un document de présentation des outils de sécurité logique et d'une procédure de gestion des accès aux équipements informatiques. Cependant elle ne possède pas de procédure de sécurité propre au système d'information.

2.4.3. Des mesures de sécurité logique⁹

Pour différents domaines d'application, la collectivité a recensé les mesures et les outils de sécurité mis en place. Parmi ces domaines on retrouve :

- L'accès au poste de travail ;
- La mise à jour de sécurité et du système d'exploitation ;
- L'antivirus ;
- L'antispam ;
- Les réseaux et pare-feu ;
- Les applications logiciels métiers associées à des bases de données ;
- Les moyens de sauvegarde.

2.4.4. Des procédures d'accès physique en place¹⁰

La collectivité a mis en place une procédure afin de gérer les accès aux différentes salles informatiques. À noter que cette procédure est en cours d'amélioration avec notamment l'ajout du contrôle d'accès via des badges pour accéder aux salles serveurs des sites locaux (hors NRO).

2.4.5. Une absence de processus de continuité de l'activité

La collectivité de Saint-Barthélemy dispose de procédures de sauvegarde des données et de restauration des données.

Cependant, elle ne dispose pas de plan de reprise ni de plan de continuité informatique. Les seules mesures sont référencées dans la carte des risques SI.

2.4.6. L'agence Caribéenne pour la Cybersécurité, une réponse au risque cyber

L'agence caribéenne pour la cybersécurité (ACCYB) a été créée en 2022 à l'initiative conjointe de ses membres fondateurs : collectivité territoriale de Guyane, région Guadeloupe et collectivité d'outre-mer de Saint-Barthélemy.

Fin 2023, la collectivité d'outre-mer de Saint-Martin a rejoint l'ACCYB. À ce jour, plusieurs entités publiques et privées de ces territoires sont membres de l'ACCYB.

Dans le cadre de ses missions, l'agence contribue à :

- La représentation des réalités des territoires français d'Amérique auprès des acteurs nationaux, européens et de la zone d'intérêt Caribéenne.
- L'acculturation du grand public et des acteurs privés et publics aux enjeux de cybersécurité et le développement de dispositif de formation adapté ;
- L'observatoire de la Cybersécurité ;

⁹ Outils_Securite_Logique_COMSBH_2024

¹⁰ Procedure acces equipements informatiques COM SBH

- La souveraineté et la résilience pour que les infrastructures du territoire soient les plus résistantes possible en cas de crise ;
- La création et le pilotage du centre de secours unique : Computer Security Incident Response Team (CSIRT). Il s'agit d'un centre de réponse aux incidents cyber dédiée aux particuliers et professionnels qui permettra de signaler une attaque et bénéficier d'un accompagnement.

L'agence travaille également avec Saint-Barthélemy sur l'optimisation de l'IXP ([lien vers le chapitre](#)).

3. PHASE 3 – DES SOLUTIONS ET DES SCÉNARIOS D'INTERVENTION POUR AMÉLIORER LA RÉSILIENCE

L'audit territorial a permis de dresser une évaluation exhaustive des réseaux télécoms, du système d'information et des risques auxquels ils sont exposés. En réponse aux faiblesses identifiées et aux possibilités d'amélioration, des solutions appropriées doivent être mises en œuvre. Ce chapitre présente les solutions et les scénarios d'intervention élaborés à partir de ces éléments.

3.1. Des outils numériques au service de la réduction des risques de catastrophes

3.1.1. Développer les systèmes d'alerte à la population

3.1.1.1. Les systèmes d'alerte de la collectivité

Comme vu précédemment, la collectivité de Saint-Barthélemy a mis en place à travers son réseau FTTO, des coffrets de rue connectés au réseau privé de la Collectivité permettant d'y brancher simplement sur un switch en PoE des points wifi, des haut-parleurs et des sirènes d'alerte pour prévenir la population.

Afin d'améliorer la résilience et l'efficacité des systèmes d'alerte, plusieurs actions sont envisagées. Tout d'abord, le renforcement du réseau de sirènes d'alerte et de haut-parleurs sera entrepris. Ces nouvelles installations seront intégrées au réseau FTTO pour garantir une communication rapide et efficace. De plus, un programme régulier de maintenance et de mise à niveau sera mis en place pour assurer le bon fonctionnement des équipements existants et nouvellement installés.

En parallèle, l'amélioration de la connaissance de la population des points wifi résilient sera une priorité. Des campagnes de sensibilisation pourront être mise en place pour informer la population de l'existence des points wifi et de leur utilisation en cas d'urgence.

Enfin, la formation de la population sera intensifiée. Des sessions de formation régulières seront organisées pour éduquer la population sur les procédures à suivre en cas d'alerte, ainsi que sur l'utilisation des sirènes, des haut-parleurs et des points wifi. De plus, des exercices de simulation d'urgence seront conduits périodiquement pour tester l'efficacité des systèmes d'alerte et la réactivité de la population. Ces exercices permettront d'identifier les points à améliorer et de renforcer la préparation des résidents.

En mettant en œuvre ces actions, la collectivité de Saint-Barthélemy vise à renforcer significativement la résilience de ses infrastructures numériques et à assurer une meilleure préparation et réponse en cas d'urgence.

3.1.1.2. Le système de l'État FR-Alert

Afin d'améliorer l'alerte à la population en cas d'événements majeurs, l'État déploie le dispositif FR-Alert.

