LES RÉSEAUX MOBILES DE 5ÈME GÉNÉRATION : QUELS ENJEUX POUR LA SÉCURITÉ NATIONALE

par Mathieu Guizout,
Trèfle Ingénierie,
Consultant Sécurité

www.groupetrefle.com

Les réseaux mobiles de cinquième génération vont devenir les tuyaux des communications de demain. La technologie 5G promet de répondre à des usages très variés (notamment l'Internet des objets, la télémédecine ou encore les voitures autonomes) et stimulera sans nul doute la croissance du trafic et du nombre d'appareils connectés. Mais elle suscite en parallèle des inquiétudes quant à la sécurité numérique des réseaux mobiles.

Dans ce contexte, le législateur est intervenu afin de garantir un déploiement de la technologie 5G soucieux des intérêts de la défense et de la sécurité nationale.

Les nouveaux défis posés par le développement des réseaux mobiles de cinquième génération

Genèse : une évolution marquée par la dépendance accrue du public aux réseaux télécoms

Pourquoi en 2020 la sécurité des réseaux mobiles est-elle devenue critique au point qu'on légifère sur le sujet ?

La réponse tient au fait que les réseaux mobiles supportent l'économie numérique qui occupe à ce jour une place proéminente dans l'économie française.

Le recours intensif à Internet par le public a poussé le secteur de la téléphonie à muer avec son temps, proposant des contenus de plus en plus élaborés, nécessitant des débits plus importants, par exemple Netflix, Uber & PokémonGO. Alors qu'à ses débuts l'utilisation d'Internet ne représentait qu'une part infime de la consommation sur les réseaux mobiles, en 2020, elle représente plus de la moitié du trafic mondial.

Un autre facteur est la dépendance de notre modèle sociétal à la technologie, dépendance qui n'a cessé de s'accroitre ces vingt dernières années. Celle-ci est désormais omniprésente et a permis d'améliorer des activités essentielles. Un exemple flagrant est celui des numéros de secours (15,17,18 & 112) qui utilisent désormais la géolocalisation ou encore la récente mise en place de systèmes de transport intelligents afin d'améliorer la réactivité, la sécurité, la mobilité et les performances environnementales du transport routier en fournissant des informations via les réseaux mobiles aux secours[1].

Aujourd'hui le recours à la technologie est devenu incontournable pour de nombreuses industries et secteurs d'activités et toute atteinte affectant les réseaux ou les services de télécommunications est susceptible d'avoir des répercussions économiques importantes.

[1] Directive 2010/40/UE du Parlement européen et du Conseil du 7 juillet 2010 concernant le cadre pour le déploiement de systèmes de transport intelligents dans le domaine du transport routier et d'interfaces avec d'autres modes de transport, transposée par l'Ordonnance n° 2012-809 du 13 juin 2012 relative aux systèmes de transport intelligents

La sécurité, enjeu majeur du développement du réseau mobile de 5ème génération

La sécurité nationale est définie comme l'« *ensemble des menaces et des risques susceptibles d'affecter la vie de la Nation, notamment en ce qui concerne la protection de la population, l'intégrité du territoire et la permanence des institutions de la République* »[2].

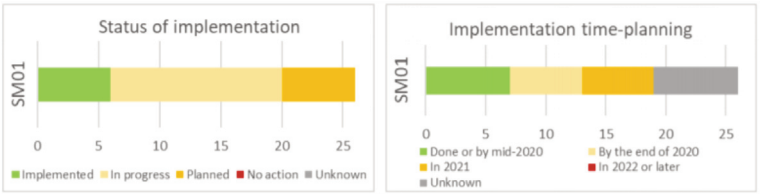
Grâce aux nouvelles technologies, les antennes 5G sont dites « intelligentes » comparées aux antennes 4G où elles étaient dites « passives ». Ces nouvelles technologies exposent les antennes à un risque d'espionnage et de destruction accrus. L'espionnage est un risque qui fait couler beaucoup d'encre depuis que deux fournisseurs étrangers ont été ciblés par des révélations / accusations d'espionnage (Tappy le robot T-Mobile[3], Espionnage sur les salons de technologie et primes spéciales sur le vol d'informations[4], l'attaque sur Nortel[5], l'affaire du DSLAM Alcatel[6] ou encore celle des commutateurs et routeurs Cisco[7], ...), les supposés liens du PDG du 1er fournisseur mondial avec l'armée chinoise[8], la loi de sécurité nationale chinoise[9] où deux équipementiers 5G majeurs ont leur siège social ou encore, la réputation d'espionnage de Pékin (Addis-Abeba[10], MessageTap[11], Opération SoftCell[12], ...).

