# Réseau et sécurité

Les réseaux informatiques et de télécommunications ont convergé au tout début des années 2000 et depuis les données sont transportées dans des paquets contenant quelques dizaines à quelques milliers de bits. Une forte confiance dans les informations transportées existait encore au début de ce siècle. Le fait d'intégrer l'Internet et les télécommunications dans un même environnement a eu des effets très positifs pour l'accès aux données disponibles partout et en énormes volumes mais également très négatifs pour la sécurité de ces informations.

Les réseaux ont beaucoup évolué en vingt ans et la grande révolution en cours est la virtualisation, c'est-à-dire le remplacement des équipements matériels par des logiciels. La puissance de calcul nécessaire pour exécuter ces logiciels est disponible dans les centres de données qui deviennent de ce fait le cœur de la nouvelle génération de réseaux. La révolution en cours veut que tous les boîtiers, équipements physiques du monde des réseaux disparaissent pour laisser la place à une infrastructure numérique composée uniquement de quatre entités : équipement terminal, antenne (sans aucun boîtier associé), fibre optique et centre de données. Finis les box, les routeurs, les commutateurs, les armoires électroniques, etc. Tout se traite dans les centres de données : traitement du signal, routage, commutation, automatisation, gestion, contrôle, application, etc.

Il ne faut pas croire que ces centres de données sont forcément des mastodontes : ils vont de l'infiniment petit à l'infiniment grand. Nous ne voyons pour le moment que la partie centrale de ce « *Cloud Continuum* » qui ira du centre de données dans son smartphone jusqu'à des *hyperscales* dépassant le milliard de serveurs en 2030. La 6G sera liée à ce *Cloud Continuum*.

Et la sécurité de ces nouvelles générations ? Le fait de passer du matériel au logiciel et surtout de rassembler ces logiciels dans des centres de données apportent très clairement un danger grandissant. Les attaques internes dans les centres de données sont nombreuses et peu répertoriées. Nous sommes dans le domaine de l'ingénierie système et non plus réseau. De plus, la distribution des centres de données, qui restent peu éloignés des antennes pour assurer des délais de latence faibles, apporte une complexité nouvelle pour la sécurité. Les migrations des machines virtuelles, leur modification, leur mise à jour, leur maintenance sont autant de points sensibles pour en assurer la sécurité.

La probabilité d'une possible catastrophe augmente sérieusement avec la 5G qui à terme deviendra l'infrastructure numérique intégrant quasiment tous les réseaux. Les bons hackeurs qui se comptent en quelques dizaines de milliers vont-ils arriver à piller la planète ? Les cyberattaques préparées par de nombreux états ne sont pas loin d'être prêtes à une destruction massive d'une bonne partie des équipements connectés en les rendant inopérants. Est-ce inéluctable ? Certainement pas car de nombreuses avancées peuvent fortement amoindrir la force des hackeurs. Une solution simple est de couper l'accès Internet des entreprises, des campus, des usines : le confinement. Plus le confinement restreint les espaces qui se communiquent, plus la sécurité est forte. Dans les zones de confinement, il n'y aura que la partie extrémité du *Cloud Continuum*. On peut envisager des communications protégées entre certaines zones de confinement, ce qui donne naissance à l'*Internet des Edges*. Il faudra se passer de Twitter, de Facebook et de nombreuses autres applications.

Il y a d'autres solutions moins radicales qui permettent d'envisager l'avenir des réseaux avec plus d'optimisme. On peut citer, les réseaux quantiques qui permettent entre autres de détecter les écoutes, les éléments sécurisés comme les iSIM (*integrated SIM*) embarquées dans les SOC (*system on a chip*) des équipements, les Clouds de sécurité portant toutes sortes de machines virtuelles dédiées à la sécurité, le *big data analytics in memory* et bien évidemment l'intelligence artificielle avec ses techniques d'apprentissage profond. Mais rien de parfait et de complet, laissant la place à une course poursuite entre défenseurs et attaquants.

La nouvelle génération d'infrastructure numérique va-t-elle dans le bon sens ? Oui, parce qu'elle limite drastiquement le nombre d'équipements intermédiaires qui sont souvent des points d'entrées pour les attaquants. Oui également parce que les centres de données sont généralement bien protégés. Mais, il n'y a que très peu de chance d'échapper à un virus qui se répandra et qui nécessitera un confinement ferme. Il faut s'y préparer, tout en espérant mettre au point des vaccins numériques. ■

**Guy Pujolle**
**Professeur des universités**
**Président, Green communications**