FR-Alert est un dispositif d'alerte et d'information des populations. Déployé sur le territoire national depuis fin juin 2022, il a été testé en conditions réelles à Saint-Martin et à Saint-Barthélemy le 20 juin 2024 lors d'un exercice cyclone conjoint collectivité/préfecture. FR-Alert permet de prévenir en temps réel toute personne détentricrice d'un téléphone portable et présente dans une zone de danger afin de l'informer des comportements à adopter pour se protéger.

Les services de l'État ont travaillé depuis plusieurs mois avec les opérateurs locaux tels qu'Orange, Dauphin Télécom, UTS, Free ou Digicel pour permettre le déploiement de ce dispositif sur les deux îles.

L'utilisation de FR-Alert à Saint-Barthélemy est limitée par des éléments liés à sa gouvernance. L'État est aujourd'hui la seule autorité capable de déclencher une alerte.

Cependant la Collectivité souhaiterait pouvoir utiliser le dispositif pour communiquer elle-même à la population. Il est donc nécessaire de définir le cadre d'utilisation du dispositif en partenariat avec la Préfecture.

3.1.2. La création d'un centre de veille pour une meilleure résilience

Afin d'améliorer significativement la résilience du territoire, la Collectivité a engagé un projet de construction d'une nouvelle caserne pour son Service Territorial d'Incendie et de Secours). Ce nouveau bâtiment hébergera le centre de traitement des appels (ci-après « CTA ») dont le rôle sera de recevoir, authentifier et enregistrer les appels 18/112 émis à Saint-Barthélemy. Grâce à un outil informatique en réseau appelé Système de Gestion Opérationnelle (ci-après « SGO »), le CTA transmet automatiquement l'alerte aux sapeurs-pompiers (volontaires ou professionnels) disponibles.

Les opérations de secours et les communications seront alors coordonnées, en temps réel, par le personnel du Centre Opérationnel Territorial d'Incendie et de Secours (COTIS). Situé dans les mêmes locaux que le CTA, le COTIS aura pour mission de veiller à la synchronisation des moyens humains et matériels. Les opérateurs du CTA/COTIS auront en charge d'informer la chaîne de commandement du STIS et ses autorités de tutelle. Ils seront ainsi en liaison avec le centre 15, l'hôpital, la police territoriale, la gendarmerie.

Les opérateurs disposeront également d'un système d'informations géographiques (SIG) qui, combiné au Système de Gestion de l'Alerte (SGA), permettra de localiser précisément une personne, une voie, un bâtiment, un terrain ou encore un véhicule de secours équipé de GPS, par exemple.

La Collectivité souhaite mutualiser le CTA/COTIS avec le Centre de Supervision Urbain (CSU) et ainsi créer son Centre de Veille Territorial doté d'outils numériques permettant d'agrèger tous types de données (alerte météo, alerte incendie dans les NRO, capteurs environnementaux, flux vidéo, etc.) provenant de sources diverses et visualisables sur un mur d'images.

Dans le cadre du déclenchement d'un plan de secours, une « salle de débordement » peut être activée, par du personnel spécifiquement formé, afin de répondre en priorité aux appels liés à l'événement.

En cas d'événement inhabituel, de grande ampleur ou de catastrophes naturelles, les opérations de secours sont coordonnées depuis une salle aménagée attenante, dédiée à la gestion de crise avec report visuel des contenus et informations du CVT. Le Centre Opérationnel Territorial est alors activé.

La livraison de la nouvelle caserne est prévue dans la première partie du 2^{ème} semestre 2024. Le CVT totalement équipé sera livré dans le courant de l'année 2025.

3.2. Améliorer le niveau de résilience des réseaux

3.2.1. Le devenir et l'amélioration des systèmes de câbles sous-marins

3.2.1.1. Évolution du système Global Caribbean Network (GCN)

3.2.1.1.1. Renouvellement de la DSP GCN

Pour rappel, la DSP du câble GCN arrive à son terme en mars 2025. L'échéance étant courte, il est indispensable que les collectivités de Saint-Barthélemy, de Saint-Martin et la Région Guadeloupe travaillent ensemble sur le sujet.

Les collectivités de Saint-Barthélemy et de Saint-Martin ont adressé un courrier à la Région sur le sujet en juin 2024, elles sont en attente d'un retour.

À date plusieurs scénarios sont envisageables pour le renouvellement de la DSP avec notamment une possibilité de déléguer la compétence à la Région Guadeloupe ou d'avoir recours à un groupement d'autorités concédantes. Toutes les possibilités devront être étudiées en collaboration avec les autres collectivités de la zone Antilles Guyane.

3.2.1.1.2. Local GCN Shell Beach

De nombreuses défaillances ont été constatées dans le local : systèmes de climatisation et d'incendie, défaut d'entretien du groupe électrogène, etc. ([voir photos](#)).

Il est recommandé d'abandonner ce local situé en zone submersible et au sein duquel il n'est pas envisageable d'engager des travaux de rénovation en site occupé. Ce déménagement des équipements de GCN ne pourra être réalisé tant que le NRO de Gustavia ne sera pas livré.

3.2.1.1.3. Local GCN Police

Au vu de l'état de ce deuxième local, il est recommandé d'engager des travaux de remise en état sur les aspects suivants : étanchéité, peinture, plancher technique, atelier énergie.

Toutefois ces travaux ne pourront être planifiés que lorsqu'il sera possible d'accueillir les équipements de GCN et des opérateurs tiers, dont SCF et SSCS au sein du NRO de Gustavia et ainsi de disposer d'un local vide. L'opérateur Canal+ Telecom dispose encore d'une ferme cuivre pour le dégroupage du NRA Orange de Gustavia avec des clients actifs. Il est donc indispensable d'aviser l'opérateur de la rénovation de ce local qui l'obligera à fermer son service DSL ou à trouver une alternative car il ne sera pas possible de migrer cette ferme dans le NRO de Gustavia qui est situé trop loin du NRA Orange.

