TRIP d'automne 2025 – TR4

La Souveraineté numérique : la sécurité face aux attaques hybrides

Participants :

- Thierry Jouan (Avicca),
- Aurélie Bitufwila-Yerbé (Région Guadeloupe),
- Achille Lerpinière (Région Île-de-France),
- Alexis Boudard (Incubateur des territoires de l'ANCT),
- Michaël Cohen (OVHcloud)

Introduction et contexte de la souveraineté - Thierry Jouan

Cette table ronde porte sur la souveraineté numérique et la sécurité face aux attaques hybrides.

Dans le contexte d'instabilité géopolitique mondial actuelle, où les menaces cyber et les allégeances technologiques sont en constante augmentation, notre dépendance croissante au numérique rend nos sociétés (États, entreprises, citoyens, etc.) de plus en plus vulnérables. Elle les expose à des risques multiples affectant leur fonctionnement et autonomie d'action : perte de contrôle économique, vulnérabilité accrue face aux cyberattaques, influence étrangère sur des secteurs critiques, ingérence politique, domination de technologies étrangères (Microsoft, Google…), perte de la maitrise des données personnelles (ex. extraterritorialité du droit américain), etc..

Cette dépendance est devenue un risque stratégique majeur, par la perte de maitrise qu'elle induit, sur les outils, les données, les coûts, et surtout, sur la capacité à décider.

Il est donc essentiel que la souveraineté numérique redevienne un choix stratégique national. Comme nous l'avons indiqué lors de la TR n° 2 sur résilience[1], avec notamment l'intervention du SGDSN, la souveraineté est un des axes majeurs de l'actualisation de la Revue Nationale Stratégique (07/25). Ce sujet a d'ailleurs fait l'objet d'une communication spécifique en Conseil des ministres en juin dernier, témoignant d'une prise de conscience au plus haut niveau de l'État. Elle constitue un pilier fondamental de la résilience, en Jouant un rôle déterminant dans la faculté d'anticiper, d'affronter et de surmonter les situations de crises

[1] https://www.avicca.org/content/trip-dautomne-2025#sk-5351

(aléas climatiques, attaques cyber, actes de malveillance, etc.) auxquelles les collectivités sont déjà confrontées.

La souveraineté numérique est cette capacité collective à maîtriser les technologies qui permettent de rester autonome en toute circonstance. Cela concerne les infrastructures et matériels, les données et les logiciels.

Mais elle ne se décrète pas, elle s'organise afin de nous défaire de nos dépendances numériques. C'est ce que nous allons voir dans le cadre de cette table ronde, avec nos intervenants-tes afin d'aborder cette question sous différents angles :

- Aurélie Bitufwila-Yerbé - Conseillère régionale Présidente de la commission numérique du conseil régional de Guadeloupe : illustration des enjeux ou vulnérabilités spécifiques auxquels sont confrontés les territoires ultramarins, et l'importance que revêtent dans ce cadre, les câbles sous-marins...
- Achille Lerpinière - DSI du conseil régional d'Île-de-France : présentation de la politique mise en œuvre par la région afin de renforcer son autonomie, à travers les infrastructures, l'hébergement et les solutions logicielles...
- Alexis Boudard - Directeur de l'incubateur des territoires de l'ANCT : présentation de la « Suite Territoriale », une plateforme sécurisée de services mutualisés destinée aux petites communes et EPCI de « petite taille » (en termes de nombre d'habitants) ...
- Michaël Cohen - Head of Data Center Development de OVHcloud : détail des fondamentaux et les stratégies possibles en termes de mise en œuvre d'un datacenter....

