SUP DE VINCI
INGÉNIERIE DES SYSTÈMES D'INFORMATION

Quels sont les défis de sécurité les plus critiques pour les réseaux 5G et comment peuvent-ils être surmontés ?

Fait par :
Lucas MOLENDI & Thomas BRAUD

20 juin 2025

Lucas MOLENDI & Thomas BRAUD

Avant-propos :

Nous sommes Lucas MOLENDI et Thomas BRAUD, étudiants en première année de Bachelor à SUP DE VINCI, campus de Nantes.
Ce rapport constitue une veille technologique sur le sujet, dans le cadre de notre évaluation en vue du passage en deuxième année (B2).
Nous remercions toutes les personnes ayant contribué à la réalisation de ce travail, ainsi que SUP DE VINCI pour nous avoir permis d'acquérir de nouvelles compétences.

Sommaire :

Lucas MOLENDI & Thomas BRAUD

I) Introduction

a) Présentation de la problématique

La 5G représente bien plus qu'une simple amélioration des performances par rapport aux anciennes générations de réseaux mobiles. Elle marque une véritable rupture technologique, notamment dans la conception, le déploiement et l'exploitation des réseaux. Grâce à son très haut débit, sa latence extrêmement faible, à sa capacité de répondre aux exigences des applications critiques en temps réel et sa prise en charge d'une densité élevée de connexions. La 5G est appelée à devenir un pilier fondamental de l'économie numérique mondiale.

Pour commencer, définissons ce qu'est un réseau mobile. Un réseau mobile est un réseau téléphonique qui permet l'utilisation simultanée de millions de téléphones sans fil, qu'ils soient immobiles ou en mouvement, y compris lors de déplacements à grande vitesse et sur une grande distance. Cela permet de se connecter à internet et d'envoyer des messages ou de passer des appels depuis la 4G. Mais également de pouvoir d'utiliser des services dépendant d'internet comme les réseaux sociaux, les applications de navigation (Waze ou Maps) ou un navigateur internet (Chrome, Safari ou Mozilla).

La 5G opère sur des fréquences comprises entre 30 et 300 GHz. En comparaison, la 4G utilise des fréquences plus basses, entre 700MHz et 2600 MHz. Cette différence permet une couverture plus large, ainsi qu'un débit plus important et une latence plus faible. Néanmoins, il est important de noter que la portée des ondes 5G est plus courtes que celle des réseaux 4G. Cela signifie que les antennes 5G doivent être placées plus proche les unes des autres pour assurer une bonne couverture réseau.

Grâce aux nouveautés de la 5G, que nous aborderons plus tard dans ce rapport. La 5G a un débit maximal de 20 gigabits par seconde contre 1 gigabit par seconde pour la 4G+. Cela ne veut pas dire que ces deux réseaux ont ce débit constant. En réalité pour les utilisateurs, les débits ne sont pas aussi importants et diffèrent selon les opérateurs.

Cependant, les nouveautés de la 5G, amènent des menaces plus graves et complexes pour la sécurité du réseau. Contrairement aux anciens réseaux, la 5G repose essentiellement sur des architectures virtualisées, des architectures décentralisées ou des architectures distribuées. Mais aussi sur une utilisation importante du cloud, du découpage réseau (Network Slicing) ainsi que sur l'intégration de dispositifs issus de l'Internet des Objets (IoT). Toutes ces évolutions, bien que bénéfiques en termes de performances ou de flexibilité, augmentent les surfaces d'attaques, multipliant les points potentiels de vulnérabilité. Ces dernières sont exploitées par des attaques de types Man-in-the-middle, d'attaque par déni de service (DDoS) et d'autres attaques d'espionnage utilisant des failles du réseau 5G.

Il est alors impératif de s'interroger et de s'informer au quotidien sur les menaces touchant spécifiquement les réseaux 5G, qu'il s'agisse d'attaques sur le cœur du réseau, d'espionnage, de données compromises ou encore de menaces

géopolitiques. Il est essentiel d'examiner les solutions possibles et les moyens de mise en œuvre de ces solutions pour y faire face le moment venu. La veille technologique est le moyen idéal pour se maintenir à jour.

C'est dans ce contexte que nous allons nous interroger, durant ce rapport sur la problématique suivante : **Quels sont les défis de sécurité les plus critiques pour les réseaux 5G et comment peuvent-ils être surmontés ?** Répondre à cette question permettra de mieux comprendre les enjeux liés à cette technologie et d'identifier les moyens nécessaires pour construire un écosystème numérique sécurisé, résiliant et digne de confiance. Pour cadrer notre discours, nous aborderons les réseaux 5G en France, les défis les plus critiques, les plus importants. Notamment liés à l'architecture de la 5G et aux attaques touchant les réseaux 5G, en se concentrant sur les attaques DDoS. Pour rester dans ce cadre, nous évoquerons, mais ne développeront pas, sauf nécessité, tout ce qui concerne les anciennes générations de réseaux, les IoT et les attaques autres que les attaques DDoS.

b) Objectifs du Projet

Pour ce rapport, nos objectifs principaux sont de réaliser une veille technologique sur un sujet donné et de valider notre passage en B2 à Sup de Vinci. Nous avons également pour objectifs de nous informer sur un sujet que nous ne connaissons pas entièrement, de gagner en compétences, connaissances notamment en ce qui concerne le travail en groupe et la gestion de projet. Il s'agit aussi de se préparer à une présentation orale et de rendre un rapport écrit.

Nous espérons avoir réalisé une veille complète qui est en accord avec les attentes du travail demandé, et être allés le plus loin possible dans la maîtrise ainsi que dans la connaissance de notre sujet.

II) Contexte et Définitions

a) Contexte

La 5G, ou 5ème génération des normes de transfert de données mobiles a été lancée en 2020 pour le grand public. Cette 5ème génération apporte de nombreux avantages par rapport à ses prédécesseurs. La 5G possède une bande passante plus large avec un très haut débit ; cette amélioration a permis d'accélérer l'usage du numérique au quotidien. Cependant, l'usage de ces réseaux ouvre aussi la porte à de nombreuses menaces. La 5G doit donc faire face à ces défis pour assurer la sécurité des données, qu'elles soient personnelles, sensibles ou industrielles.

b) Mot clés

Avant de rentrer concrètement dans le rapport, nous allons expliquer quelques mots-clés importants pour la compréhension des recherches. D'autres mots sont

définis dans le glossaire situé à la fin du rapport. Les mots présents dans le glossaire sont définis comme des liens cliquable, et un autre lien cliquable vous ramène à votre lecture.

Le premier terme important à comprendre est « réseau ». Un réseau est un ensemble d'éléments interconnectés qui permettent la communication et l'échange de données. Ces éléments peuvent être des ordinateurs, des serveurs, des équipements de télécommunications et d'autres dispositifs électroniques. Les prochains termes sont plus spécifiques aux réseaux 5G.

Le Software-Defined Networking (SDN) est une approche de l'architecture réseau qui permet de contrôler ou de programmer le réseau de manière intelligente et centralisée à l'aide d'applications logicielles. Le SDN agit comme un chef d'orchestre qui dirige tout le trafic du réseau de manière intelligente, en temps réel, selon les besoins. Cela permet un réseau plus flexible, plus sûr et plus facile à gérer.

Le Network Functions Virtualisation (NFV ou virtualisation des fonctions réseau) est un moyen de réduire les coûts et d'accélérer le déploiement des services pour les opérateurs réseau en dissociant des fonctions comme le pare-feu ou le chiffrement de tout matériel dédié, en les déplaçant vers des serveurs virtuels. Le NFV, c'est comme remplacer une boîte pleine d'appareils réseau par un ordinateur puissant qui peut faire fonctionner tous ces appareils en version logicielle. Dans la 5G, cela permet d'avoir un réseau plus rapide à adapter, moins coûteux à maintenir et prêt à évoluer en temps réel.

Le Network Slicing est une technologie qui permet de segmenter un réseau 5G en plusieurs réseaux virtuels indépendants, appelés « slices » ou tranches. Pour un exemple plus concret, le Network Slicing, c'est comme créer plusieurs autoroutes virtuelles sur une même route physique, chacune réservée à un type de véhicule (à un usage) avec des règles précises. Cela rend le réseau plus efficace, plus adaptable et plus sécurisé pour répondre aux besoins variés de la 5G.

III) Etats de l'Art : L'émergence des réseaux 5G et ses défis

1) La complexification et la diversité du réseau

a) La multiplication des vecteurs d'attaques

La 5G représente une avancée majeure en matière de connectivité : plus rapide, plus dense et décentralisée. Cette évolution technologique redéfinit également les risques de sécurité en multipliant les vecteurs d'attaque. Contrairement aux générations précédentes, l'architecture de la 5G repose sur des infrastructures virtualisées, s'appuyant sur deux technologies clés : le NFV (Network Functions Virtualization) et le SDN (Software-Defined Network). Ces technologies assurent une gestion flexible des ressources du réseau et garantissent leurs disponibilités.

L'un des piliers de cette architecture est le Network Slicing, qui permet de diviser le réseau en segments virtuels adaptés à différents usages, comme pour des

applications ou des entreprises. Si cette flexibilité permet d'optimiser les performances, elle implique aussi des exigences élevées en matière de sécurité. Une mauvaise isolation entre les tranches peut entraîner des attaques transversales, compromettant la totalité du réseau.

La décentralisation du traitement des données via le Multi-Access Edge Computing (MEC) réduit la latence, mais augmente également la surface d'attaque. Le nombre d'appareils sur le réseau 5G est jusqu'à 100 fois supérieur à celui de la 4G, ce qui multiplie les points d'entrée potentiels. L'exploitation d'un seul appareil peut suffire à déclencher des attaques en cascade.

En raison du nombre élevé d'appareils connectés, le réseau 5G traite un volume considérable de données privées qu'il collecte et partage à grande échelle. Combiné à la rapidité et à la capacité du réseau, cet afflux de données ouvre la voie à de nouvelles formes de surveillance ou d'exploitation par des acteurs malveillants ou étatiques, élargissant ainsi les vecteurs d'attaque.

Les vecteurs d'attaque devraient continuer à se multiplier avec la densification du réseau 5G, notamment à travers le développement de nouvelles technologies comme l'Internet des objets (IoT). L'IoT est réputé pour son manque de sécurité : ces appareils peuvent être infectés par des malwares ou intégrés à des botnets menant des attaques DDoS. Le risque de corruption de ces dispositifs est particulièrement préoccupant dans les infrastructures critiques, où ils sont présents en grand nombre, comme dans les transports, le domaine de l'énergie et le domaine de la santé.

Enfin, les réseaux 5G sont également exposés aux attaques sur les chaînes d'approvisionnement. De plus, de nombreux opérateurs font le choix de la diversification, en ayant recours à plusieurs fournisseurs, notamment pour les services de cloud. Dans ce contexte, des acteurs malveillants peuvent tenter de compromettre un ou plusieurs points de la chaîne d'approvisionnement en matériel et logiciels pour infiltrer les réseaux et les appareils 5G. Cette menace est croissante et stratégique : la cybersécurité 5G devient un enjeu national. Comme l'a déclaré Guillaume Poupard, directeur de l'ANSSI (Agence nationale de la sécurité des systèmes d'information), « […] Dans trois quatre ans couper la 5G, cela reviendra à couper le courant en termes d'impact. ».

b) Interconnexion et dépendances

Aujourd'hui, la 5G cohabite avec la 4G mais aussi la 4G LTE, ainsi qu'avec d'autres générations de réseaux, toutes caractérisées par des normes de débit différentes. Comme évoqué précédemment, la 5G est également confrontée à un nombre croissant d'attaques, dues notamment à la cohabitation des réseaux de données mobiles qui, eux-mêmes, ne sont pas encore parfaitement sécurisés. De plus, la 5G doit répondre à une demande constante en matière de capacité, de débit et de tolérance de connectivité, afin de permettre à l'industrie 4.0, aux smart city et aux outils de l'IoT de rester fonctionnels en continu. Cette interconnexion permanente accroît les risques de failles de sécurité et d'attaques pouvant survenir à tout moment.

En effet, d'après l'étude de Nokia en 2023, les failles dues aux outils de l'IoT sont responsables de 48 % des attaques sur les réseaux 5G en tant que point d'entrée en raison de la mauvaise sécurisation des outils de l'IoT.

2) Les technologies de virtualisation et la segmentation du réseau.

a) SDN & NFV : Opportunité et Vulnérabilités.