Une fois rénové, ce local pourra éventuellement être réaffecté pour l'hébergement d'équipements d'opérateurs télécom spécifiques ou pour les besoins de la Collectivité. Ce local est secouru par le groupe électrogène de la Police Territoriale et n'est pas situé en zone submersible. Il est donc particulièrement disposé à demeurer un espace dédié à l'activation des réseaux de télécommunications.

3.2.1.2. Projet de troisième câble sous-marin

3.2.1.2.1. Enjeux pour Saint-Barthélemy

Les Caraïbes sont connectées à internet via de nombreux câbles sous-marins. Cependant, chaque île ne dispose que d'un ou deux points d'interconnexion, ce qui constitue un point de défaillance unique.

À Saint-Barthélemy, l'état actuel de la connexion externe à l'île, à travers les câbles GCN et SSCS, n'est pas satisfaisant pour les acteurs du territoire, qui constatent l'existence d'un point de défaillance unique. En effet, ces câbles ont le même point d'atterrissage à Gustavia, Shell Beach. Dans une optique de résilience des réseaux, il serait préférable que ces câbles arrivent à deux endroits différents sur l'île.

Par ailleurs, ces câbles posent des limites et sont source de mécontentements concernant les prix pour les plus petits opérateurs, ainsi que la disponibilité et la qualité des réseaux. La bande passante sur les câbles supporte les coûts de maintenance du système de câbles. Le marché est relativement opaque et les prix observés sont de 10 à 50 fois supérieurs à ceux pratiqués dans l'UE continentale, en partie à cause d'une mauvaise efficacité opérationnelle.

Un troisième câble serait nécessaire pour pallier les limites identifiées. Ceci permettrait de réduire une partie des risques tout en dédoublant les accès à l'internet mondial.

Une structure de portage commune avec les îles voisines, ayant des besoins communs, serait pertinente sur ce sujet.

3.2.1.2.2. Structure de portage ad-hoc

L'objectif est de trouver une solution pour pallier les obstacles actuels. Cela pourrait passer par la mise en place d'une ou plusieurs structures de coopération, facilitant la mise en place d'un nouveau câble entre les acteurs régionaux, aidant chaque membre à bénéficier de développements et d'investissements communs, tout en promouvant l'innovation et en limitant les impacts écologiques.

Les points d'échange Internet ont été encouragés par l'Internet Society et la CTU et soutenus par les gouvernements locaux, mais ils sont fragmentés en termes de gouvernance, d'offres de services et d'aspects techniques. Ils ne sont pas encore interconnectés.

La création d'une structure de portage permettrait de regrouper, dans une seule entité, les IXP et les projets de systèmes câblés afin de maximiser leur utilité, de minimiser les coûts et d'établir des dispositions pour leur maintenance, leur remplacement et les nouveaux déploiements par le biais d'une activité commerciale saine.

La structure proposée devra permettre de gérer les IXP et les systèmes câblés afin de gagner en compétences et de réaliser des économies d'échelle.

3.2.1.2.3. Financements mobilisables

Les coûts pour la future structure pour les ressources humaines envisagées sont estimés à 4-500 k€/an tout compris. Les coûts d'infrastructure devraient pouvoir être maintenus en dessous de 100 k€/an. Les événements ponctuels organisés par la future structure sont estimés à 60 k€/an, progressivement couverts par les cotisations des membres.

L'Europe finance les projets de câbles télécoms au travers de trois programmes :

- INTERREG ¹¹: programme qui a pour but de promouvoir la coopération entre les régions européennes et le développement de solutions communes ;
- Connecting Europe Facility (CEF) : Mécanisme pour l'interconnexion en Europe notamment en matière de télécommunications, qui vise à une plus grande connectivité entre les États membres de l'UE ;
- BELLA ¹²(Building the Europe to Latin America and the Caribbean) : programme cofinancé par la Commission Européenne visant à renforcer et étendre l'écosystème numérique de l'Amérique latine et des Caraïbes en reliant ces territoires au continent européen.

Dans le cadre du projet d'un troisième câble sous-marin, il sera possible de mobiliser à minima un des trois fonds (ou les trois en fonction du statut des partenaires du projet).

À noter que les câbles sont subventionnés, par ces trois programmes, mais leur modèle commercial inclut rarement leur cycle de vie global, comme la redondance et le remplacement.

Le coût d'investissement du projet étant très élevé, il est essentiel d'étudier la mise en place d'une structure de portage ad-hoc.

La Banque des territoires finance également ce type d'infrastructure à travers des investissements auprès de sociétés de projets et en prêts aux collectivités.

Les recettes proviendraient des éléments suivants :

- Des financements européens et d'organismes publics étatiques (banque des territoires, gouvernements, financement local) pour initier les premiers événements et les mises en œuvre techniques concernant les IXP. Le financement couvre principalement les ressources humaines jusqu'à ce que la structure soit autonome grâce aux cotisations des membres et aux abonnements aux services des opérateurs de réseaux ;
- Des cotisations des membres de la structure de portage ;
- Des redevances de la DSP GCN si celle-ci est transférée à la future structure ;
- Des frais de service (environ 400 k€/an pour le peering, le transit partiel et les cours de formation).

3.2.2. L'évolution des réseaux de fibre optique

3.2.2.1. Le devenir des réseaux FttO et FttH

Le marché global de performance en cours pour FttH se terminera fin 2026.