Les Etats-Unis ont changé de stratégie, elle est particulièrement visible sous l'administration Trump passant d'une diplomatie « de derrière les rideaux » à une stratégie du « *Name and Shame* » envers la Chine. Les attaques que Washington attribue à la Chine font désormais l'objet de déclarations publiques (actes d'accusations contenant les photos des attaquants chinois, gel des actifs et prohibition d'utiliser le Dollar). Le bannissement des équipementiers chinois et les mesures d'interdiction de commercer du département du commerce sont vues par certains observateurs comme une mesure de rétorsion pour ces attaques. La plupart des révélations d'espionnage imputées à Pékin proviennent des États-Unis. Des preuves peuvent exister, elles sont sûrement couvertes par le secret et le grand public ne peut y avoir accès.

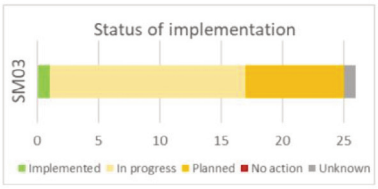
Les mesures d'incitations européennes

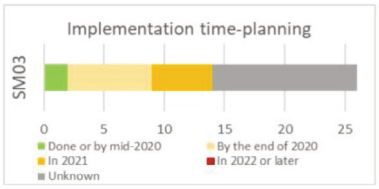
L'Union Européenne s'est prononcée sur la sécurité du marché de la 5G à travers deux séries de mesures, les mesures Stratégiques **SMXX** et les mesures Techniques **TMXX**, publiés dans la boite à outils 5G[13], après une concertation des États membres, le 29 janvier 2020 à l'occasion du FIC 2020. Les États membres restent souverains dans leur manière de mettre en œuvre ces deux types de mesures stratégiques[14] :

- **SM01** Renforcer les pouvoirs réglementaires des autorités nationales notamment en matière d'examen des procédures de marché et de déploiement liés aux réseaux.



[2] Article L1111-1 du Code de la Défense.
[3] Chinese Telecommunications Device Manufacturer and its U.S. Affiliate Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction Of Justice, U.S. DoJ, 28 janvier 2019
[4] Chinese Telecommunications Conglomerate Huawei and Subsidiaries Charged in Racketeering Conspiracy and Conspiracy to Steal Trade Secrets, U.S. DoJ, 13 février 2020
[5] Did a Chinese Hack Kill Canada's Greatest Tech Company?, Natalie Obiko Pearson, Bloomberg, 1er juillet 2020
[6] La France écarte subtilement le chinois Huawei de ses réseaux 5G, Laurent LAGNEAUX, OPEX360, 23 juillet 2020
[7] Huawei's Yearslong Rise Is Littered With Accusations of Theft and Dubious Ethics, WSJ, 25 mai 2019
[8] Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE, U.S. House of Representatives, Permanent Select Committee on Intelligence, 112th Congress, 8 octobre 2012
[9] Article 7 of the National Intelligence Law of the People's Republic, 28th meeting of the Standing Committee of the 12th National People's Congress, 27 June 2017
[10] A Addis-Abeba, le siège de l'Union africaine espionné par Pékin, Le Monde, 26 janvier 2018
[11] MESSAGETAP: Who's Reading Your Text Messages?, FireEye, 31 octobre 2019
[12] Operation Soft Cell: A Worldwide Campaign Against Telecommunications Providers, Cybereason, 25 juin 2019
[13] Secure 5G deployment in the EU: Implementing the EU toolbox - Communication from the Commission
[14] Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity July 2020





■ **SM03** Évaluation du profil de risque des équipementiers 5G (Ericsson, Huawei, Nokia et Samsung, ...) et application de restrictions pour les équipementiers 5G considérés comme présentant des risques élevés - y compris les exclusions nécessaires pour atténuer efficacement les risques pour les actifs clés.