La virtualisation des éléments nécessaires au fonctionnement des réseaux 5G apporte de nombreux bénéfices, mais également de nombreuses faiblesses. Les faiblesses sont importantes. L'une d'elles est la difficulté à installer un réseau dont l'architecture est virtuelle. Pour réduire les coûts, les opérateurs virtualisent généralement tous les équipements d'un ou plusieurs réseaux sur un seul appareil créant une faiblesse. Si une attaque a lieu via un objet de l'IoT contaminé, l'opérateur. Ce qui permettrait de couper tous les réseaux par une seule faille. Cependant, la virtualisation apporte de nombreux avantages, dans un réseau virtualisé il y a moins de risque de panne car moins de matériels physiques différents. Au niveau de la maintenance et de la création, on observe aussi des réductions significatives des coûts car peu de matériel physique est à acheter, mais en contrepartie, il faut payer des développeurs pour créer les logiciels. L'architecture virtuelle a d'autres qualités, comme la capacité de gestion du réseau simplifiée grâce aux fonctions SDN et NFV.

Malgré tout, même si l'architecture physique a été réduite en taille, il reste une architecture logicielle qui a fait son apparition. Cette architecture utilise des fonctions comme le SDN et le NFV. Le SDN permet une gestion de l'entièreté du réseau, aidé par le NFV permettant la virtualisation. Le NFV, utilise-lui du VNFM pour contrôler certaines parties de ces réseaux. Ce qui est problématique, car on passe d'une dépendance matérielle à une dépendance logicielle pour la 5G.

La dépendance logicielle peut devenir grave, car de nombreux logiciels et technologies possèdent des exploits nécessitant des mises à jour ainsi qu'une analyse constante de façon à éviter tout risque de faille. Cela pose aussi un problème sur l'utilisation rapide d'une nouvelle technologie. Cette dernière pourrait avoir des failles de sécurité créées dans sa configuration, qui sont encore inconnues de ses développeurs. Ces failles dites *« zero day »* sont généralement les plus grosses failles logicielles et celles qui ont le plus gros impact si elles viennent à être exploitées.

Pour tester la fiabilité de leurs fonctions, les opérateurs ont également pris l'habitude de les tester sur des architectures virtuelles sans se servir d'architectures physiques. Des chercheurs appartenant à la Sandia National Laboratories ont comparé les performances des architectures physiques et des architectures virtuelles. Leurs observations de ces deux architectures ont été similaires au niveau des tests de latence, des débits, des transferts réseau et de la charge des processeurs. Les deux architectures sont identiques. Par exemple : avec certaines micro-configurations ou certains logiciels, l'architecture physique devient moins

performante. L'utilisation des logiciels de virtualisation **Virtuo** et **e1000** a donné des résultats équivalents avec une architecture virtuelle. On peut donc imaginer que les tests sur les fonctions devraient donc encore être effectués sur des architectures physiques ou hybrides, de façon à observer les potentiels problèmes pouvant survenir dus à l'hétérogénéité du réseau.

b) Network slicing et isolation des tranches

L'un des grands atouts de la 5G est le Network Slicing, qui transforme l'architecture réseau mais nécessite une isolation rigoureuse pour garantir la sécurité de chaque tranche.

Le Network Slicing permet de diviser un réseau en tranches virtuelles indépendantes, bien qu'elles partagent la même infrastructure physique ou virtuelle. Chaque tranche est adaptée à un usage spécifique grâce aux technologies SDN et NFV, qui assurent une répartition dynamique des ressources et permettent de définir des politiques réseaux propres à chaque tranche.

Cette approche offre une flexibilité importante : les opérateurs peuvent adapter la qualité des services selon les besoins, comme créer un réseau dédié aux secours.

Pour un exemple concret, en 2018, Orange et Ericsson ont décidé de tester le Network Slicing à travers une expérience. Ils avaient déployé un réseau expérimental sur une piste de test automobile dans l'est de la France, pour tester des cas d'usage en situation réelle. Des tranches du réseau avaient été allouées au transport intelligent de la voiture, d'autres tranches au divertissement, comme les flux vidéo et audio utilisés par les passagers. Lors de ce test, le réseau mobile a été paramétré pour offrir deux services distincts : une faible latence pour le service de transport intelligent et des débits importants pour les services dédiés aux passagers. Ce test a été rendu possible grâce au Network Slicing, qui offre la possibilité de paramétrer le réseau sur mesure. Finalement, cette expérience a validé le fait que deux services distincts ont parfaitement pu être délivrés en simultané, sans que l'un prenne les ressources de l'autre.

Vous trouverez quelques exemples du Network Slicing et du partage des tranches en annexe. (Image).

Maintenant que le fonctionnement du Network Slicing est mieux compris, intéressons-nous aux tranches en elles-mêmes et à leur isolation.

Chaque tranche est créée, modifiée et attribuée dynamiquement selon les accords de niveau de service (SLA : Service Level Agreement). Ce sont les opérateurs qui ont le pouvoir d'agir sur les tranches.

Chaque tranche peut définir sa topologie logique, ses spécifications, sa fiabilité et son niveau de sécurité afin de répondre aux besoins variés des services, des entreprises ou des consommateurs. Par exemple, une tranche peut être optimisée pour les jeux sensibles à la latence ou les applications de réalité virtuelle.

Pour résumer, chaque tranche peut être optimisée avec des caractéristiques spécifiques (latence, sécurité, bande passante...) selon les besoins du client.

L'isolation entre les tranches est indispensable pour qu'elles coexistent sans interférer. C'est là que rentrent en jeu le NFV et le SDN : ils agissent comme orchestrateurs, surveillent et empêchent qu'une tranche utilise les ressources d'une autre. Chaque tranche doit posséder ses propres instances logicielles telles que le routeur ou le serveur DNS. Des outils de détection d'intrusion, des pare-feux et des politiques d'accès spécifiques doivent être appliqués à chaque tranche. Cela permet d'identifier et de bloquer les menaces localement.

L'isolation garantit trois aspects fondamentaux :

- La performance : Chaque tranche est définie par rapport à une exigence particulière, exprimée sous forme de KPI (indicateur clé de performance). L'isolation assure le respect de ce KPI. Un service doit respecter l'objectif de performance qui lui est fixé, quel que soit le niveau de congestion du réseau (la saturation du réseau) ou le niveau de performance des autres tranches.

- La sécurité et la confidentialité : Aucune tranche ne doit subir les attaques ou les erreurs des autres. De plus, chaque tranche a ses propres fonctions de sécurité qui empêchent notamment les entités non autorisées d'accéder au droit de lecture ou d'écriture sur la configuration d'une tranche réseau.

- La gestion du réseau : Chaque tranche est administrée comme un réseau séparé, évitant les attaques en cascade.

3) Les attaques via les failles des réseaux 5G.

Alors que la 5G s'impose comme le pilier futur des infrastructures numériques modernes, elle doit aussi faire face à de nombreuses attaques. Nous allons évoquer les plus importantes et nous irons plus dans le détail avec les attaques DDoS.
La 5G présente des vulnérabilités spécifiques au mobile, comme avec les attaques Torpedo, Piercer et IMSI Cracking. Ces dernières permettent de suivre la position d'un utilisateur ou de récupérer son IMSI (identifiant unique de carte SIM). L'IMSI peut ensuite être utilisé pour surveiller, usurper ou intercepter les communications d'un abonné.

Les interfaces du réseau 5G sont aussi sensibles aux attaques, notamment l'API (Application Programming Interface ou « interface de programmation d'application »), qui constitue la partie centrale du réseau. Selon Fortinet, ces attaques représentent environ 18 % des menaces détectées sur les réseaux 5G.

Comme évoqué plus tôt, la prolifération des IoT via les réseaux 5G a augmenté les risques d'attaques, ces appareils étant connus pour leurs nombreuses vulnérabilités. En effet, on estime que 45 % à 50 % des attaques sur les réseaux 5G viennent des IoT selon Nokia ou encore de GSMA (GSM Association).

A la manière de ses prédécesseurs, la 5G est elle aussi victime des attaques touchant tout type de réseau ou de matériels informatiques, comme les attaques de type Man-in-the-middle (MITM) et DDoS.

L'attaque MITM est une attaque ayant pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre puisse se douter que leur canal de communications a été détourné. Selon le rapport de Cybersecurity and Infrastructure Security Agency (CISA), les attaques MITM contre les réseaux 5G ont augmenté de 20 % par rapport à 2022.

Une attaque DDoS vise à saturer un service ou une fonction du réseau comme un DNS ou un routeur, en inondant la cible de requêtes jusqu'à provoquer son ralentissement ou son indisponibilité. Dans un réseau 5G, ces attaques exploitent souvent les IoT piratés pour former un botnet, capable d'envoyer des milliers de requêtes malveillantes.

Selon un rapport d'A10 Networks en 2023, ces attaques ont augmenté de 25 % dans les réseaux 5G par rapport aux réseaux 4G. Les attaques visaient principalement les infrastructures de cloud et de virtualisation, très utilisées dans les réseaux 5G. Selon le même rapport, les attaques DDoS ciblant les réseaux 5G en 2023 ont augmenté de 35 % par rapport à 2022.

Un autre rapport de NETSCOUT signale 7,9 millions d'attaques DDoS au premier semestre 2023. Au cours du deuxième semestre 2022, NETSCOUT avait constaté une explosion des attaques chez les opérateurs mobiles en Asie-Pacifique (+294 %). Cette explosion est liée au fait qu'un grand nombre d'amateurs de jeux en ligne transfèrent leur activité vers la technologie d'accès sans fil fixe (FWA) en 5G. Leur étude conclut aussi que les attaques DDoS se renouvellent peu, avec un taux moyen de renouvellement des adresses IP de seulement 10 %.

IV) Méthodologie

Pour la collecte et l'analyse des informations, nous avons réalisé une veille active avec des mots-clés qui nous ont mené à des articles sur Internet, pris des informations venant d'IA et consulté des publications sur LinkedIn. Nous avons également analysé des enquêtes pour obtenir des statistiques et des graphiques.
Comme outils, nous avons utilisé Notion pour stocker et organiser les informations. Nous avons aussi utilisé XMind et Mural pour réaliser des cartes mentales, notamment afin de faciliter notre organisation. En ce qui concerne l'écriture et la présentation de notre rapport, nous avons utilisé Word, PowerPoint ainsi qu'Excel pour créer des graphiques liés à nos données. Pour les outils de veille à proprement parler, nous avons utilisé les Alertes Google afin de recevoir des notifications sur les sujets suivis. Pour chaque source, on a évalué ses critères de fiabilité selon leur auteur, le site ou l'entreprise ayant rédigé l'article. Après avoir lu chaque article, nous indiquions le niveau de pertinence selon notre propre évaluation
Dans les annexes, vous trouverez des captures de notre espace Notion, ainsi que des visuels de XMind et Mural.

V) Comment surmonter ces défis ?

1) Renforcer la sécurité les architectures SDN et NFV.

Il y a différents moyens de renforcer la sécurité des infrastructures logicielles. On peut notamment citer : une vérification des requêtes de contrôle de façon systématique, une surveillance des communications entre différentes fonctions, une isolation des fonctions ainsi qu'une isolation des données sensibles. Cela pourrait entre autres, permettre une augmentation de la sécurité des architectures SDN et NFV.

On a observé depuis l'apparition de la 5G (destinées au public) que de nouvelles formules apparaissaient proposant en théorie un meilleur chiffrement de bout en bout. Cependant cela n'est pas encore totalement exploitable dû au matériel réseau n'ayant pas encore les capacités de faire fonctionner pleinement ce système. Tout en gardant l'ancien qui est encore en expansion et en installation dans certaines zones (du territoire français).

Le chiffrement de bout en bout peut également se rapprocher du tunnel VPN qui commence à faire son apparition pour les communications entre différentes fonctions. Pour protéger les fonctions, les capacités du SDN sont généralement restreintes pour éviter une prise de contrôle des outils réseau en cas d'attaque. Pour le NFV, il faut obligatoirement augmenter la sécurisation de l'orchestrateur NFVM pour éviter une prise de contrôle, sans lui réduire ses capacités déjà limitées sur l'entièreté du réseau.

2) Sécuriser le Network Slicing grâce à une isolation stricte

Pour surmonter ces défis un des moyens est de sécuriser le Network Slicing avec une isolation encore plus stricte.