L'exploitation technique du réseau Smartfibre est assurée par le biais d'un marché de maintien en condition opérationnelle. Les extensions et les raccordements finals sont réalisés dans le cadre d'un marché de travaux. Tous deux devront être relancés à la fin de l'année 2026.

¹¹ <https://www.interregeurope.eu/>

¹² <https://bella-programme.eu/en/>

En anticipation de l'échéance de fin 2026, la Collectivité doit d'ores et déjà porter des réflexions sur le devenir de la gestion des réseaux dont elle est propriétaire, y compris de ses NRO. Plusieurs possibilités sont envisageables :

- Relancer un marché global de performance englobant les deux réseaux avec allotissement ou non, ou bien pour chacun d'eux, alloti ou non ;
- Gérer les réseaux en régie pour la commercialisation et en marchés simples pour les extensions, raccordements et la MCO ;
- Déléguer le service public télécom dans le cadre d'une ou de deux concessions.

Toutes ces options doivent être étudiées de manière anticipée dès la fin de l'année 2024 afin d'assurer une continuité de service pérenne et résiliente.

3.2.2.2. Les nœuds de raccordements optique (NRO)

Au-delà des travaux de réparation à réaliser dans les deux locaux actuellement occupés par GCN, il est essentiel d'envisager une perspective d'utilisation des salles serveurs tiers pour offrir des perspectives commerciales aux entreprises locales. En effet, ces salles serveurs peuvent fournir des capacités de stockage de données et d'hébergement de sites internet en local par exemple, ce qui représenterait une opportunité significative pour les entreprises de Saint-Barthélemy.

En développant cette infrastructure, les entreprises locales pourraient bénéficier de services de stockage de données sécurisés, de solutions d'hébergement de sites web robustes, et d'une réduction des coûts associés à l'utilisation de serveurs distants. De plus, cela permettrait de diminuer la latence, d'améliorer la vitesse d'accès aux données pour les utilisateurs locaux et d'assurer la souveraineté des données.

Par ailleurs, l'utilisation de ces nœuds de raccordements optiques pourrait répondre aux besoins spécifiques de la collectivité, notamment en intégrant des solutions basées sur l'intelligence artificielle (ci-après « IA »). L'IA pourrait par exemple être exploitée pour optimiser la gestion des infrastructures, prévoir les besoins en maintenance, et améliorer la résilience des réseaux. De plus, ces technologies pourraient être utilisées pour développer des services publics innovants, comme des systèmes de surveillance intelligents, des outils de gestion de crise, et des applications pour l'amélioration de la qualité de vie des résidents.

Les NRO de la collectivité offrent donc une multitude de possibilités pour le développement économique local, l'amélioration des services publics, et le renforcement de la résilience numérique de la collectivité.

3.2.3. Vers un réseau mobile plus résilient

Le passage de l'ouragan IRMA a révélé la nécessité de prendre des mesures sur le réseau mobile. Afin d'assurer la continuité des services de télécommunications, il est recommandé de mettre en place une solution d'itinérance mobile locale (roaming local). Cela implique que les opérateurs présents sur l'île doivent router les communications au sein de l'île via le réseau d'accès radio (ci-après « RAN » pour Radio Access Network en anglais). Pour aller plus loin, il est possible de faire du RAN Sharing total, c'est-à-dire que les opérateurs mutualisent leur réseau sur une antenne. Sur ce sujet, un courrier en date du 23 mai 2024 a été communiqué à l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ci-après « l'ARCEP ») par la Collectivité.

De plus, du fait de l'incapacité des acteurs privés à acquérir du foncier à Saint-Barthélemy, la collectivité construit sous sa maîtrise foncière, les points hauts du réseau mobile.

L'opérateur Dauphin Télécom va renforcer la couverture mobile sur l'île au travers du projet O27 en partenariat avec la Banque des territoires (groupe Caisse des dépôts). Celui-ci permettra d'améliorer la résilience du territoire et de répondre aux exigences de l'ARCEP.

En effet, la couverture mobile actuelle et la qualité de service sont en deçà des exigences de l'ARCEP. Ce projet permettra également de :

- Assurer la communication entre les habitants, notamment lors de catastrophes naturelles ;
- Désenclaver le territoire en l'intégrant dans le tissu national ;
- Renforcer l'activité économique avec le développement commercial grâce notamment à une communication et un accès à l'information fluide et fiable.

Ce projet en est à ses débuts. Le commencement de la phase de construction est prévu en avril 2026 et la livraison des ouvrages en mars 2028. 9 sites, identifiés comme résilients, sont concernés. En complément, au minimum 6 autres points hauts dits « secondaires » ont été identifiés. Le coût moyen pour un site est de 509 k€.