Retours d'expériences de la région Guadeloupe - Aurélie Bitufwila-Yerbé

Enjeux des câbles sous-marins

Les territoires ultramarins sont confrontés à différentes vulnérabilités :

- Risques environnementaux : séismes susceptibles de provoquer des tsunamis, glissements de terrain, ouragans...
- Menaces numériques : cyberattaques ciblant directement les infrastructures de connectivité (câbles sous-marins)...
- Contraintes d'insularité : inégalités et difficultés d'accès à la connectivité spécifiques aux territoires insulaires

Les câbles sous-marins sont aujourd'hui issus majoritairement de l'initiative privée. La position géographique de la Guadeloupe, territoire plus proche des États-Unis que de la France hexagonale, présente un modèle économique peu viable pour les acteurs privés. La région a donc dû prendre des initiatives publiques pour construire ses propres infrastructures. Cela représente des enjeux de coopération internationale complexes, avec des liaisons avec des territoires non français de la Caraïbe. Pour

renforcer la résilience du territoire, plusieurs câbles ont ainsi été déployés afin de sécuriser la connectivité numérique du territoire. Cette approche s'est révélée d'autant plus nécessaire que le câble a déjà subi une attaque en mars 2023, qui a eu de lourdes conséquences notamment sur les territoires de Saint-Martin et de Saint-Barthélemy, où les entreprises ont rencontré d'importantes difficultés, constituant une véritable catastrophe tant sur le plan numérique qu'économique.

Thierry Jouan : les câbles sous-marins illustrent parfaitement la notion de souveraineté numérique. Les GAFAM ont réussi en une dizaine d'années à prendre la position de leader sur ce marché grâce à leur capacité d'investissement hors du commun, devenant ainsi incontournables. Cette situation crée une triple dépendance pour les territoires :

- Dépendance technique : la capacité à tirer un câble nécessite des compétences et moyens spécifiques. Construire un câble sous-marin nécessite 4 à 5 ans, ce qui relève véritablement de l'aménagement du territoire et impose aux collectivités une anticipation rigoureuse ;
- Dépendance économique : l'achat de capacité auprès d'un acteur expose à des évolutions de prix subies sans possibilité de réaction ;
- Dépendance juridique : l'extraterritorialité expose les données transitant sur les câbles à la législation du pays d'origine des opérateurs.

Regardons maintenant la stratégie adoptée par le conseil régional d'Ile-de-France sur le renforcement de sa souveraineté numérique.

Politique de souveraineté numérique de la région Île-de-France - Achille Lerpinière

Pour donner un ordre de grandeur, la région représente 12 000 employés, dont près de 10 000 personnes dans les lycées. Elle dispose d'un budget annuel de 6 milliards d'euros, dont 1,5 milliard consacré à la rénovation du bâtimentaire des lycées. Sur le plan numérique, les investissements s'élèvent à environ 25 millions d'euros pour le siège (formation sanitaire et sociale, achats, finances, RH, etc.) et 175 millions d'euros pour le numérique des lycées.

Transformation numérique des lycées et choix souverains

La région a opéré un virage numérique majeur avec un basculement vers des manuels numériques pour plus de la moitié des lycéens. Un choix particulièrement innovant concerne la création de manuels libres et granulaires, où la région a rémunéré des professeurs pour rédiger du contenu sous licence libre, déployé ensuite sur la plateforme française Pearltrees[2]. Il y a également la partie ENT (Espace Numérique de Travail) régional, Monlycée.net[3], fruit d'un appel d'offres remporté par Worldline, hébergé dans ses data centers à Seclin, dont une partie est certifiée Secnum. Il y a également la brique Pronote, portée par

[2] https://www.ac-paris.fr/pearltrees-124313
[3] https://monlycee.net/

l'Éducation nationale (notes et cahiers de texte). La région a également fait le choix de permettre aux élèves d'utiliser soit des licences Microsoft A5 pour l'éducation, soit LibreOffice, mais en imposant que le stockage se fasse sur Léviia[4], un hébergeur français offrant près de 1 To de capacité par lycéen.

Sur le plan matériel, la région fournit un PC portable à chaque lycéen, qu'ils peuvent conserver à la fin de leur scolarité, soit 500 000 laptops déployés. Le choix s'est porté sur Unowhy[5], un fabricant intégrateur français également francilien, qui assure l'assemblage et le SAV en France avec l'aide de Log'issimo, filiale de La Poste. Une transformation majeure est en cours avec la sortie progressive de tous les desktops et serveurs physiques des lycées. La région centralise l'administration réseau et sécurité au niveau de ses data centers (1 implanté à Saint-Ouen et 2 autres mutualisés avec le syndicat mixte Val-d'Oise numérique), partagés avec la Haute Autorité de Santé et l'Agence de biomédecine, pour disposer de data centers Tier 3+ entièrement « à la main » de la région.