Pour avoir une isolation plus stricte sur les réseaux 5G, il faut déployer des pare-feux, qui filtrent le trafic et peuvent aussi protéger les fonctions du NFV. Il existe de multiples pare-feux tels que FortiGate de Fortinet qui est l'un des plus utilisés dans les environnements 5G et cloud. En effet il supporte la segmentation des tranches et l'intégration SDN/NFV, mais aussi il permet de protéger les interfaces critiques comme l'API. On peut aussi citer le Palo Alto Network Next-Gen Firewall, le Juniper SRX Series ou le Check Point Quantum. Le choix du pare-feu dépendra des besoins, ils possèdent tous des caractéristiques différentes.

La mise en place IDS (Instruction Detection System) ou IPS (Intrusion Prevention System) augmente également l'isolation. L'IDS détecte les intrusions, analyse le trafic sur le réseau et analyse les logs pour identifier les comportements suspects comme des scans de ports, des tentatives de connexions anormales, des signatures d'attaques connues. Cependant, il ne bloque pas l'attaque, il alerte seulement les administrateurs. L'IPS est préventif, il bloque automatiquement le trafic malveillant dès qu'il le détecte. Il agit en temps réel, souvent placé entre deux segments du réseau. Dans les réseaux 5G, l'IDS et IPS sont souvent intégrées aux pare-feux. Ils sont virtualisés et dirigés dynamiquement avec les fonctions SDN/NFV.

Une meilleure isolation passe aussi par la mise en place de politiques d'accès distinctes pour chaque tranche avec :

- Des authentifications plus ou moins forte

- Empêcher la priorité d'une tranche sur les autres
- La mise en place d'instances logicielles indépendantes pour les fonctions critiques (DNS, routage, etc.) et
- L'application de SLA (accord de niveau de services) avec des critères de sécurité propre à chaque tranche.

Il est aussi nécessaire de mettre en place une surveillance des performances et des alertes spécifiques par tranche. La surveillance des performances permet de suivre les KPI propres à chaque tranche comme la latence, le débit, la disponibilité, le temps de réponse, etc. Cette surveillance vérifie que chaque tranche respecte les SLA mis en place et permet d'optimiser les ressources allouées pour garantir les performances. Parmi les systèmes de supervision classiques, on peut nommer Zabbix ou Observium, mais il existe des systèmes spécifiques aux réseaux 5G comme O-RAN SMO ou ONAP. Tous ces systèmes de supervision peuvent déclencher des alertes en temps réel si un seuil est franchi sur une tranche, par exemple une latence supérieure à 50 ms (millisecondes) ou une bande passante saturée. Une alerte est également déclenchée si le service présente une dégradation ou qu'une attaque intervient sur l'une des tranches.

Enfin le point important pour s'assurer de la bonne isolation des tranches est d'évaluer régulièrement leur solidité contre des scénarios d'attaques.

3) Limiter les vecteurs d'attaque et les interconnexions vulnérables

La limitation des vecteurs d'attaque passe notamment par une disparition des anciennes générations qui ne permettent pas une sécurisation complète des données. L'hétérogénéité des réseaux amène également de nombreux problèmes de maintenance et de portabilité car le matériel vieillissant n'est pas toujours compatible avec les nouvelles normes. De plus il tombe plus fréquemment en panne. Ce qui demande un travail de maintenance de l'architecture matérielle supérieur, là où l'architecture logicielle dont dépend la 5G ne souffre pas de ce problème. Sauf sur le matériel qui rassemble toutes les fonctions essentielles au bon fonctionnement du réseau. Elle dépend du matériel sur lequel tout est rassemblé. La 5G est aussi dépendante des mises à jour logiciels.

Pour protéger les architectures logicielles, tout en agissant également sur les architectures matérielles, des méthodes d'authentification sont utilisées. Cependant, elles sont aussi affectées par de nombreuses fuites de données, en raison d'une mauvaise sécurisation de ces méthodes d'authentification et du matériel utilisé bien que leur nombre soit réduit grâce à l'architecture logicielle.

Pour maintenir une sécurité optimale de l'architecture 5G on peut également réfléchir à sécuriser au mieux son centre dont dépendent toutes ses fonctions : l'API. On peut aussi protéger les différentes couches du réseau 5G en surveillant et protégeant les parties interconnectées entre plusieurs couches afin de réduire les risques de propagation en cas d'attaque. Une autre possibilité serait de réduire le nombre de points d'interconnexions au niveau médian c'est-à-dire en équilibrant l'impact de cette réduction avec l'augmentation de la sécurité.

4) Renforcer la résilience face aux attaques DDoS

Face à la montée en puissance des attaques DDoS sur les infrastructures 5G, il devient indispensable de mettre en place des stratégies de résilience afin de garantir la continuité des services.

Une des stratégies est de mettre en place des quotas pour définir des seuils maximaux pour l'utilisation des ressources comme la bande passante, le nombre de requêtes, le volume de données par utilisateurs, etc. Ces quotas évitent qu'un acteur malveillant ne monopolise trop de ressources, comme dans le cas d'une attaque DDoS. De la même manière, établir une restriction de débit pour restreindre le nombre de requêtes ou la quantité de trafic autorisée, permet de freiner les tentatives de surcharge du réseau. La segmentation du réseau en segments indépendants grâce aux technologies des réseaux 5G limite la propagation d'une attaque.

Comme pour l'isolation des tranches, pour résister au mieux aux attaques DDoS, chaque tranche doit disposer de ses propres instances logicielles pour les fonctions critiques comme les serveurs DNS ou les routeurs. Maintenant ces composants doivent être renforcés par des mécanismes de sécurité spécifiques, par exemple un filtrage des requêtes DNS malveillantes ou une authentification stricte pour les modifications de routages. Pour les protéger davantage, l'utilisation de la micro-segmentation est judicieuse. Elle permet d'isoler chaque composant dans un sous-ensemble sécurisé avec ses propres règles d'accès.

Avec la montée en puissance de l'IA et du machine Learning, il est important de l'implanter pour améliorer la sécurité. L'IA et le Machine Learning peuvent être utilisés pour analyser en temps réel le trafic réseau et repérer des schémas de comportement inhabituels, semblables aux caractéristiques d'attaques DDoS comme une hausse soudaine du trafic, des requêtes répétitives, des flux depuis des adresses IP inconnues, etc. Ils peuvent aussi repérer des caractéristiques d'autres attaques. De plus, les modèles de Machine Learning peuvent s'entraîner sur les données réseau ou de faux réseaux virtuels et s'adapter aux potentielles évolutions des menaces y compris des nouvelles formes d'attaques non connues (zero-day). Un des avantages de l'IA est qu'une fois une anomalie détectée, elle peut déclencher automatiquement des mesures de protection comme le blocage d'IP, la redirection du flux vers un centre de nettoyage du trafic (scrubing center) virtuel ou physique qui filtre le bon trafic du mauvais trafic et renvoie le bon trafic vers le réseau. Avec la capacité de mettre en place des réponses automatisées l'IA peut activer un mode de mitigation, un mode qui active automatiquement des règles temporaires dans les pare-feux, des quotas dynamiques, une priorisation du trafic ou une limitation de la bande passante. L'objectif, limiter l'impact de l'attaque sans couper l'accès aux vrais utilisateurs.

Nous savons que les objets connectés (IoT) dont la sécurité est minimale sont des cibles faciles pour les cybercriminels. Une fois infectés ces appareils se transforment en botnets qui sont utilisés pour lancer des attaques DDoS. Pour limiter cela, il est crucial de mettre en place des politiques de sécurité spécifiques aux IoT. Comme une authentification forte, une mise à jour automatique et régulière des firmwares pour corriger les vulnérabilités. Il faut également mettre en place une restriction des communications réseau, chaque IoT doit avoir un accès limité uniquement aux ressources nécessaires, c'est le principe du moindre privilège. Il convient aussi de segmenter et de mettre en place une surveillance du comportement réseau des IoT pour détecter des anomalies comme un pic de trafic anormal ou une communication avec une IP suspecte.

5) Mise à jour constante des pratiques de cybersécurité

Les cybermenaces évoluent sans cesse, pour garantir la résilience du réseau 5G, il faut adopter une approche dynamique et réactive de la cybersécurité.

Pour cela, il est obligatoire de mettre en place une veille technologique active, pour suivre les vulnérabilités comme Torpedo ou l'IMSI Cracking. Suivre ces vulnérabilités permet de mieux anticiper les menaces, de réduire le temps de réaction face à celles-ci et de renforcer la conformité d'une entreprise ou d'un opérateur par rapport aux bonnes pratiques de cybersécurité exigées par les régulateurs ou les partenaires. La mise en place de cette veille technologique peut se faire via des abonnements aux bases de données et alertes comme le CVE (Common Vulnerability and Exposures), les bulletins CERT, ou les GSMA Security Reports. Il est aussi possible d'utiliser des outils de veilles automatisées comme Threat Intelligence Platforms (TIP), ou des plateformes telles que Shodan ou VulnDB. Il est également nécessaire d'analyser les publications de chercheurs, de surveiller les conférences. On peut citer Black Hat ou DEF CON et de lire les articles académiques spécialisés dans la sécurité mobile 5G.

Face aux cybermenaces, une des meilleures solutions reste de former en continu les équipes qui sont liées de près ou de loin à la 5G. Les menaces et le fonctionnement des réseaux 5G sont différents des anciens réseaux mobiles. Il est crucial que les équipes comprennent ces spécificités si besoin, en les vulgarisant. Pour cela il est nécessaire d'organiser des sessions régulières comme des cours sur les attaques ou le fonctionnement général sur le réseau 5G, tout en rendant cela compréhensible pour tout le monde. Une autre méthode est d'organiser des simulations d'incidents. Ces simulations permettent de tester les réflexes des équipes en cas de cyberattaque et d'identifier de potentielles failles dans les procédures de défense. De la même manière, mettre en place des exercices de crise est une bonne chose, puisqu'en période de crise, chaque minute compte.

Enfin la collaboration entre les autorités et les partenaires aide à la mise à jour constante des pratiques de cybersécurité. Cela passe par le partage de renseignements sur les menaces via des plateformes comme l'ANSSI en France. Il faut aussi créer des centres type SOC (Security Operations Center) qui sont chargés de surveiller, analyser, détecter et répondre aux incidents de sécurité, 24h/24 et 7j/7. Publier et consulter des indicateurs de compromission (IOC), des rapports de vulnérabilités, ou des typologies d'attaques observées vont aussi dans ce sens. L'autre moyen pour pousser à la collaboration est d'harmoniser les standards de sécurité entre les opérateurs. Pour cela, il faut avancer vers une adoption de standards communs, par exemple le 3GPP. De plus définir des politiques communes pour l'authentification, le chiffrement, la gestion des incidents ou pour l'isolation des tranches aide à cette harmonisation. Il est aussi possible de mettre en place des accords entre opérateurs pour des audits, des contrôles ou même pour de l'entraide, dans le développement de nouvelle technologie comme on a pu le voir pour la 5G avec Orange et Ericsson.

VI) Proposition et Recommandations

La 5G offre de nombreuses perspectives d'évolution comme la 5G + qui obtient une faible amélioration comme l'avait fait la 4G+ pour la 4G. La 5G + est donc une

version de la 5G légèrement améliorée au niveau de la fréquence et de la bande passante. Couramment appelé 5G + ou 5G SA (Standalone), cette version dérivée de la 5G se différencie par son utilisation d'une architecture à 100% 5G, comparée à la 5G classique (not Standalone) qui elle dépend d'une architecture hybride entre la 5G et la 4G. Seulement la 5G + n'est encore que peu développée et va mettre du temps à l'être car elle requiert une installation matérielle comme des antennes 3,5GHz.

On observe aussi l'apparition de méthodes évoquées dans le rapport pour corriger les failles existantes que nous avons déjà relevées. Par exemple, pour résoudre la sécurisation des données nous préconisions l'utilisation de tunnels VPN au moins pour les communications entre les fonctions. Depuis peu certains opérateurs travaillant sur le noyau de l'architecture 5G commencent à l'utiliser pour les fonctions réseaux. Mais aussi pour les tranches de réseaux utilisées pour transporter des données à risque provenant de diverses applications (bancaire, authentification, etc…).

La 5G est une technologie vouée à se développer. Elle fut limitée lors de son apparition par la compatibilité des appareils présents sur le marché ou par le prix des forfaits mobiles, plus onéreux en raison de la crise COVID. Actuellement, les forfaits et les appareils compatibles sont à prix plus abordable.