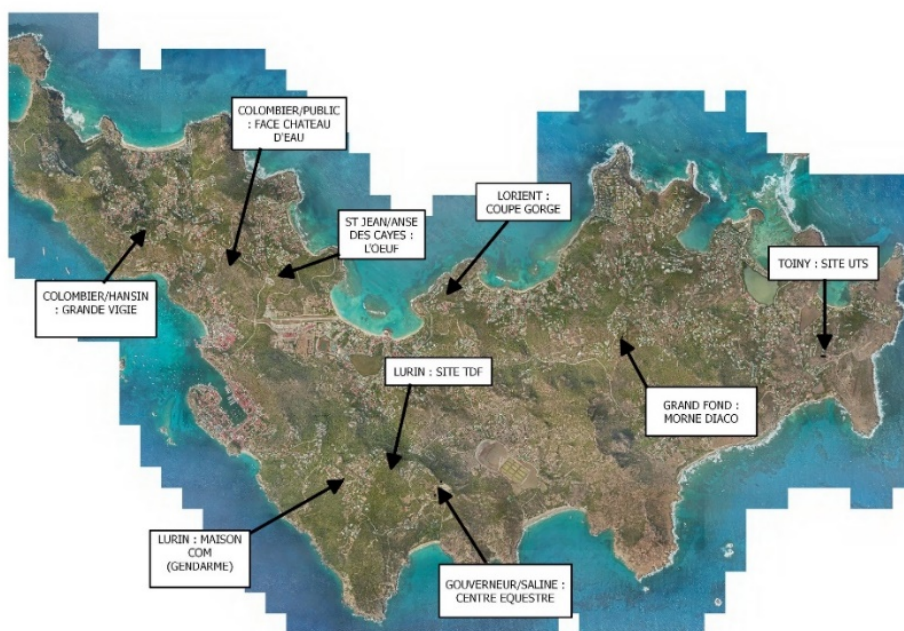


Figure 15 : Cartographie des 9 sites résilients identifiés

3.2.4. Le point d'échange SBH-IX à exploiter pour une meilleure résilience

3.2.4.1. La création d'un cœur de réseau

À la suite du passage de l'ouragan IRMA, Saint-Barthélemy a identifié des mesures à mettre en place afin d'assurer une continuité de service pour les communications.

Cette continuité de service peut être assurée par :

- Le routage local des numéros d'urgence : ce système permettra l'accessibilité et la fonctionnalité des numéros d'urgence (pompiers, Samu, police, etc.) même en cas d'isolement total d'île ;
- L'interconnexion locale des systèmes voix fixe et mobile : ceci est possible que si les opérateurs interconnectent localement leurs réseaux et qu'ils routent et commutent localement les communications internes.

Cependant la mise en place de ces mesures ne peut se faire sans router par l'IXP. Mais pour permettre ce routage, il est nécessaire que les opérateurs installent un cœur de réseau à Saint-Barthélemy. De cette façon, les communications seront assurées même en cas d'isolement de l'île, étant donné que, dans des situations à risque, l'urgence est de maintenir informée la population.

Les opérateurs indiquent que les coûts sont élevés et la rentabilité n'est pas assurée. Pour surmonter ces réticences, il est crucial de proposer une stratégie incitative ou contraignante. Une approche pourrait être d'offrir des subventions ou des incitations fiscales aux opérateurs qui investissent dans l'infrastructure nécessaire. Parallèlement, il pourrait être envisagé de mettre en place des régulations qui obligeraient les opérateurs à se conformer à ces exigences pour obtenir ou renouveler leurs licences d'exploitation. Une telle stratégie garantirait que les opérateurs contribuent à la résilience et à la fiabilité des communications sur l'île.

3.2.4.2. La mise en place d'un routage internet local

Des mesures sont recommandées afin d'assurer un accès internet aux habitants de l'île à la suite de la survenue d'un risque. Pour cela il est recommandé que :

- Les opérateurs échangent le trafic dans les points d'interconnexion prévus par la Collectivité (IX) ;
- Les opérateurs assurent la présence locale des équipements et services permettant de maintenir l'accès à internet pour les habitants ;
- La collectivité devra mettre en place les moyens nécessaires afin d'assurer l'accessibilité au site internet même en cas d'isolement.

À date, seuls la Collectivité et Solutech font du peering.

3.2.4.3. Des recommandations RH pour la gestion de l'IXP

Concernant la gestion du point d'interconnexion, plus précisément afin d'assurer les actions de peering (interconnexion des différents opérateurs) au sein de l'IXP (point d'interconnexion), 3 rôles bien identifiés sont nécessaires. Pour chacun de ces rôles, les fonctions identifiées sont :

- 1 IXP Manager ;
- 1 coordinateur de peering IXP ;
- 1 coordinateur de peering.

Ces trois rôles peuvent être tenus par la même personne. Mais dans un souci de résilience, la collectivité souhaite disposer de deux personnes différentes afin d'assurer le backup de l'IXP.

3.2.5. Poursuivre l'amélioration du niveau de résilience du réseau électrique

Pour rappel, l'état actuel du réseau électrique est le suivant :

- 100% des câbles moyenne tension (ci-après « réseau HTA ») sont enterrés ;
- 90% des réseaux basse tension (ci-après « réseau BT ») sont enterrés ;
- ¼ des postes ont moins de 5 ans et ont été renforcés.

Dans la continuité des travaux de reconstruction du réseau de distribution publique d'électricité poste Irma, l'enterrement des réseaux basse tension doit être poursuivi. Le renouvellement et le renforcement des postes électrique doivent également être poursuivis.

La Collectivité et EDF SEI doivent poursuivre leurs démarches et leurs réflexions afin de renforcer la résilience du réseau électrique qui est un élément clé pour la résilience des réseaux télécoms. Cela est fait systématiquement à l'occasion de travaux de voirie. Il reste actuellement trois zones à enterrer : Grande Saline, Flamands et Anse des Cayes. Le principal écueil concerne les enfouissements en zone privée (voies privées ouvertes à la circulation) qui dépendent de l'accord des propriétaires.

Un projet de renouvellement des moteurs de la centrale thermique exploitée par EDF SEI est en cours et permettra de renforcer les capacités de production d'électricité de l'île et de répondre à la demande croissante tirée par le dynamisme économique du territoire. Situé en zone inondable et submersible, la nouvelle centrale sera réhaussée de 1,5 mètre.