L'objectif est de créer une structure hyperconvergée dans ces data centers pour éliminer les serveurs physiques dans les lycées et supprimer le besoin en desktops pour les logiciels des secteurs technico-professionnels (Solidworks, Autodesk, etc.). Plutôt que de maintenir de grosses machines physiques tournant parfois sur Windows 7 ou Windows 10 sans support, le lycéen disposera d'un dock et d'un double écran, connectera son laptop (Unowhy ou BYOD) et accédera directement en virtualisation à la puissance de calcul dans les data centers régionaux. Cette solution a été mise en place avec Weytop[6], une startup française spécialisée dans la virtualisation sur serveurs Dell, offrant de la puissance CPU et GPU dans les data centers.

Résilience et cybersécurité

La feuille de route régionale s'articule autour de la souveraineté et de la résilience. La présence de deux data centers sur la partie lycée répond à un impératif de continuité : l'un sert de backup à l'autre, permettant en moins de 12 heures de basculer l'intégralité des sauvegardes et applicatifs sur le data center de secours. La région a malheureusement subi plusieurs cyberattaques importantes, non pas de groupes internationaux comme Qiling, qui frappe actuellement les Hauts-de-France, mais souvent de l'intérieur, par des lycéens. Ces attaques ont permis des prises de contrôle au niveau local sur les machines, sur les serveurs locaux, voire une remontée vers les serveurs centraux permettant de contrôler n'importe quel laptop. Face à ces menaces, la région a décidé de tout transformer déployant des outils cyber au-dessus de l'infrastructure, notamment Palo Alto Cortex[7] qui s'est révélé bien plus efficace que les EDR locaux précédemment utilisés.

La mise en œuvre de ces actions nécessite du temps du fait des volumes d'équipements en jeu (10 000 serveurs physiques, 200 000 desktops, 9 à 14 manuels par élèves, etc.). Il s'agit d'une orientation

[4] https://www.leviia.com/cas-pratique/region-ile-de-france/
[5] https://iledefrance-unowhy.com
[6] https://www.weytop.com/
[7] https://www.paloaltonetworks.fr/cortex

stratégique de la Présidente de la région qui a pour objectif d'anticiper d'éventuelles crises et de faire en sorte que les élèves et enseignants soient totalement autonomes. Cela nécessite que toute la connaissance soit digitalisée. L'objectif est également de s'affranchir au maximum des GAFAM.

Stratégie de souveraineté

La stratégie de souveraineté de la région comporte trois axes principaux :

- Le réglementaire : la conformité à NIS2, au RGPD, et pour les formations sanitaires et sociales à HDS, impose un minimum de souveraineté ;
- Le développement économique : avec près d'un milliard d'euros par an qui y est consacré, la région privilégie les startups françaises capables de fournir les mêmes services, soit via appels d'offres, soit via des centrales d'achat (ex. CANUT). Il y a également les marchés d'innovation, avec un seuil limite passé à 136 k€ TTC (100 k€ il y a un an), qui permettent d'aller vite et d'acheter du francilien ;
- L'innovation technologique : la région travaille depuis 2023 avec la startup Lighton[8] sur l'IA générative (dans le cadre de marchés d'innovation), pour mettre en place un « tech assistant ». Cette IA générative est alimentée avec toute la documentation existante sur l'IT, le cyber, la politique de sécurité, pour que les agents puissent résoudre leurs problèmes informatiques ou leurs demandes de services de manière autonome, sans créer de ticket auprès de l'infogérant (économie de 10 à 15 €/ticket). Toute nouvelle connaissance relative à la gestion du SI est intégrée dans cette IA, ce qui permet à l'infogérant d'améliorer également la qualité de ses services. Compte tenu de la sensibilité de ces données, la région a acquis des serveurs HPE équipés de puces NVIDIA H100, implantés dans ses data centers, permettant de faire tourner les IA génératives dans les data centers de la région.