VII) Comment avons-nous exploité nos acquis théoriques

Nous nous sommes servis de nombreuses pour ce projet des nombreuses connaissances théoriques enseignées dans les différents modules, plus particulièrement celles acquises dans les mises en situation et initiation réseau, pour faciliter notre compréhension du réseau et de l'architecture de la 5G. Nous étions alors en possession du vocabulaire indispensable pour nos recherches. Nous avons également utilisé nos compétences acquises lors des cours de veille technologique pour la veille active et passive, notamment grâce à l'apprentissage de l'outil Notion. Les cours d'expression écrite et de suite Office 365 nous ont aussi aidé dans la rédaction du rapport écrit. Les compétences développées lors de nos cours d'expression orale nous seront indispensables pour notre soutenance. Ce sont principalement les compétences acquises dans les modules précédemment cités qui nous ont été les plus utiles. Mais pour la compréhension, l'analyse et la rédaction, nous avons utilisé de nombreuses autres compétences acquises dans l'ensemble des modules que l'on a suivis durant notre année de formation.

VIII) Conclusion

Pour répondre à notre problématique, les réseaux 5G font face à de nombreux défis de sécurité notamment à cause de leur architecture innovante. En effet cette dernière augmente les vecteurs d'attaques avec la multiplication des IoT, la densification du réseau et les risques liés à la coexistence des réseaux 5G avec les anciens réseaux. Les nouvelles technologies comme le SDN, le NFV et le Network Slicing apportent aussi leur lot de nouveaux défis. Allant de la dépendance du réseau à ces technologies. Aux nouvelles failles qu'elles créent comme une isolation trop faible des tranches qui offrent un accès au réseau à de potentiels hackeurs. En plus des nouveautés des réseaux 5G, il faut ajouter les attaques touchant les réseaux

depuis des années, comme les attaques DDoS, MITM, Torpedo, Piercer ou encore IMSI Cracking.

Cependant tous ses défis peuvent être surmontés, soit en renforçant les infrastructures liées aux nouvelles technologies des réseaux 5G soit en améliorant ces nouvelles technologies comme le SDN ou le NFV. Cela passe aussi par une sécurisation plus forte des réseaux 5G, notamment par une isolation plus stricte des tranches créées par le Network Slicing. Il faut également limiter les vecteurs d'attaques, les interconnexions vulnérables et renforcer la résilience des réseaux 5G face aux attaques DDoS par exemple. Pour surmonter ces défis, il est primordial, de mettre en place des veilles technologies actives pour suivre les tendances en termes de sécurité, de former en continu les équipes face aux attaques en effectuant des exercices de crise ou des simulations d'incidents. Enfin, avec une collaboration entre les autorités et les entreprises, tous ces défis pourront être surmontés plus facilement.

Cette veille technologique nous a permis d'augmenter nos connaissances autour du réseau et plus particulièrement la 5G. Nous avons pris connaissance des technologies liées à la 5G comme le Network Slicing, le SDN ou encore le NFV. Pour le NFV et SDN, ces technologies ne sont pas propres à la 5G mais liées à l'architecture des réseaux informatiques modernes. Nous nous sommes aussi améliorés dans la rédaction des rapports clairs et structurés, tout en renforçant notre maîtrise de la langue française. Nous nous sommes également améliorés dans la gestion de projet, en développant une meilleure organisation, une planification plus rigoureuse et une communication plus fluide entre les membres de l'équipe. Enfin ce projet contribuera aussi à améliorer notre aisance à l'oral, notamment à travers les mini-oraux autour de notre projet au cours de notre année, mais surtout avec notre soutenance de fin de projet. Tout cela est possible grâce à nos formateurs et nos accompagnants sur ce projet.

Pour conclure ce rapport, arrêtons-nous sur l'importance de la veille technologique dans la sécurisation et l'évolution des réseaux 5G. En effet il est primordial de rester à jour face aux menaces de sécurité, pour réagir le plus rapidement et de la meilleure manière possible face aux attaques. La veille technologique est exactement faite pour ça. Elle est l'outil parfait pour anticiper les menaces futures et pour intégrer les bonnes pratiques en temps voulu. La veille technologique facilite la prise de décision, renforce la capacité d'adaptation et contribue à bâtir une cybersécurité agile et évolutive, capable de suivre le rythme des transformations numériques. La prochaine de ces transformations numériques est le développement de la 5G+, puis de la 6G.

ANNEXES

IX) Webographie

- *Zscaler*, **Qu'est-ce que la sécurité 5G ?**

URL: https://www.zscaler.com/fr/zpedia/what-is-5g-security

- *Chloé-Anne TOUMA,* **Quels sont les défis liés à l'intégration des technologies de la 5G ?** 8 décembre 2022

URL: https://www.cscience.ca/quels-sont-les-defis-lies-a-lintegration-des-technologies-de-la-5g/?gclid=Cj0KCQiAs5i8BhDmARIsAGE4xHxExfJO_OHFgB3CrQ67PoMmkc2-Ujx73-QN1oOxhtQ24iPq5X6EfbUaAjmLEALw_wcB

- *Orange Cyberdéfense,* **Protection des réseaux 5G : Le rôle de l'intelligence sur la menace** 7 décembre 2022

URL: https://www.orangecyberdefense.com/fr/insights/blog/threat-management/protection-des-reseaux-5g-le-role-de-lintelligence-sur-la-menace

- *La rédaction,* **Vulnérabilité 5G : Les nouveaux terrains de jeu des cybercriminels** 15 mars 2024

URL: https://www.servicesmobiles.fr/vulnerabilites-5g-les-nouveaux-terrains-de-jeu-des-cybercriminels-95941

- *Secure-IC* **Mise en œuvre de solutions de sécurité 5G robustes**

URL: https://www.secure-ic.fr/applications/challenges/5g/?utm_source=chatgpt.com

- *Maria Korolov et Jean Elyan,* **Le network slicing 5G potentiellement vulnérable aux attaques** 02 juin 2023

URL: https://www.secure-ic.fr/applications/challenges/5g/?utm_source=chatgpt.com

- *Key Factor,* **Multiplication des appareils IoT non sécurisés**

URL: https://www.keyfactor.com/fr/solutions/telecom-5g-security/?utm_source=chatgpt.com

- *Radware,* **Attaques par déni de service (DDoS)** :

URL: https://fr.radware.com/solutions/5g-network-protection/?utm_source=chatgpt.com

- *Cours des comptes européennes,* **Menaces liées aux fournisseurs à haut risque** mars 2022

URL : https://op.europa.eu/webpub/eca/special-reports/security-5g-networks-03-2022/fr/?utm_source=chatgpt.com

- Fortinet, **Qu'est-ce que la technologie sans fil 5G ?** :

URL: https://www.fortinet.com/fr/resources/cyberglossary/what-is-5g

- Chat GPT : Nous l'avons utilisé pour nous corriger sur la syntaxe, la grammaire, l'orthographe et la conjugaison. Nous nous en sommes également servis pour approfondir nos recherches, notamment en obtenant des liens vers des articles ou des réponses à nos questions. Nous avons pris soin de vérifier toutes les informations qu'il nous fournissait.

- *Roshan Williams,* **Potential cyber security issues with 5G Network** 29 décembre 2024

URL : https://www.linkedin.com/pulse/potential-cyber-security-issues-5g-network-roshan-williams-fpduc/?trackingId=TyF8HEqWQBymW9CKiymKWQ%3D%3D

- *Chroma Campus,* **5G and Cyber Security: Challenges in the New Era of Connectivity** 10 décembre 2024

URL: https://www.linkedin.com/pulse/5g-cyber-security-challenges-new-era-connectivity-croma-campus-d0fhc/?trackingId=3kjttHYnSduwz6FDJysyyQ%3D%3D

- *Ravina Sonawane* **Turbo-Charging Communication: Securing 5G with Encryption Partners** 8 Janvier 2025

URL: https://www.linkedin.com/pulse/turbo-charging-communication-securing-5g-encryption-ravina-sonawane-88hsf/?trackingId=IAoSBzQLT9yYpWV%2BRYf77g%3D%3D

- *Luka Zorko,* **Qu'est-ce que le découpage du réseau 5G ?** 16 novembre 2022

URL: https://tridenstechnology.com/fr/quest-ce-que-le-decoupage-du-reseau-5g/

- *Abdelkader El Fayedh***, IoT, IA et 5G : Quels impacts sur la cybersécurité ?** 23 janvier 2023

UR: Considérations liées à la cybersécurité pour les réseaux 5G :

- *Kasperby***, La technologie 5G est-elle dangereuse ? Les avantages et les inconvénients du réseau 5G**

URL: https://www.kaspersky.fr/resource-center/threats/5g-pros-and-cons

- *Ditri Trio,* **Cinq défis de sécurité 5G que les fournisseurs de services doivent relever** 30 juillet 2020

URL: https://www.nomios.be/fr/actualite/cinq-defis-de-securite-5g/

- *Big Media,* **5G et 6G : quels impacts sur l'innovation et la durabilité en entreprise ?** 18 décembre 2024

URL: https://bigmedia.bpifrance.fr/nos-dossiers/5g-et-6g-quels-impacts-sur-linnovation-et-la-durabilite-en-entreprise#:~:text=La%205G%20entreprise%20offre%20des,service%20pour%20ses%20cslients%20professionnels.

- SFR Business, **Comment la 5G impacte-t-elle la sécurité des usines 4.0 ?** 23 avril 2025

URL: https://www.sfrbusiness.fr/room/5g/comment-la-5g-impacte-securite-usine-40.html

- *Effrei Paris Panthéon ASSAS Université,* ***Cybersécurité : quand les objets connectés et le réseau 5G se menacent*** 28 novembre 2023

URL: https://www.efrei.fr/cybersecurite-quand-les-objets-connectes-et-le-reseau-5g-se-menacent/

- *Juliette Walk Jean Marc Muselli,* **5G : quels risques pour les entreprises ?** 7 avril 2021

URL: https://www.exclusive-networks.com/fr/5g-quels-risques-pour-les-entreprises-par-jean-marc-muselli/

- *Martin Koppe,* **La 5G en mal de sécurité** 23 novembre 2018

URL: https://lejournal.cnrs.fr/articles/la-5g-en-mal-de-securite

- *Thalès,* **Établir l'intégrité, la confidentialité et la disponibilité sur les réseaux 5G**

URL: https://cpl.thalesgroup.com/fr/encryption/5g-security

- *NetScout* ***system INC,*** **Statistiques attaque DDOS** 26 septembre 2023

URL: https://www.businesswire.com/news/home/20230926660640/fr?utm=

- *Réseaux Orange***, Network Slicing**

URL: https://reseaux.orange.fr/actualites/5g-network-slicing.html

- *Bouygues Telecom,* **Network Slicing**

URL: https://www.bouyguestelecom-entreprises.fr/mag-business/lexique/network-slicing/

- *Bouygues Telecom,* **Tout savoir sur la 5G IOT** 23 janvier 2025

URL: https://objenious.com/blogpost/tout-savoir-sur-la-5g-iot/?hl=fr-FR

- *Tiphaine Claveau et Adlen Ksentini,* **Quèsaco le SDN (Software-Defined Networking) ?** 10 mars 2020

URL: https://imtech.imt.fr/2020/03/10/quesaco-le-sdn-software-defined-networking/

- *Frédéric Launay,* **Architecture 5G** 26 février 2021

URL: https://blogs.univ-poitiers.fr/f-launay/tag/nfv/

- *Gilbert Kallenborn,* **Attaques et Statistiques** 16 juin 2020

URL: https://www.01net.com/actualites/les-reseaux5g-deja-plombes-par-de-vieux-tunnels-gprs-vulnerables-1933998.html

- *Frédéric Launay,* **Les tranches de réseau : Network Slicing** 11 février 2018

URL: https://blogs.univ-poitiers.fr/f-launay/2018/02/11/les-tranches-de-reseau-network-slicing/#:~:text=L%27isolation%20est%20une%20exigence,physique%20et%20les%20m%C3%AAmes%20infrastructures.

X) Glossaires

Tous les mots sont rangés dans l'ordre alphabétique

- **3GPP** : Organisme international de normalisation pour les technologies mobiles. Pour revenir au texte : 3GPP.

- **4G LTE** : Le réseau mobile 4G reposant sur la norme LTE, elle fait circuler les appels vocaux non plus sur le réseau téléphonique, mais directement sur internet. Pour revenir au texte : 4G LTE.

- **A10 Networks** : Entreprise américaine cotée en bourse, spécialisée dans la fabrication de contrôleurs et d'applications. Les contrôleurs sont utiles pour le bon fonctionnement du clavier par exemple. Ils ont des partenaires comme Thales ou IBM. Pour revenir au texte : A10 Networks.