3.3. Renforcer la sécurité informatique de la Collectivité

3.3.1. La construction d'un Schéma directeur des systèmes d'information - SDSI

Des mesures et des protocoles ont été mis en place par la Collectivité. Cependant, afin de coordonner la politique liée au système d'information, il est recommandé d'établir un schéma directeur des systèmes d'information (ci-après « SDSI »). Au-delà de la coordination stratégique, la mise en place d'un tel schéma permettra à la Collectivité de :

- Améliorer l'efficacité opérationnelle des agents ;
- Sécuriser et de s'assurer de la conformité du système d'information ;
- Améliorer la gouvernance avec des rôles clairement définis et identifiés. Ceci permet également d'améliorer la coordination entre les acteurs ;
- Rendre visible les actions en cours et futures liées au système d'information.

Le lancement de cette action est prévu pour le second semestre 2024.

3.3.2. La mise en place d'un plan de reprise d'activité et plan de continuité d'activité - PRA / PCA

Le système d'information de la collectivité est exposé principalement à des risques naturels et à des risques de cyberattaque et cyber malveillance. Cependant, pour assurer un niveau élevé de résilience, il est primordial que les opérations essentielles se poursuivent sans interruption majeure en cas de survenue d'un sinistre.

Dans ce contexte, il est fortement conseillé à la collectivité de construire son plan de continuité d'activité et de reprise d'activité.

Le PCA prévoit des mesures préventives et des procédures à suivre pour maintenir les services critiques en fonctionnement, minimisant ainsi les perturbations et les impacts négatifs sur les citoyens et les services publics.

Le PRA, quant à lui, détaille les étapes nécessaires pour restaurer les systèmes informatiques et les données après un incident, assurant une reprise rapide et efficace des activités normales.

3.3.3. Une collaboration au service de la sécurité informatique des acteurs du territoire

Afin d'être un territoire résilient en matière de cybersécurité, la Collectivité devra s'appuyer sur l'ACCYB. En coopérant avec cette agence et les partenaires de celle-ci, Saint-Barthélemy disposera de moyens et de compétences renforcés sur le sujet.

Sur Saint-Barthélemy, les actions suivantes vont être menées :

- Observatoire : scanner les sites internet des membres de l'agence pour détecter les vulnérabilités sur toutes les portes d'entrée. La configuration du système, sa mise à jour, la vulnérabilité aux attaques vont être étudiées ;
- Diagnostic de maturité cyber : Réalisation des diagnostics acteurs privés et publics ;
- NIS2 : Loi informatique et liberté pendant sur la cybersécurité du RGPD avec la directive NIS2. Ils vont effectuer un recensement des acteurs les plus sensibles sur St-Barthélemy en lien avec la préfecture et la collectivité (port, aéroport, EDF, acteurs du tourisme, etc.) ;
- Serious game : mise à disposition lors de manifestation pour sensibiliser le grand public aux enjeux de la cybersécurité. La limite de leur action est la sensibilisation. Ils mettent ensuite en relation les entreprises qui réalisent des formations cybersécurité.

3.3.4. Vers une amélioration du traitement des données de la Collectivité

Une mission sur la donnée est en cours au sein de la Collectivité. Une personne en interne a été missionnée sur ce projet afin de permettre l'utilisation de la donnée pour :

- Piloter et coordonner la gestion du territoire (politiques et services publics) ;
- Ouvrir la donnée au grand public (OpenData).

Ce projet comporte cinq grandes étapes, présentées dans le schéma ci-dessous :

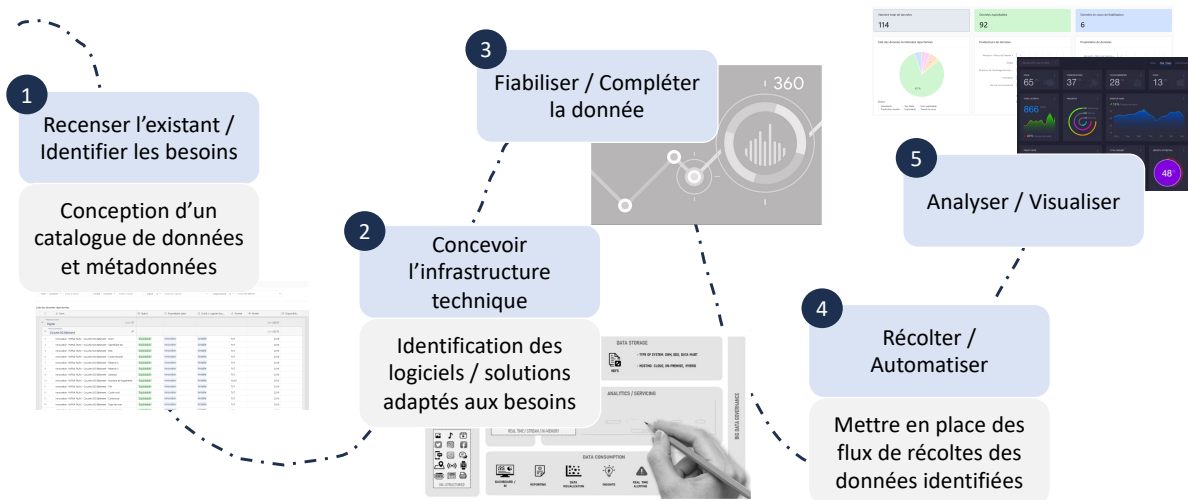


Figure 16 : Méthodologie du projet sur la donnée

Cette mission est en cours et aboutira dans le courant de l'année 2025.

