Résilience et souveraineté : le nouveau standard des infrastructures critiques

Christel Heydemann
Directrice générale d'Orange

Les réseaux de télécommunication sont désormais au cœur de la vie de toute société moderne. Qu'il s'agisse d'individus ou d'entreprises, la digitalisation s'intensifie et avec elle, l'utilisation des réseaux croit de manière exponentielle. Et ces tendances ne vont pas s'arrêter avec l'avènement de l'Intelligence Artificielle (IA), dont les impacts technologiques et sociétaux sont déjà visibles.

Les menaces extérieures prennent de plus en plus d'ampleur et deviennent des facteurs de risque forts : cyberattaques, catastrophes naturelles (inondations, tempêtes…), incertitudes géopolitiques ou économiques. La crise énergétique de 2022, la panne en péninsule ibérique en 2025 dont l'impact a été ressenti jusqu'au Maroc ou encore la dépendance des chaînes d'approvisionnement à des fournisseurs non européens sont autant de phénomènes qui illustrent la vulnérabilité des réseaux. La dépendance à des composants clés – du cloud aux semi-conducteurs - pose également des enjeux stratégiques majeurs.

Sécurité, Résilience et Ouverture : 3 piliers d'un réseau robuste

La complexité croissante des réseaux impose désormais des mises à jour logicielles sans interruption de service, ce qui constitue un défi majeur. Elles doivent se faire maintenant sans interruption, et deviennent un défi majeur. Réaliser des tests en amont est pratique courante et l'IA, qui permet l'automatisation par l'analyse systématique des données, devient un outil utile et précieux pour identifier les points importants à tester. La simulation sur maquette ou jumeaux numériques facilite ces vérifications et réduisent les risques de pannes majeures.

Pour garantir la continuité opérationnelle des services, les opérateurs doivent mettre en place des mécanismes de sauvegarde et de restauration robustes. La cybersécurité, en particulier, est une priorité tant les attaques sont nombreuses et sophistiquées et nécessite des stratégies pour protéger la confidentialité des données et renforcer la confiance des clients. Chez Orange, la résilience va de pair avec l'ouverture technologique : diversification des fournisseurs, standards ouverts et respect des exigences de souveraineté des pays où nous opérons. Nous proposons une certaine flexibilité qui s'inscrit dans une démarche de résilience, afin d'éviter des dépendances trop fortes.

Pour l'Europe, cela se traduit notamment par des offres de cloud de confiance, comme le cloud privé Cloud Avenue. En France, par des offres de cloud de confiance comme Bleu, en association avec Capgemini.

Enfin, l'évolution des besoins digitaux impactera fortement la robustesse des réseaux. Si le streaming vidéo domine encore aujourd'hui, d'ici 2030, une part majoritaire du trafic pourrait être liée à l'IA, avec des échanges entre machines et agents. Cela pourrait transformer profondément l'architecture des réseaux, notamment avec la montée de la vidéo remontante : par exemple avec des lunettes connectées, le sens du trafic serait inversé, de l'utilisateur vers le premier lieu d'inférence dans le réseau. L'architecture du réseau doit être conçue pour tenir compte de ces incertitudes.

Vers des réseaux résilients et stratégiques

Dans le cadre du nouveau plan stratégique d'Orange, Trust the Future, la priorité est claire : bâtir et opérer des réseaux résilients, sécurisés et de confiance en s'appuyant sur des partenaires fiables, notamment les autres acteurs d'infrastructures. ■