- **Adresses IP : Une adresse IP (Internet Protocol) est le numéro** d'identification unique attribué à chaque appareil connecté à Internet. C'est une étiquette numérique attribuée aux dispositifs qui utilisent Internet pour communiquer. Pour revenir au texte : Adresse IP.

- **Alertes Google** : Un outil de Google qui permet de recevoir par mail des notifications sur des sujets précis que l'on définit au préalable. Pour revenir au texte : Alertes Google.

- **ANSSI** : Agence nationale de la sécurité des systèmes d'information, un service français créé par décret en juillet 2009. Pour revenir au texte : ANSSI.

- **API** : Une API (application programming interface ou « interface de programmation d'application ») est une interface logicielle qui permet de « connecter » un logiciel ou un service à un autre logiciel ou service afin d'échanger des données et des fonctionnalités. D'après *la CNIL.* Pour revenir au texte : API.

- **Architecture décentralisée** : Une architecture décentralisée signifie que les fonctions du réseau 5G ne sont plus concentrées dans un seul centre (comme c'était souvent le cas avec les anciens réseaux), mais réparties à plusieurs endroits, plus proches des utilisateurs. Pour revenir au texte : Architecture décentralisée.

- **Architecture distribuée** : Une architecture distribuée signifie que les différentes fonctions du réseau 5G sont réparties sur plusieurs équipements et lieux géographiques, au lieu d'être centralisées dans un seul endroit. Pour revenir au texte : Architecture distribuée.

- **Architecture virtualisée** : Une architecture virtualisée signifie que les fonctions réseau (routeurs, DNS, pare-feu…) ne sont plus forcément assurées par des équipements physiques mais par des logiciels qui tournent sur des serveurs standards. Pour revenir au texte : Architecture virtualisée.

- **Bande passante** : Le terme « bande passante » est utilisé pour décrire la quantité de données digitales qui, en un temps prédéfini, peut être transmise d'un point A à un point B. Elle permet donc de mesurer le débit d'un réseau, et plus précisément la quantité d'information pouvant être téléchargée ou transférée en un temps limité. Pour revenir au texte : Bande passante.

- **Black Hat** : Black Hat est une société fondée en 1997 par Jeff Moss, réputée pour organiser un réseau de conférences fournissant des points de vue nouveaux et exclusifs sur la sécurité de l'information. *D'après Wikipédia*. Pour revenir au texte : Black Hat.

- **Botnets** : Un botnet est un réseau d'ordinateurs infectés par des logiciels malveillants qui sont sous le contrôle d'une seule partie attaquante, connue sous le nom de « bot-herder ». Chaque machine individuelle sous le contrôle du bot-herder est connue sous le nom de bot. Pour revenir au texte : botnets.

- **CERT** : Un computer emergency response team (CERT) est un centre d'alerte et de réaction aux attaques informatiques, destiné aux entreprises ou aux

administrations, mais dont les informations sont généralement accessibles à tous. *D'après Wikipédia.* Pour revenir au texte : CERT.

- **Check Point Quantum** : Exemple de Pare-feu. Pour revenir au texte : Check Point Quantum.

- **CISA (Cybersécurity and infrastructure security Agency)** : CISA est une agence fédérale américaine sous la supervision du département de la Sécurité intérieure des États-Unis. Son objectif est d'améliorer la sécurité informatique à tous les niveaux du gouvernement, de coordonner les programmes de cybersécurité avec les États. Pour revenir au texte : CISA.

- **Cloud** : Le cloud computing est la disponibilité à la demande de ressources informatiques (telles que le stockage et l'infrastructure) en tant que services sur Internet. Ainsi, les particuliers et les entreprises n'ont plus besoin de gérer eux-mêmes leurs ressources physiques, et de ne payer que ce qu'ils utilisent. *D'après Google Cloud.* Pour revenir au texte : Cloud.

- **Couverture réseau** : Désigne la zone géographique concernée par une connexion. Plus la zone est étendue, plus la couverture est puissante. A contrario, une zone non couverte par le réseau est appelée une zone blanche. Pour revenir au texte : Couverture.

- **CVE** : Common Vulnerabilities and Exposures ou CVE est un dictionnaire des informations publiques relatives aux vulnérabilités de sécurité informatique. Pour revenir au texte : CVE.

- **DDoS** : Une attaque par déni de service est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. *D'après Wikipédia.* Pour revenir au texte : DDoS.

- **Débit** : Le débit, c'est la vitesse à laquelle les données sont transmises entre notre appareil (ordinateurs, téléphone…) et Internet. On le mesure généralement en mégabits par seconde ou gigabits par seconde. Plus le débit est élevé, plus on peut télécharger ou envoyer des fichiers rapidement, regarder des vidéos sans coupure, ou jouer en ligne sans latence. Pour revenir au texte : débit.

- **DEF CON** : La DEF CON est la convention hacker la plus connue à travers le monde. Elle est tenue chaque année à Las Vegas, Nevada aux États-Unis. Pour revenir au texte : DEF CON.

- **DNS** : Le *Domain Name System* (Système de nom de domaine) ou DNS est un service informatique distribué qui associe les noms de domaine Internet avec leurs adresses IP ou d'autres types d'enregistrements. *D'après Wikipédia.* Pour revenir au texte : DNS.

- **Ericsson** : Ericsson est une entreprise suédoise de télécommunications. Pour revenir au texte : Ericsson

- **Excel** : Microsoft Excel est un logiciel tableur de la suite bureautique Microsoft Office développé et distribué par l'éditeur Microsoft. Pour revenir au texte : Excel

- **Exploits** : Un exploit ou code d'exploitation est, dans le domaine de la sécurité informatique, un élément de programme permettant à un individu ou à un logiciel malveillant d'exploiter une faille de sécurité informatique dans un système informatique. *D'après Wikipédia*. Pour revenir au texte : Exploits.

- **FortiGate** : Exemple de pare-feu. Pour revenir au texte : FortiGate.

- **Fortinet** : Fortinet est une multinationale américaine dont le siège social se situe à Sunnyvale (Californie). Elle conçoit et commercialise, entre autres, des logiciels, équipements (appliances) et services de cybersécurité tels que des pares-feux, anti-virus, systèmes de prévention d'intrusion et de sécurité des terminaux. Elle occupe le quatrième rang mondial des acteurs de la sécurité réseau quant au chiffre d'affaires. L'entreprise est en partenariat avec Cisco, Google ou encore IBM. *D'après Wikipédia.* Pour revenir au texte : Fortinet.

- **Flux de données** : Un flux de données est la transmission d'une séquence de signaux cohérents codés numériquement pour transmettre des informations. Typiquement, les symboles transmis sont regroupés en des séries de paquets. *D'après Wikipédia.* Pour revenir au texte : Flux de données.

- **Fréquence** : La fréquence correspond au nombre d'opérations effectuées en un temps donné. Pour revenir au texte : Fréquence.

- **FWA** : Le Fixed Wireless Access (FWA) désigne une connexion Internet haut débit fournie via un réseau mobile, comme la 5G, sans avoir besoin de câbles (fibre ou ADSL) jusqu'au domicile ou au bureau. Pour revenir au texte : FWA.

- **GSMA (GSM association)** : La GSM Association (GSMA ou *Global System for Mobile Communications*), autrefois dénommé *Groupe Spécial Mobile* est une association internationale représentant les intérêts de plus de 750 opérateurs

et constructeurs de téléphonie mobile de 220 pays du monde, auxquels s'ajoutent 400 autres entreprises de la sphère de la téléphonie mobile plus large, qui sont membres associés. *D'après Wikipédia.* Pour revenir au texte : GSMA.

- **GSMA Security Reports** : Rapport de sécurité de GSMA. Pour revenir au texte : GSMA Security Reports.

- **IDS** : Un système de détection des intrusions (IDS) est une application qui surveille le trafic réseau et recherche les menaces connues et les activités suspectes ou malveillantes. L'IDS envoie des alertes aux équipes informatiques et de sécurité lorsqu'il détecte des risques et des menaces de sécurité. *D'après Wikipédia.* Pour revenir au texte : IDS.

- **IMSI** : L'International Mobile Subscriber Identity (IMSI, soit " identité internationale d'abonné mobile") est un numéro unique, qui permet à un réseau de téléphonie mobile d'identifier un usager. Ce numéro est stocké dans la carte SIM et n'est pas connu de l'utilisateur. Pour revenir au texte : IMSI.

- **IMSI Cracking** : Une technique d'attaques utilisée pour intercepter ou découvrir l'IMSI d'un utilisateur mobile. Pour revenir au texte : IMSI Cracking.

- **Industrie 4.0** : Le concept d'industrie 4.0 (également appelé industrie du futur ou quatrième révolution industrielle) désigne une nouvelle manière d'organiser les moyens de production. Cette nouvelle industrie se caractérise par la convergence du monde virtuel, de la conception numérique et de la gestion (opérations, finance et marketing) avec les produits et objets du monde physique. *D'après Wikipédia.* Pour revenir au texte : Industrie.

- **Instance logicielle :** Les instances logicielles désignent des copies indépendantes d'un même logiciel qui fonctionnent en parallèle sur un ou plusieurs serveurs. Par exemple, dans le cloud, on peut lancer plusieurs instances d'une application pour gérer plus d'utilisateurs ou répartir la charge. Cela permet de rendre un service plus flexible et plus fiable. Pour revenir au texte : Instances logicielles.

- **IOC** (Indicators of Compromise) : Lors d'un incident de cybersécurité, les indicateurs de compromission sont des indices et des preuves d'une fuite de données. Ces miettes numériques peuvent révéler non seulement qu'une attaque a eu lieu, mais aussi la plupart du temps quels outils ont été utilisés dans l'attaque et qui est derrière elle. Pour revenir au texte : IOC.

- **IoT** : L'Internet des objets ou IoT est l'interconnexion entre l'Internet et des objets, des lieux et des environnements physiques. Pour revenir au texte : IoT.

- **IPS** : Un système de prévention d'intrusion (ou IPS, *intrusion prevention system*) est un outil des spécialistes en sécurité des systèmes d'information, similaire aux systèmes de détection d'intrusion (ou IDS, *intrusion detection system*), permettant de prendre des mesures afin de diminuer les impacts d'une attaque. C'est un IDS actif, il peut par exemple détecter un balayage automatisé malveillant, et bloquer les ports. *D'après Wikipédia.* Pour revenir au texte : IPS.

- **Juniper SRX Series** : Exemple de pare-feu. Pour revenir au texte : Juniper.

- **KPI** : Les KPI (Indicateurs Clés de Performance) sont des mesures quantitatives utilisées pour évaluer l'efficacité, la performance ou la qualité d'un service informatique. Pour revenir au texte : KPI.

- **L'IA** : L'intelligence artificielle ou IA est la capacité des machines à effectuer des tâches typiquement associées à l'intelligence humaine, comme l'apprentissage, le raisonnement, la résolution de problème, la perception ou la prise de décision. *D'après Wikipédia*. Pour revenir au texte : IA.

- **Latence** : En informatique, la latence est le délai de transmission dans les communications informatiques. Il désigne le temps nécessaire à un paquet de données pour passer de la source à la destination à travers un réseau. À n'importe quel paquet transmis par réseau correspond donc une valeur de latence. *D'après Wikipédia.* Pour revenir au texte : latence.

- **LinkedIn** : LinkedIn est un réseau social professionnel. Pour revenir au texte : LinkedIn.

- **Machine Learning** : Le machine Learning ou apprentissage automatique, c'est quand un ordinateur apprend à reconnaître des choses tout seul en regardant beaucoup d'exemples, sans qu'on lui dise exactement quoi faire. Pour revenir au texte : Machine Learning.

- **Malwares** : Un logiciel malveillant ou malware, aussi dénommé logiciel nuisible ou programme malveillant, est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté. *D'après Wikipédia*. Pour revenir au texte : Malwares.

- **Man in the middle** : L'attaque de l'homme du milieu ou *man-in-the-middle attack* (MITM) est une attaque ayant pour but d'intercepter les communications

entre deux parties, sans que ni l'une ni l'autre puisse se douter que le canal de communication entre elles a été détourné. *D'après Wikipédia.* Pour revenir au texte : MITM.

- **MEC (multi-access Edge computing) :** Dans le domaine des réseaux et des réseaux mobiles, le MEC est un concept dont l'architecture est standardisée. Un environnement MEC permet de fournir à des applications des services réseau ; en particulier des communications ultra-fiables à faible latence et un accès très haut débit. Pour revenir au texte : MEC.

- **Mural** : Mural est une plateforme de collaboration visuelle qui permet aux équipes de travailler ensemble en temps réel. Pour revenir au texte : Mural.