3.3.5. Des locaux accueillant les opérateurs et hébergeant les données

L'hébergement des données est un élément essentiel pour la sécurité informatique. La Collectivité a pour projet d'installer des espaces d'hébergement de serveurs dans les NRO de Gustavia et de Saint-Jean ; le NRO de Lorient étant trop petit pour accueillir ce type d'infrastructures. L'organisation des NRO permet de disposer d'espaces d'hébergement dédiés pour répondre aux besoins des différents acteurs :

- Les opérateurs : un espace sera dédié à l'hébergements de leurs équipements d'activation des réseaux de fibre optique ;
- La Collectivité : un espace permettra d'héberger les équipements de la Collectivité uniquement ;
- Les entreprises et autres acteurs : un espace d'accueil de serveurs tiers permettra de proposer des services d'hébergement aux acteurs locaux.

Cette organisation est valable pour les NRO de Gustavia et de Saint-Jean qui disposent des surfaces adaptées.

4. PRIORISATION DES ACTIONS

La réalisation des phases précédentes a permis d'identifier un certain nombre d'actions à poursuivre et/ou à démarrer. Dans le cadre du schéma de résilience, il est pertinent de réaliser les actions selon l'ordre de priorité défini ci-dessous ; le niveau 1 étant le niveau de priorité le plus élevé.

PRIORITÉ 1		
SYSTÈMES D'ALERTE ET DE GESTION DE CRISE		
› Développer les systèmes d'alerte à la population.	2023-2027	○ 2 ○ ○ ○ ○ ○
› Créer un centre de veille territorial.	2023-2027	○ 2 ○ ○ ○ ○ ○
RÉSEAUX TÉLÉCOMS ET ÉLECTRIQUE		
› Assurer la continuité de fonctionnement du câble GCN.	2024 - 2034	1 ○ ○ ○ ○ ○ ○
› Migrer les équipements GCN, SCF, SSCS dans le futur NRO de Gustavia et engager les travaux de remise en état des locaux occupés mis à disposition de GCN.	2025	1 ○ ○ ○ ○ ○ ○
› Construire un troisième câble sous-marin, en collaboration avec d'autres îles caribéennes, avec un point d'atterrissage différent de Shell Beach.	2024 - 2027	○ ○ ○ 4 ○ ○
› Lancer les réflexions, étudier et mettre en place les modalités techniques, juridiques et financières de gestion du service public industriel et commercial des réseaux Télécom	2024 - 2027	○ 2 ○ ○ ○ ○ ○
› Poursuivre la démarche engagée sur le réseau mobile et les sites résilients.	2024 - 2028	○ 2 ○ ○ ○ ○ ○
› Poursuivre les travaux d'enfouissement du réseau électrique.	2024 - 2028	○ ○ ○ 4 ○ ○
› Renouveler les moteurs de la centrale électrique.	2024 - 2028	○ ○ ○ ○ 5 ○
SÉCURITÉ INFORMATIQUE DE LA COLLECTIVITÉ		
› Construire le Schéma Directeur des Systèmes d'Information de la Collectivité.	2024 - 2025	1 ○ ○ ○ ○ ○ ○
› Mettre en place les actions d'amélioration de la sécurité de la donnée en débutant par l'audit cyber.	2024	1 ○ ○ ○ ○ ○ ○
› Poursuivre le projet autour de la donnée.	2024 - 2026	1 ○ ○ ○ ○ ○ ○

Echelle :	
1	Moins de 100 k€
2	Entre 100 k€ et 500 k€
3	Entre 500 k€ et 1 million
4	Entre 1 et 10 millions
5	Plus de 10 millions

PRIORITÉ 2

RÉSEAUX TÉLÉCOMS

- › Développer SBH-IX en collaboration avec les IXP des Îles voisines. 2024-2026 
- › Poursuivre la démarche engagée sur le réseau mobile avec la volonté de faire du RAN Sharing total. 2024-2028 

SÉCURITÉ INFORMATIQUE DE LA COLLECTIVITÉ

- › Construire le plan de reprise d'activité du SI de la Collectivité. 2024 - 2025 
- › Construire le plan de continuité d'activité du SI de la Collectivité. 2024 - 2025 
- › Collaborer avec l'ACCYB pour sensibiliser sur le sujet de la cybersécurité. 2024 - 2027 

Echelle :

	Moins de 100 k€
	Entre 100 k€ et 500 k€
	Entre 500 k€ et 1 million
	Entre 1 et 10 millions
	Plus de 10 millions

ANNEXE 1 : LISTE DES ACTEURS RENCONTRÉS

Partenaires externes :

- Banque des territoires ;
- Chambre économique multi professionnelle de Saint-Barthélemy (CEM) ;
- Comité Territorial du Tourisme de Saint-Barthélemy (CTTSB) ;
- Conseil économique, social, culturel et environnemental de Saint-Barthélemy (CESCE) ;
- Agence Territoriale de l'Environnement de Saint-Barthélemy (ATE) ;
- Agence Caribéenne pour la Cybersécurité ;
- Préfecture de Saint-Barthélemy ;
- Association des hôtels et villas ;
- Association des agences immobilières ;
- Solutech ;
- Dauphin Télécom ;
- St Barth Télécom ;
- Canal + Télécom ;
- Orange ;
- EDF ;
- Saur ;
- Paprec ;
- SIDEM.

Directions :

- Police territoriale ;
- Direction des Ressources Humaines ;
- Direction des Services techniques ;
- Direction de l'environnement ;
- Direction de la Cohésion Sociale ;
- Service territorial des archives ;
- Service Informatique / réseaux ;
- Direction de l'aménagement du territoire ;
- Direction des Affaires Scolaires et Formations ;
- Direction des Affaires Portuaires et Maritime ;
- Direction de l'Aéroport « Rémy de Haenen » ;
- Direction générale des finances ;
- Direction de l'état civil ;
- Direction de la circulation ;
- Coordinatrice maison de la santé ;
- Service des assemblées ;
- Service de la communication ;
- Service de l'assainissement ;
- Service territorial d'incendie et de secours ;
- Droit de Quai.