Thierry Jouan : cela nécessitera un partage des bonnes pratiques afin de favoriser l'essaimage vers d'autres territoires. Rejoignons l'échelle des communes et EPCI qui n'ont pas l'effet d'échelle suffisant pour mener ce type actions, avec l'offre de services de l'incubateur des territoires, avec notamment la suite territoriale.

Offre de services de l'Incubateur des territoires de l'ANCT – Alexis Boudard

L'incubateur des territoires représente le volet « service numérique » de l'ANCT. Il a pour mission de créer avec et pour les collectivités locales un certain nombre de services numériques (ex. BAL).

À la fin de l'année 2023, à la demande de différentes associations d'élus et de certains opérateurs de collectivités locales, le SGDSN et l'ANCT se sont rapprochés pour formaliser une convention de partenariat dans l'objectif d'offrir un socle minimal de services aux plus petites collectivités locales. L'objectif était de travailler sur les sujets du risque cyber et de l'identité numérique de ces collectivités. Les chiffres révélant l'ampleur du problème :

[8] https://www.lighton.ai/fr/home

- 11 000 collectivités n'ont pas de nom de domaine permettant de les identifier ;
- 20 000 adresses électroniques ne permettent pas d'identifier l'interlocuteur d'une collectivité ;
- Utilisation d'adresses Gmail ou Yahoo, créant autant de failles potentielles.

Depuis 1 an ½, l'incubateur a construit, avec différents partenaires (SGDSN, ANSSI, associations d'élus-es...), une plateforme appelée Suite territoriale[9]. Celle-ci sera déployée à partir du 1er janvier 2026. Elle s'articule autour de trois volets complémentaires :

- L'identité numérique professionnelle avec ProConnect, une fédération d'identité pour les élus locaux et agents publics, équivalente à FranceConnect pour les citoyens. Cette brique technique permet de relier des systèmes d'information publics et privés avec la même capacité de déploiement que FranceConnect ;
- Une offre de solutions numériques de base (nom de domaine, messagerie, stockage), en partenariat avec les structures de mutualisation existantes. L'objectif est de valoriser les offres déjà proposées par certains opérateurs locaux et de combler les manques là où aucune solution n'existe, garantissant ainsi une continuité de service public sur l'ensemble du territoire ;
- Un accès à un ensemble de services (outils ministériels, solutions proposées par les OPSN, outils d'éditeurs respectant certains critères de référencement, etc.).

Thierry Jouan : concentrons-nous maintenant sur une autre brique essentielle à la souveraineté, celle relative à l'hébergement.

Solutions d'hébergement souverain d'OVHcloud – Michaël Cohen

OVHcloud représente aujourd'hui un acteur majeur avec 46 data centers déployés sur 4 continents, servant 1,6 million de clients avec 500 000 serveurs construits en interne et environ 3 000 salariés. L'entreprise s'est positionnée autour du slogan "Innovation for Freedom", incarnant une conviction profonde en faveur de la souveraineté numérique.

Conception de la souveraineté

La souveraineté ne se résume pas à une simple localisation géographique des data center, elle traduit une véritable capacité d'action et une liberté. OVHcloud structure son approche autour de trois piliers fondamentaux de souveraineté :

- Technologique : développement d'un modèle entièrement intégré, avec une usine située à Croix, près de Lille, qui fabrique des serveurs conçus en interne. Cette maîtrise s'étend au design des technologies de refroidissement, des data centers, des lignes électriques des systèmes de cooling (pratique du direct liquid cooling depuis plus de 20 ans), des logiciels, etc. L'objectif est d'atteindre le maximum

[9] https://suiteterritoriale.anct.gouv.fr/

d'autonomie technologique possible, même si certains composants comme les puces restent dépendants de fondeurs externes (Intel, AMD, Nvidia…) ;
- Données : engagement formel à ne jamais consulter les données confiées par les clients. Cette garantie constitue un engagement fondamental de l'entreprise ;
- Opérationnelle : réalisation en interne de l'exploitation des datacenters, du développement des logiciels fournissant les services, de la mise en place d'un NOC (Network Operations Center). Cette indépendance opérationnelle permet de réduire au maximum la dépendance vis-à-vis de tiers.