- **NETSCOUT** : NETSCOUT est une entreprise américaine dans le domaine de l'informatique connue pour être un fournisseur de produits de gestion des performances des applications et des performances du réseau. Ils ont de nombreux partenaires comme Google, Microsoft ou encore Palo Alto. Pour revenir au texte : NETSCOUT.

- **Nokia :** Nokia est une marque anciennement connue pour ses téléphones, et qui aujourd'hui a comme secteur d'activité principal la 5G. Nokia a signé plusieurs contrats importants avec des opérateurs comme Verizon, SFR ou encore Orange. Pour revenir au texte : Nokia

- **Notion :** Notion est un outil numérique tout-en-un qui permet d'organiser et de gérer des informations. On l'utilise pour prendre des notes, créer des bases de données, gérer des projets ou collaborer en équipe. Il est apprécié pour sa flexibilité et sa facilité d'utilisation, que ce soit pour un usage personnel ou professionnel. Pour revenir au texte : Notion.

- **Observium** : Observium est une plate-forme de surveillance et de gestion du réseau qui fournit des informations en temps réel sur la santé et les performances du réseau. Il peut détecter automatiquement les appareils et services réseau, recueillir des mesures de performance et générer des alertes lorsque des problèmes sont détectés. Pour revenir au texte : Observium.

- **ONAP** : ONAP est une plate-forme pour l'orchestration, la gestion et l'automatisation des services d'informatique de réseau et de périphérie pour les opérateurs de réseaux, les fournisseurs de cloud et les entreprises. L'orchestration et l'automatisation en temps réel des fonctions de réseau physiques et virtuelles permettent une automatisation rapide des nouveaux services et une gestion complète du cycle de vie, essentiels pour les réseaux

5G et de nouvelle génération. *D'après leur site officiel.* Pour revenir au texte : ONAP.

- **Orange** : Orange est un opérateur français et un des principaux opérateurs dans le monde. Pour revenir au texte : Orange.

- **O-RAN SMO :** Le O-RAN SMO est un composant clé dans les réseaux mobiles modernes, surtout dans l'architecture Open RAN. Il sert à superviser, configurer et optimiser automatiquement les équipements radios provenant de différents fabricants. L'objectif est de rendre les réseaux plus ouverts, flexibles et moins dépendants d'un seul fournisseur. Pour revenir au texte : O-RAN.

- **Palo Alto Network Next-Gen Firewall**: Un exemple de pare-feu. Pour revenir au texte : Palo Alto Network.

- **Pare-feu** : Dispositif qui protège un système informatique connecté à Internet des tentatives d'intrusion qui pourraient en provenir. Pour revenir au texte : Pare-feu

- **Piercer** : Piercer est une attaque qui permet à un pirate d'associer l'adresse IP d'un téléphone à son identité IMSI. Une fois l'IMSI volé, l'attaquant peut suivre une personne, contourner l'anonymat ou lancer des attaques depuis l'appareil de la personne piratée. Pour revenir au texte : Piercer.

- **Powerpoint** : Powerpoint est un logiciel du pack Office qui sert à faire des présentations sous forme de diaporama. Pour revenir au texte : Powerpoint.

- **Processeurs** : Un processeur ou unité centrale de traitement est un composant électronique présent dans de nombreux dispositifs électroniques qui exécute les instructions machine des programmes informatiques. *D'après Wikipédia.* Pour revenir au texte : Processeurs.

- **Routeur :** Un routeur est un équipement réseau informatique assurant le routage des paquets. Son rôle est de faire transiter des paquets d'une interface réseau vers leur destination, au mieux, selon un ensemble de règles. Pour revenir au texte : routeur.

- **Sandia National Laboratories** : Sandia National Laboratories est un centre de recherche et de développement scientifique situé aux États-Unis. Pour revenir au texte : Sandia.

- **Scrubing center :** Un scrubing center est un type d'installation ou de service utilisé dans la sécurité de l'information et des réseaux. Il filtre le trafic malveillant

à partir d'un réseau ou d'une connexion Internet. Ces centres se spécialisent dans la surveillance et le filtrage du trafic pour détecter les activités malveillantes, telles que les attaques par déni de service distribué (DDoS), l'activité des botnets, la propagation de logiciels malveillants et d'autres cybermenaces. Pour revenir au texte : Scrubing.

- **Serveur** : Un serveur informatique est un dispositif informatique qui offre des services à un ou plusieurs clients. Les services les plus courants sont : l'accès aux informations du World Wide Web ; le courrier électronique ; le partage de périphériques ; le commerce électronique ; le stockage en base de données. *D'après Wikipédia.* Pour revenir au texte : serveur.

- **Serveur DNS** : Un serveur Domain Name System ou DNS fonctionne comme un annuaire d'Internet. Il permet à nos appareils de trouver le bon chemin vers un site web, en transformant le nom du site en adresse IP compréhensible pour les machines. Pour revenir au texte : Serveur DNS.

- **Shodan :** Un moteur de recherche spécialisé qui permet de détecter les appareils connectés à Internet et leurs vulnérabilités. Pour revenir au texte : Shodan.

- **SLA (services level agreement)** : Le service-level agreement ou " accord de niveau de service" est un document qui définit la qualité de service, prestation prescrite entre un fournisseur de service et un client. D'après Wikipédia. Pour revenir au texte : SLA.

- **Smart city** : Une ville intelligente est un syntagme désignant la capacité d'une ville à utiliser les technologies de l'information et de la communication pour améliorer la qualité des services urbains ou réduire leurs coûts. *D'après Wikipédia.* Pour revenir au texte : Smart City.

- **SOC** : Le Centre des Opérations de Sécurité est une division, dans une entreprise, qui assure la sécurité de l'organisation et surtout le volet sécurité de l'information. Si on fait référence à un SOC dans un bâtiment, il s'agit d'un lieu où est supervisé le site, avec des logiciels de traitement de données spécifiques. *D'après Wikipédia.* Pour revenir au texte : SOC

- **Système de transport intelligent** : Les systèmes de transport intelligents sont les applications des nouvelles technologies de l'information et de la communication au domaine des transports et de sa logistique. *D'après Wikipédia.* Pour revenir au texte : Transport Intelligent.

- **Threat Intelligence Platforms (TIP) :** Des plateformes centralisant et analysant des informations sur les menaces pour aider à anticiper les attaques. Pour revenir au texte : TIP.

- **Torpedo :** Ce processus a pour but de déterminer si un appareil se trouve à proximité. L'attaque exploite un problème de notifications lors d'un appel entrant ou bien lors de la réception d'un message. Pour revenir au texte : Torpedo.

- **Tunnel VPN :** Un tunnel VPN capture et crypte les données à l'aide de protocoles qui protègent les données en provenance et à destination de vos appareils. Pour revenir au texte : Tunnel VPN.

- **Veille active** : La veille active permet à une entreprise de se maintenir informée de l'évolution de son secteur d'activité. Elle répond à un projet ou un objectif précis. Elle peut être temporaire, occasionnelle, permanente. Pour revenir au texte : veille active.

- **Virtualisation :** En informatique, la virtualisation c'est l'action de créer une version virtuelle et du même niveau d'abstraction d'un élément, en particulier du matériel programmable, du stockage et des ressources réseaux. *D'après Wikipédia.* Pour revenir au texte : virtualisation.

- **VNFM :** VNFM ou le gestionnaire des fonctions de réseau virtuel est un élément clé du cadre architectural de gestion et d'organisation de la virtualisation des fonctions réseaux (NFV). Le NFV définit des normes pour les ressources de calcul, de stockage et de mise en réseau qui peuvent être utilisées pour construire des fonctions de réseau virtualisées. Pour revenir au texte : VNFM.

- **VulnDB** : Une base de données recensant de façon détaillée les vulnérabilités connues dans les logiciels et matériels. Pour revenir au texte : VulnDB.

- **Word :** Word est un logiciel du pack Office qui permet de rédiger du texte. Pour revenir au texte : Word.

- **XMind** : XMind est un logiciel de carte mentale et de brainstorming, développé par XMind Ltd. En plus des éléments de gestion, le logiciel peut être utilisé pour capturer des idées, clarifier la pensée, gérer des informations complexes et promouvoir la collaboration d'équipe. *D'après Wikipédia*, pour revenir au texte : XMind.

- **Zabbix :** Zabbix est un logiciel libre permettant de surveiller l'état de divers services réseau, serveurs et autres matériels réseau, et produisant des

graphiques dynamiques de consommation des ressources. D'après Wikipédia, pour revenir au texte : Zabbix.

- **Zero Day** : Une faille Zero Day est une faille de sécurité inconnue du fabricant d'un logiciel ou d'un système. Cela signifie qu'aucun correctif n'existe encore et que les pirates peuvent l'exploiter avant que les développeurs ne découvrent et ne corrigent la faille. C'est une des formes de vulnérabilités les plus dangereuses car elle laisse les systèmes sans défense. Pour revenir au texte : zéro day.

XI) Documents supplémentaires

Pour des informations supplémentaires ou en compléments sur le SDN et NFV

Schéma des couches utilisé par l'architecture 5G

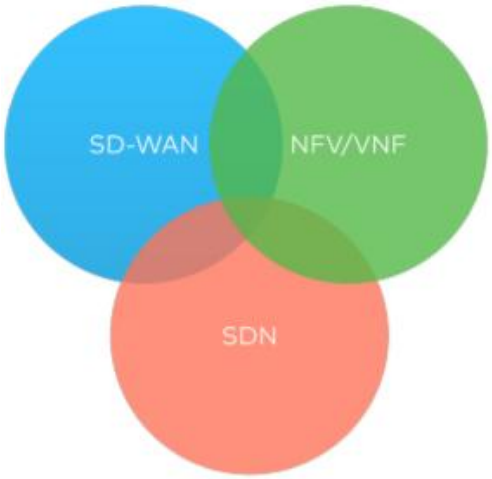


Schéma de comparaison entre les architecture virtuelle et hybride, comprenant les niveaux et couche des différentes fonctions

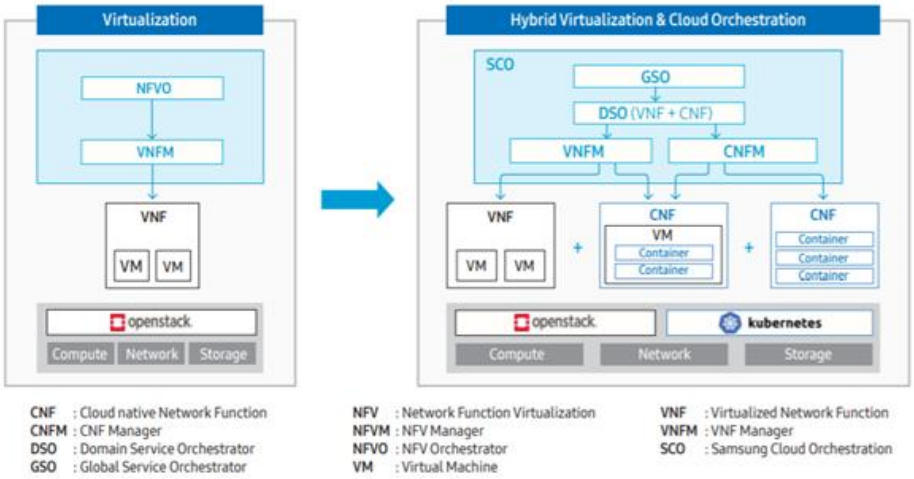
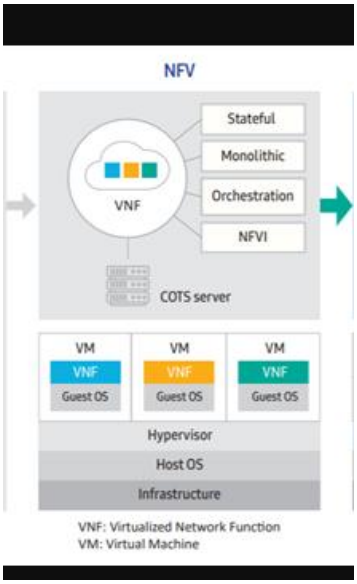