ANNEXE 2 : DÉGÂTS D'IRMA SUR LES INFRASTRUCTURES TÉLÉCOMS



Figure 17 : Dégâts d'IRMA sur les infrastructures télécoms



Figure 19 : Dégâts d'IRMA sur les infrastructures télécoms



Figure 18 : Dégâts d'IRMA sur les infrastructures télécoms

ANNEXE 3 : LOCAL GCN SHELL BEACH – PHOTOS VISITE TERRAIN



Figure 20 : Local Shell Beach - Vue extérieure



Figure 21 : Climatisation non fonctionnelle



Figure 23 : Système incendie non fonctionnel



Figure 22 : arrivée du câble GCN



Figure 24 : Connexion du câble GCN
 au local Police

ANNEXE 4 : LOCAL GCN POLICE – PHOTOS VISITE TERRAIN



Figure 26 : Local Police - Vue extérieure



Figure 25 : Entreposage de matériel



Figure 27 : Traces d'infiltration d'eau



Figure 29 : Traces d'infiltration d'eau



Figure 28 : Câbles SCF-1

ANNEXE 5 : NRO DE LORIENT - PHOTOS VISITE TERRAIN



Figure 31 : NRO Lorient - Vue de l'extérieur



Figure 30 : SRO-977-003-L3



Figure 33 : Poste électrique à proximité du
NRO



Figure 32 : Allée intérieure



Figure 34 : Répartiteur de transport
optique - RTO

ANNEXE 6 : NRO DE GUSTAVIA – PHOTOS VISITE TERRAIN



Figure 35 : NRO Gustavia - Vue de l'extérieur

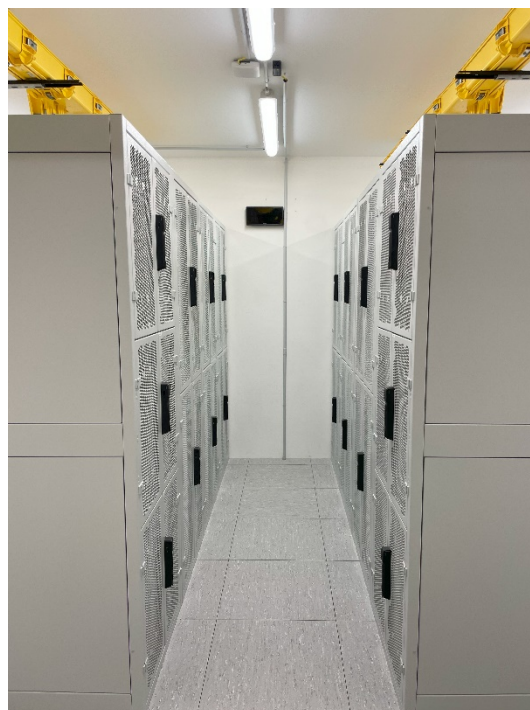


Figure 36 : Allée intérieure



Figure 38 : Dispositif incendie et climatisation



Figure 37 : Allée intérieure en travaux

ANNEXE 7 : COFFRETS DE RUE- PHOTOS VISITE TERRAIN



Figure 40 : Coffret vu de l'extérieur



Figure 39 : Raccordements internes au coffret

GLOSSAIRE

- **ACCYB** : Agence caribéenne de la cybersécurité
- **ANSSI** : Agence Nationale de la Sécurité des Systèmes d'Information ;
- **ARCEP** : Autorité de Régulation des Communications Electroniques, des Postes et de la distribution de la Presse ;
- **BMH** : Beach Manhole ;
- **BRGM** : Bureau de Recherches Géologiques et Minières ;
- **CaribNOG** : Caribbean Network Operators Group ;
- **CCP** : Code de la Commande Publique ;
- **COT** : Centre Operational Territorial ;
- **CTU** : Union des Télécommunications des Caraïbes ;
- **DNS** : Domain Name System ;
- **DSP** : Délégation de service public ;
- **FAI** : Fournisseur d'Accès à Internet ;
- **FTTH** : Fiber To The Home ;
- **FTTO** : Fiber To The Office ;
- **GCN** : Global Caribbean Network ;
- **GTI** : Garantie de Temps d'Intervention ;
- **GTR** : Garantie de Temps de Rétablissement ;
- **IPE** : Informations préalables enrichies ;
- **IXP** : Internet Exchange Point ;
- **MGP** : Marché Global de Performance ;
- **MPLS** : Multiprotocol Label Switching ;
- **NRA** : Noeud de Raccordement Abonés ;
- **NRO** : Noeud de Raccordement Optique ;
- **OC** : Opérateur Commercial ;
- **OI** : Opérateur d'Infrastructures ;
- **PM** : Point de Mutualisation ;
- **PRDM** : Point de Raccordement Distant Mutualisé ;
- **RAN** : Radio Access Network ;
- **RTO** : Répartiteur Technique Optique ;
- **SDSI** : Schéma Directeur des Systèmes d'Information ;
- **SPLANG** : Société Publique Locale pour l'Aménagement Numérique de la Guyane ;
- **SRO** : Sous-Répartiteur Optique ;
- **SSCS** : Saba, Statia Cable System ;
- **STIS** : Service Territorial d'Incendie et de Secours ;
- **TIC** : Technologies de l'Information et de la Communication ;
- **UE** : Union européenne.