La taille critique d'OVHcloud permet à l'entreprise de réaliser des investissements massifs, notamment pour se protéger contre les attaques DDoS. La souveraineté complète reste un objectif difficile à atteindre, nécessitant une approche pragmatique centrée sur la maîtrise des éléments stratégiquement critiques.

Autonomie vs autarcie

L'autonomie ne signifie pas nécessairement tout faire soi-même, mais plutôt de maîtriser ce qui est stratégiquement important. Concrètement, cela implique de maîtriser ses données, ses fournisseurs, de répartir intelligemment ses données et d'éviter la dépendance à un acteur unique.

Thierry Jouan : la stratégie envers les fournisseurs est un sujet qui a également été traité par la région Île-de-France.

Mutualisation et coopération inter-régionale - Achille Lerpinière

Ce sujet recouvre différents aspects au niveau régional :

- L'ensemble des DSI et directeurs du numérique des régions ont constitué un groupe de travail permanent pour partager leurs feuilles de route respectives (IA, numérique éducatif, etc.). Cette collaboration permet de constater que toutes les régions n'avancent pas au même rythme, certaines étant limitées par des contraintes d'infrastructure ; par ex. la virtualisation des PC lycéens nécessite une bande passante d'au moins 1 Go ; certaines régions ne disposent encore que de 200 Mo ;
- Lancement par la région d'un important marché public de création d'une centrale d'achats à disposition des collectivités locale d'Île-de-France, permettant de bénéficier d'un effet d'échelle et de réductions tarifaires (ex. photocopieurs). La démarche a été lancée sur le sujet de la cybersécurité, avec la création, il y a 2 ans, de la plateforme « Urgence Cyber Île-de-France » (cofinancée par l'ANSSI). Ce dispositif fait partie du réseau national des CISERT, et est désormais raccordé aux 17Cyber[10]. Toutes les collectivités, PME, ETI et associations d'Île-de-France peuvent appeler cette plateforme en cas de cyberattaque pour recevoir gratuitement les gestes de premier secours. Le dispositif pratique également une démarche proactive, en se rendant dans les collectivités pour présenter aux maires, élus-es et DSI les bonnes postures de sécurité à appliquer et pour les accompagner ;

[10] https://17cyber.gouv.fr/

- Lancement d'un observatoire des risques cyber, développé depuis deux ans avec Board of Cyber[11]. Il propose un scan non intrusif de tous les applicatifs exposés sur Internet d'une collectivité, avec un scoring technique sur de multiples critères (vulnérabilités TLS, Active Directory, etc.) qui attribue une note entre 0 et 1 000 (la moyenne acceptable est de 650). Les collectivités sont scannées par paquets de 300, reçoivent leur score accompagné de recommandations de bonnes pratiques, puis sont réévaluées six mois plus tard pour mesurer les progrès réalisés ;
- Mise en place d'une centrale d'achat pour remédiation cyber de niveaux 1, 2 et 3, donnant respectivement accès à Orange Cyber Défense, Intrinsec[12]et Allemande à des tarifs négociés inférieurs aux prix publics. Cette initiative vise à simplifier les démarches administratives des petites collectivités tout en les protégeant des surfacturations pratiquées par certains acteurs qui profitent de situations critiques. À noter qu'en cas d'incident cyber, la remédiation de niveau 1 est offerte.

Dans le cadre de la préparation à la mise en œuvre de la directive NIS2, dont la transposition en droit français est attendue pour 2026, la région déploie avec Board of Cyber un dispositif de scan des fournisseurs pour toutes les collectivités de plus de 30 000 habitants en Île-de-France. Ces collectivités, qui seront considérées comme "entités essentielles", devront être responsables de la sécurité de leurs fournisseurs. Le système scanne leurs 500 principaux fournisseurs pour identifier ceux présentant des failles de sécurité importantes, y compris parmi les fournisseurs français.