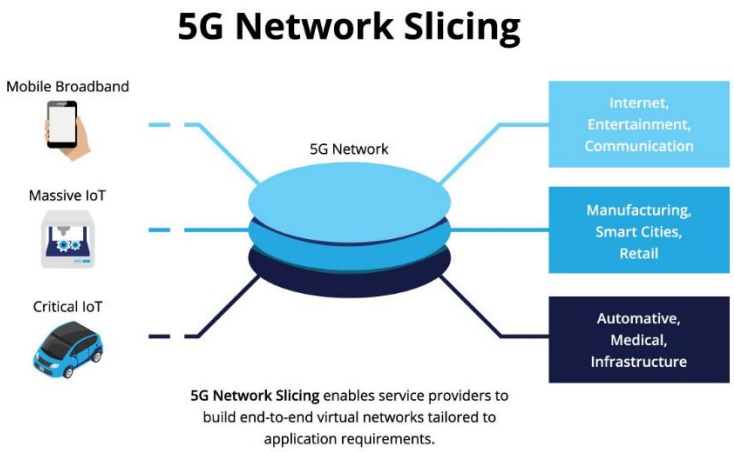
Schéma explicatif du fonctionnement du NFV



Pour des informations supplémentaires ou en complément sur le Network Slicing

Schéma représentatif du Network slicing sur un réseaux 5G

Lucas MOLENDI & Thomas BRAUD



Pour des informations supplémentaires ou en compléments sur les attaques touchants les réseaux 5G :

Diagramme sur les statistiques des sources des attaques 5G

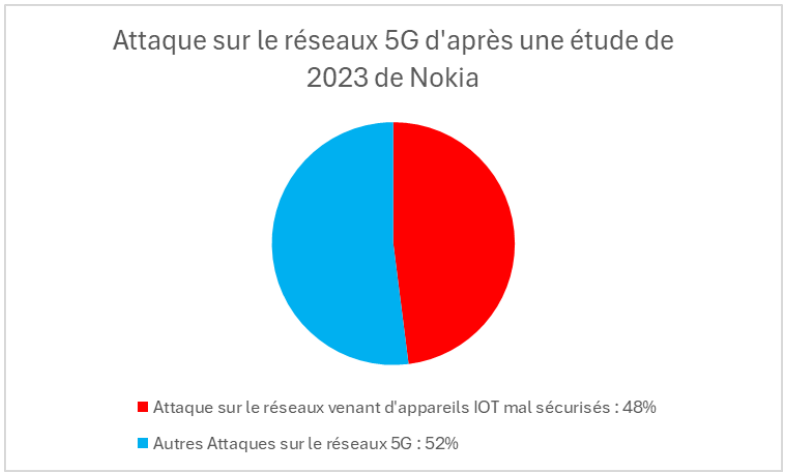
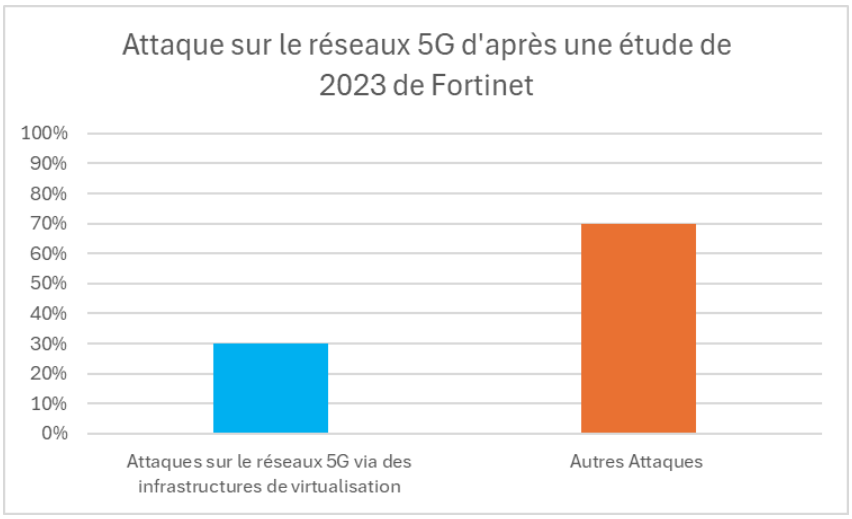


Diagramme sur les origines des faiblesse 5G en 2023



Lucas MOLENDI & Thomas BRAUD

Statistiques d'un rapport de Gcore

Diagramme montrant les industries les plus touché par des attaques

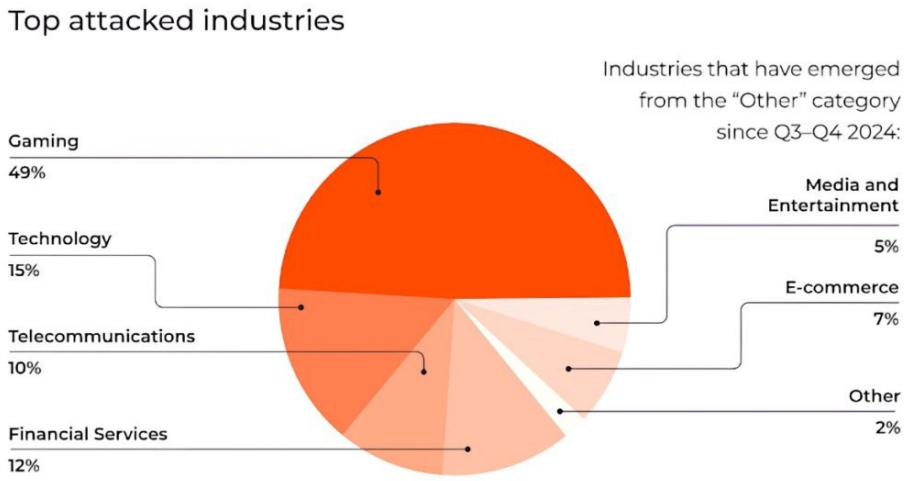
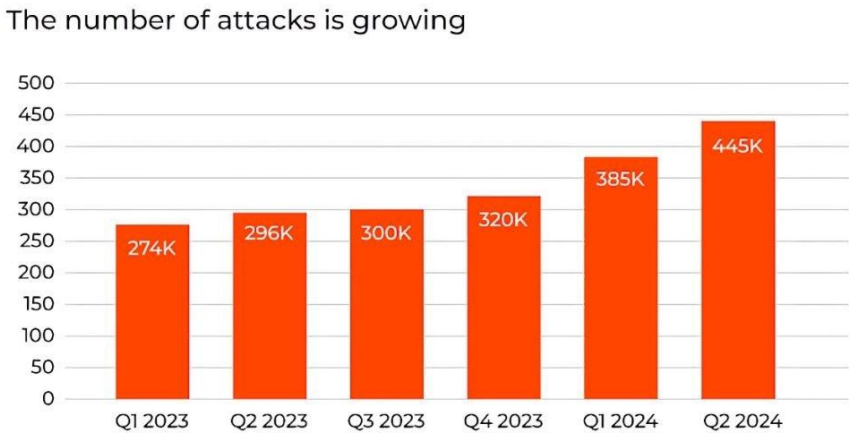


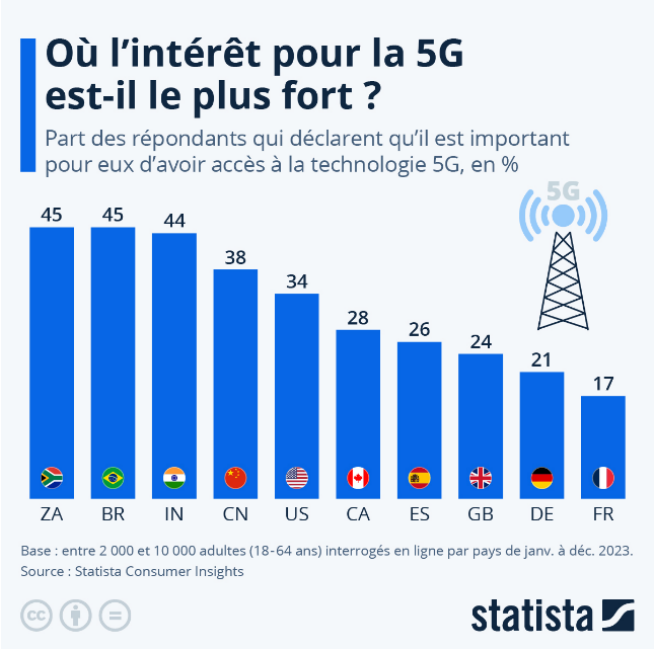
Diagramme montrant le nombres d'attaque par trimestre



Pour des informations supplémentaires ou complémentaires sur la 5G :

Diagramme de l'intérêt des pays pour la 5G.

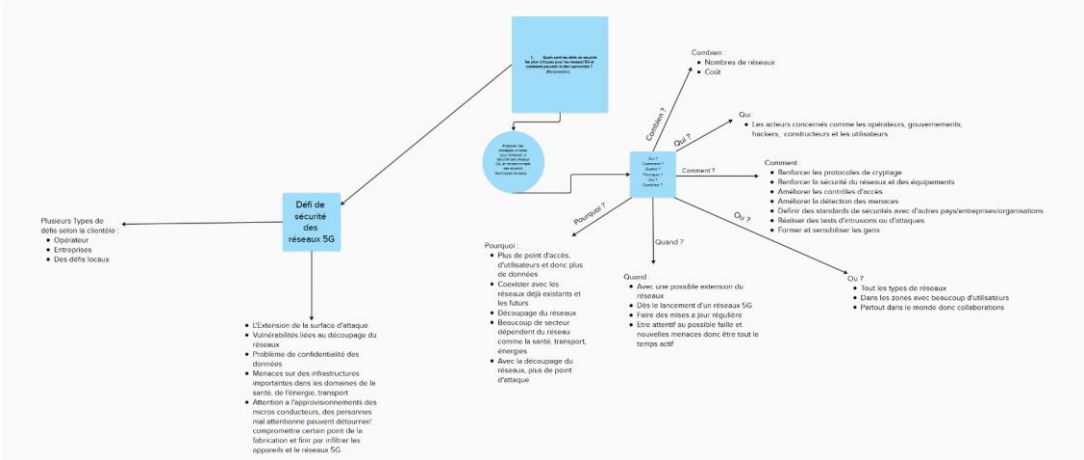
Lucas MOLENDI & Thomas BRAUD



Pour des informations sur notre méthodologie :

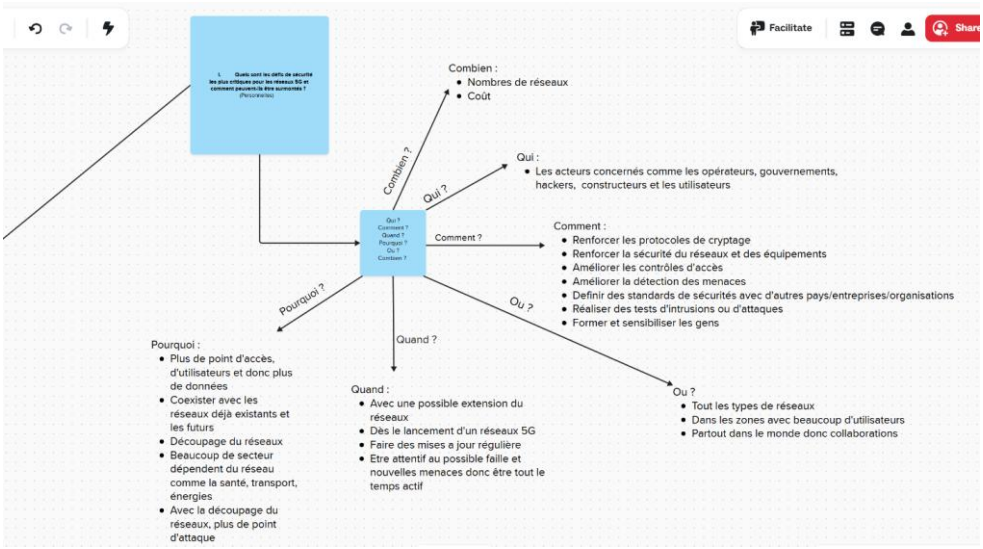
Mural

Vue d'ensemble du Mural (utilisé pour le brainstorming)