Au niveau national, l'association Epsilon regroupe les régions de France et agit comme un équivalent du CIGREF pour le secteur public, portant des demandes collectives de baisse de coûts auprès des GAFAM. À titre d'exemple, face à l'augmentation de 60% des licences A5 éducation de Microsoft, les régions ont refusé collectivement. Microsoft a alors proposé 30%, ce qui a été accueilli avec réserve, laissant espérer une proposition finale à 10% qui pourrait être acceptée. Ces initiatives de mutualisation répondent directement aux contraintes budgétaires croissantes des collectivités, imposant une négociation permanente avec les fournisseurs. Elles démontrent également qu'au-delà des partenariats avec leurs cabinets conseils (juridiques, financiers, etc.), la force du collectif constitue le levier le plus efficace pour préserver la souveraineté numérique tout en maîtrisant les coûts.

Suite territoriale et OPSN – Alexis Boudard

Lors du Salon des Maires, une première déclaration commune réunissant 13 OPSN partenaires a été signée avec l'ANCT. Cela regroupe des structures orientées sur les infrastructures (Megalis Bretagne, Gironde Numérique, La Fibre 64, etc.), dont certaines qui engagent une transition des infrastructures vers les services (Eure Normandie Numérique, etc.), et d'autres orientées sur les services. Ce partenariat innovant permet à ces acteurs de proposer la plateforme sur leur territoire sur laquelle ils vont retrouver l'identité numérique et un socle de services de base, avec la possibilité de proposer en marque blanche, leurs propres

[11] https://www.boardofcyber.io/
[12] https://www.intrinsec.com/

services aux collectivités locales. Cette approche garantit l'accompagnement de proximité indispensable, notamment sur les questions de RGPD, de support technique, de formation et de sensibilisation. Il s'agit d'un partenariat innovant entre l'ANCT et ces acteurs qui permet à la fois de faire bénéficier le plus grand nombre de services mais aussi et surtout d'un accompagnement.

Pour accompagner ce déploiement, une cartographie nationale est en ligne[13] sur le site de La Suite territoriale. Elle réutilise des données publiques en open data (ex. servicepublic.gouv.fr) pour visualiser la conformité des collectivités au référentiel[14]. Cette mise en visibilité de la réalité locale à l'échelle nationale, régionale, départementale ou intercommunale permet à chaque collectivité de se situer et d'identifier immédiatement les solutions disponibles, qu'elles soient publiques ou privées, locales ou nationales.

Hébergement souverain d'OVHcloud – Michaël Cohen

Clarification sur le Patriot Act et le Cloud Act

Le Patriot Act est une loi qui s'applique aux entreprises américaines. Les activités d'OVHcloud sont parfaitement scindées : l'entité américaine est soumise aux lois américaines, y compris le Patriot Act, tandis que le reste du groupe n'y est pas soumis, y compris au Cloud Act qui a pourtant une portée extraterritoriale. Cette séparation est concrète et opérationnelle. La scission est totale en termes d'organisation, de management, de gouvernance, d'outils et de données.

Solutions d'infrastructure résiliente

OVHcloud propose plusieurs types de solutions adaptées aux exigences de ses clients :

- Régions multi-AZ (Availability Zones) : Cette architecture constitue le premier niveau de résilience. Elle repose sur un minimum de trois data centers interconnectés, suffisamment éloignés pour ne pas être affectés par un même incident (attentat terroriste, catastrophe naturelle), mais suffisamment proches pour permettre une synchronisation des données. Un client adoptant cette solution 3AZ répartit sa charge et ses données sur les trois sites avec réplication mutuelle. En cas de défaillance d'un site, les deux autres continuent à se répliquer et assurent une continuité transparente pour le client. Cette solution est actuellement disponible à Paris et Milan, et en cours de développement à Berlin ;
- SecNumCloud : Ce label représente le plus haut niveau de sécurité, avec 2 000 exigences à respecter. OVHcloud dispose de zones dédiées aux produits qualifiés SecNumCloud situées à Gravelines, Roubaix et Strasbourg. Ces infrastructures constituent de véritables "coffres-forts dans le coffre-fort", avec une isolation totale : même lors d'une visite autorisée d'un data center OVHcloud standard, l'accès au data center SecNumCloud reste interdit. Les exigences opérationnelles et de contrôle

[13] https://suiteterritoriale.anct.gouv.fr/conformite/cartographie
[14] https://suiteterritoriale.anct.gouv.fr/conformite/referentiel

d'accès sont radicalement différentes. Cette offre permet d'héberger des données sensibles qui ne peuvent être confiées à des infrastructures standard ;

- OPCP (On-Prem Cloud Platform) : Cette solution répond aux besoins des organisations qui souhaitent conserver leurs données critiques en interne. Certains clients refusent catégoriquement que leurs données sortent de leurs locaux. OVHcloud propose alors de déployer sa technologique cloud directement chez le client. Cette infrastructure peut être totalement déconnectée et managée par le client lui-même, lui garantissant qu'aucun acteur tiers ne peut accéder à ses données. Cette solution a notamment été mise en place avec DEEP au Luxembourg et suscite l'intérêt de nombreux acteurs français.

Thierry Jouan : Il y a des initiatives publiques de mise en œuvre de data centers locaux. Quels sont les points essentiels à respecter pour ce type de projet ?

Michaël Cohen : On peut déjà noter qu'il est positif que les acteurs publics arrivent à se coordonner pour avoir une action commune, mais la mutualisation amène une complexité dans la gouvernance, notamment sur le partage des tâches. Le bénéfice utilisateur doit rester prioritaire : service, performance, coûts, résilience, etc.

Thierry Jouan : Revenons sur les territoires ultramarins, notamment sur le sujet de la mutualisation, avec l'articulation de projets de câbles sous-marins portés par plusieurs collectivités. Cela pourrait être envisageable sur la partie hébergement, certains de ces territoires ne sont pas exposés aux mêmes risques ; il peut être intéressant de privilégier un de ces territoires pour l'implantation d'un datacenter.

Spécificités outre-mer et coopération caribéenne - Aurélie Bitufwila-Yerbé

Les différences structurelles influencent la gouvernance du numérique. La Martinique et la Guyane sont des collectivités uniques, la Guadeloupe conserve un système bicéphale (département et région), auquel s'ajoutent les intercommunalités et les communes. Cette organisation administrative permet de clarifier les compétences, la région Guadeloupe ayant obtenu une identification claire de la compétence numérique.

Cette position stratégique a permis à la région de porter en 2022 le projet de création de l'Agence caribéenne pour la cybersécurité. Cette initiative publique, développée en association avec Saint-Martin et la Guyane, constitue une réponse collective aux enjeux de souveraineté et de résilience dans la Caraïbe. L'agence remplit plusieurs missions essentielles :

- Mise en place d'un observatoire de la cybersécurité régionale ;
- Réalisation d'actions de sensibilisation et de pédagogie auprès des acteurs locaux ;
- Déploiement d'outils de scan similaires à Board of Cyber pour évaluer la maturité cyber des organisations ;
- Préparation à l'application de la directive NIS2 dans des territoires.

La région Guadeloupe s'est donc positionnée comme animatrice de l'éveil des consciences sur ces enjeux numériques, cherchant à mobiliser tant les acteurs publics que privés autour de la nécessité de mutualiser les moyens. Cette approche collaborative s'avère d'autant plus indispensable que les coûts financiers de la souveraineté numérique sont particulièrement lourds à porter pour une collectivité territoriale insulaire. La résilience numérique implique des tests réguliers, des mécanismes de redondance et des partenariats public-privé suffisamment robustes pour garantir la protection et la conservation des données.

Au-delà des frontières administratives françaises, la Guadeloupe développe une coopération caribéenne structurée, notamment à travers la CTU (Caribbean Telecommunications Union)[15], qui facilite les échanges et permet de construire une coopération régionale durable pour l'ensemble des territoires de la zone. Cette dimension internationale est cruciale compte tenu de l'interconnexion des câbles sous-marins avec des îles anglophones voisines.

Thierry JOUAN : Je tiens à signaler que des initiatives similaires existent dans d'autres territoires ultramarins : La Réunion, confrontée à l'extinction du câble SAFE en 2027, et la Guyane, avec le projet de câble Lum@link qui rejoindra le Portugal. Ces projets partagent une volonté commune forte : garantir la souveraineté technique en s'assurant que plusieurs paires de fibres appartiennent directement à la collectivité, évitant ainsi une dépendance exclusive vis-à-vis d'opérateurs privés.

[15] https://ctu.int/