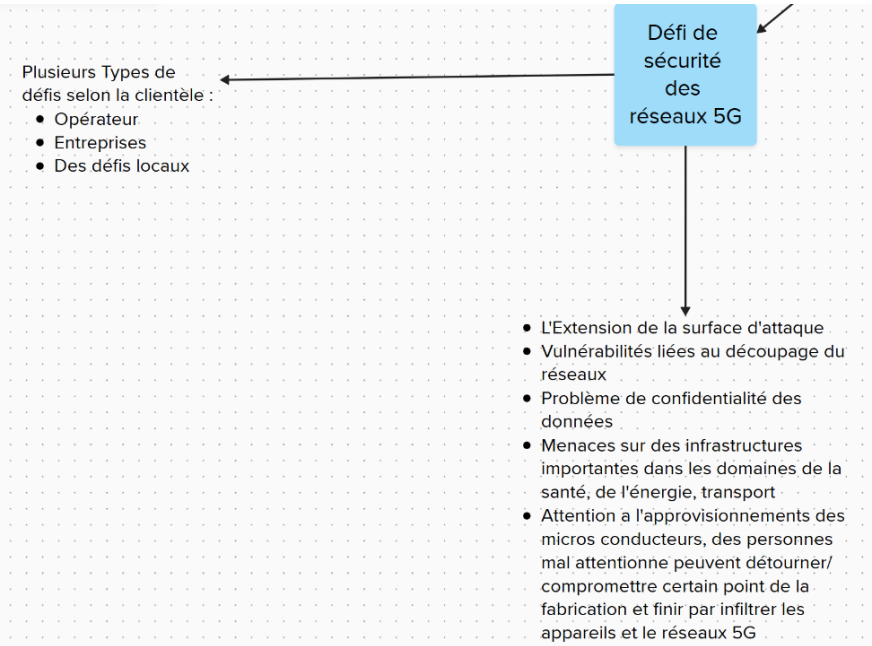


Le QQOQCP

Lucas MOLENDI & Thomas BRAUD



Les défis de sécurités : Nos premières idées



XMind

Schéma Xmind utilisé pour l'organisation

Lucas MOLENDI & Thomas BRAUD

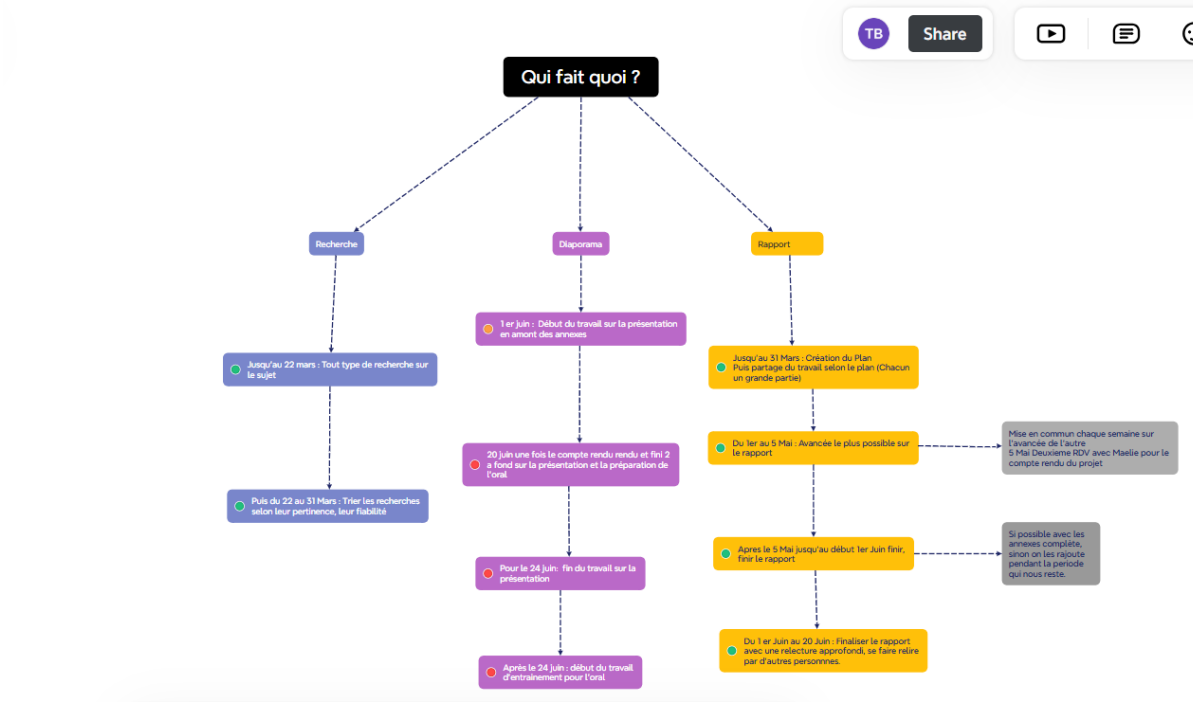
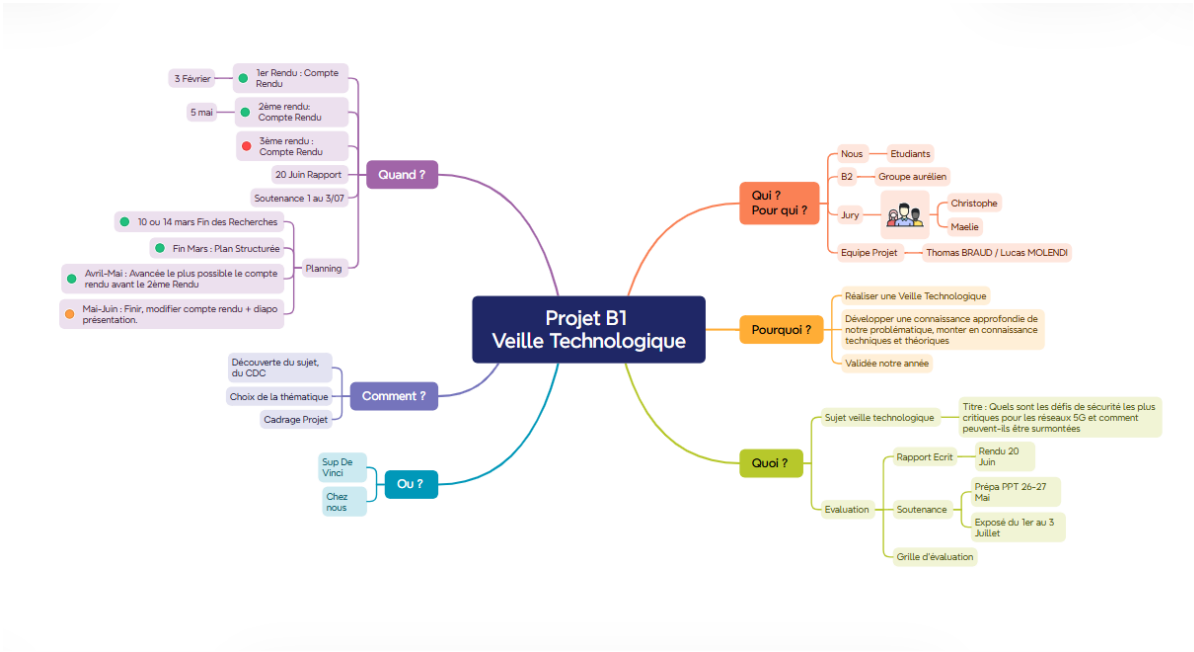


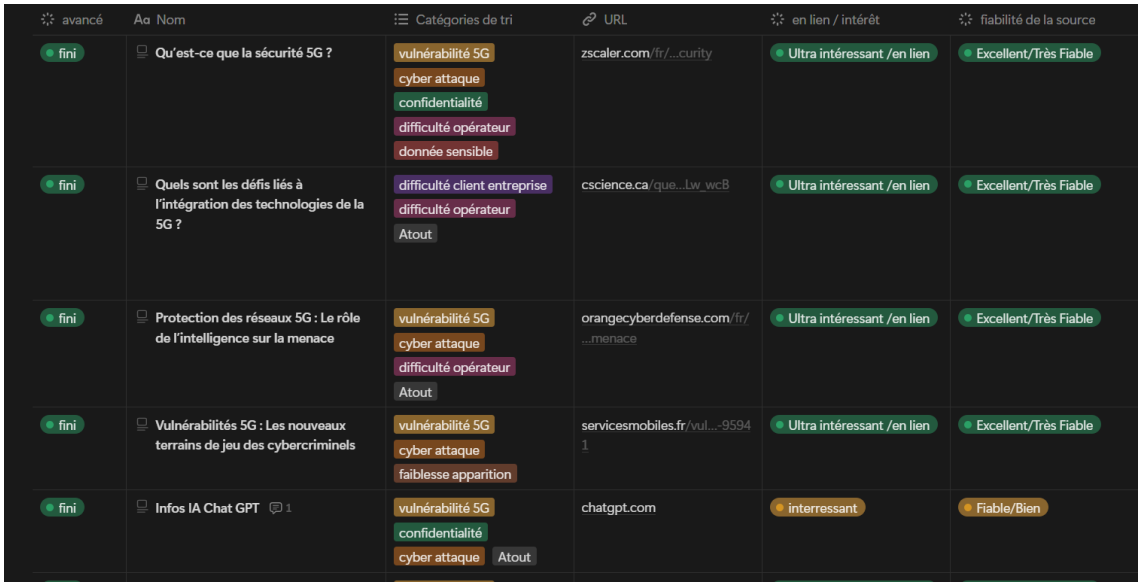
Schéma Xmind du cadrage du projet



Notion

Quelques captures de notre tableau regroupant nos articles. (Tout les articles ne sont pas dans les captures)

Lucas MOLENDI & Thomas BRAUD



avancé	Nom	Catégories de tri	URL	en lien / intérêt	fiabilité de la source
fini	Qu'est-ce que la sécurité 5G ?	vulnérabilité 5G, cyber attaque, confidentialité, difficulté opérateur, donnée sensible	zscaler.com/fr/...curity	Ultra intéressant /en lien	Excellent/Très Fiable
fini	Quels sont les défis liés à l'intégration des technologies de la 5G ?	difficulté client entreprise, difficulté opérateur, Atout	cscience.ca/que...Lw_wcB	Ultra intéressant /en lien	Excellent/Très Fiable
fini	Protection des réseaux 5G : Le rôle de l'intelligence sur la menace	vulnérabilité 5G, cyber attaque, difficulté opérateur, Atout	orangecyberdefense.com/fr/...menace	Ultra intéressant /en lien	Excellent/Très Fiable
fini	Vulnérabilités 5G : Les nouveaux terrains de jeu des cybercriminels	vulnérabilité 5G, cyber attaque, faiblesse apparition	servicesmobiles.fr/vul...-95941	Ultra intéressant /en lien	Excellent/Très Fiable
fini	Infos IA Chat GPT 1	vulnérabilité 5G, confidentialité, cyber attaque, Atout	chatgpt.com	interressant	Fiable/Bien
fini	Potential cyber security i OUVRIR 5G Network	vulnérabilité 5G, cyber attaque, confidentialité, donnée sensible, IoT, Atout	linkedin.com/pul...%3D%3D	Ultra intéressant /en lien	Excellent/Très Fiable
fini	5G and Cyber Security: Challenges in the New Era of Connectivity	donnée sensible, Atout, DécoupageRéseaux	linkedin.com/pul...%3D%3D	Ultra intéressant /en lien	Fiable/Bien
fini	Turbo-Charging Communication: Securing 5G with Encryption Partners	confidentialité, cyber attaque, Collaboration, IoT	linkedin.com/pul...%3D%3D	interressant	Excellent/Très Fiable
fini	Qu'est-ce que le découpage du réseau 5G ?	Atout, DécoupageRéseaux	tridenstechnology.com/fr/...au-5g/	interressant	Fiable/Bien

Capture d'écran montrant un résumé d'article rédigé dans les feuilles de chaque article

Défis pour les opérateurs :

- **Virtualisation du réseau** : La 5G repose sur des réseaux virtualisés, nécessitant la mise en place de services infonuagiques.
- **Maintenance et automatisation** : Les opérateurs doivent gérer des opérations quotidiennes complexes, incluant l'automatisation et des approches CI/CD pour assurer la fiabilité du réseau.

Défis pour les entreprises :

- **Connectivité sur demande et sécurisée** : Les entreprises recherchent une connectivité fiable et rapide pour des applications telles que l'Internet des objets, la réalité augmentée et les véhicules connectés.
- **Souveraineté des données et rapidité des tests** : Elles exigent également une souveraineté des données et la capacité de réaliser des tests rapidement.

L'article souligne également les défis locaux, notamment le manque de main-d'œuvre qualifiée, l'évolution du marché et les difficultés d'approvisionnement en composants essentiels.

Selon l'Association canadienne des télécommunications sans fil, la 5G pourrait créer 250 000 emplois permanents à temps plein au Canada d'ici 2026, posant des défis en matière de ressources humaines.

Enfin, la pandémie a accentué le besoin de services multicloud, avec une augmentation significative du trafic de données mobiles, nécessitant des systèmes plus performants pour répondre à la demande croissante.