En dépit d'un ralentissement notable dû à la pandémie du COVID-19 et les mesures restrictives qui ont été mises en place, certains États ont bien avancé sur la mise en œuvre de ces mesures stratégiques (notamment la France, l'Italie & les Pays-Bas), il reste que l'Union Européenne est globalement un peu en retard sur son calendrier initial.

On peut déplorer que l'Union Européenne n'ait pas opté pour un outil juridique commun, avec l'adoption d'une directive ou d'un règlement pour répondre de manière unie sur un sujet critique pour le futur des télécommunications européennes, qui s'inscrit dans le marché numérique unique (DSM[15]).

Rappel du cadre juridique français encadrant la sécurité des réseaux :

En France, la problématique de la protection des réseaux est ancienne et les opérateurs sont déjà astreints à des obligations réglementaires en matière de sécurité des réseaux, notamment :

- Des mesures relatives aux traitements des données à caractère personnel, aux fins d'assurer assurer la protection, l'intégrité et la confidentialité des informations identifiantes détenues et traitées[16].

- Des mesures afin de garantir le secret des correspondances et la neutralité des services au regard des contenus des messages transmis[17].

- Des mesures afin d'assurer l'intégrité des réseaux et la continuité des services fournis, en particulier pour assurer la sécurité desdits réseaux et services à un niveau adapté aux risques existants[18].

En parallèle, certaines dispositions encadrent plus spécifiquement les activités des entités en charge des infrastructures critiques du secteur « Communications électroniques, audiovisuel et information ». L'arrêté du 2 juin 2006[19] a en effet reconnu ce secteur comme un des douze secteurs d'activité d'importance vitale et les réseaux mobiles comme étant nécessaires à la production et à la distribution de biens ou de services indispensables à la réalisation de l'un ou plusieurs des cinq objectifs suivants : la satisfaction des besoins essentiels pour la vie des populations, l'exercice de l'autorité de l'Etat, le fonctionnement de l'économie, le maintien du potentiel de défense, la sécurité de la Nation[20].

Les opérateurs télécoms concernés par le statut d'Opérateur d'Importance Vitale (OIV)[21] sont à ce titre assujettis à un corpus normatif visant à préserver la sécurité nationale, notamment la directive nationale de sécurité (DNS)[22] ou encore la loi de programmation militaire qui impose aux OIV le renforcement de la sécurité de leurs systèmes d'information[23].

L'année 2018 sera marquée par la transposition en droit français[24] de la directive Network and Information system Security (NIS), un dispositif de cybersécurité pour les opérateurs de services essentiels, en complémentarité du dispositif de cybersécurité des OIV.

[15] A Digital Single Market for the benefit of all Europeans, European Commission, 6 mai 2015
[16] Article L. 34-1 et Article D. 98-5 II du Code des Postes et des Communications Electroniques.
[17] Article L. 33-1 et Article D. 98-5 I du Code des Postes et des Communications Electroniques.
[18] Article D98.5 III du Code des Postes et des Communications Electroniques.
[19] Arrêté du Premier ministre du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs, modifié par l'arrêté du 3 juillet 2008.
[20] Article R 1332-2 du Code de la Défense.
[21] Pour des raisons de sécurité nationale, la liste des OIV n'est pas publique et il est demandé aux entités concernées de garder cette qualification secrète.
[22] Cette directive est classifiée.
[23] Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.
[24] Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité et les arrêtés du 13 juin, 1er août et 14 septembre 2018.

Les nouvelles mesures législatives pour encadrer les équipements 5G

En 2019, alors que la préparation du déploiement de la 5G s'accélérait, le législateur, afin de pallier les questions sécuritaires posées par les équipements de cinquième génération, a adopté la loi n° 2019-810 du 1er août 2019 *visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles*.

La loi ° 2019-810 du 1er août 2019 vise à compléter le cadre juridique actuellement en vigueur concernant les opérateurs d'importance vitale (OIV) en soumettant à une autorisation du Premier ministre, destinée à préserver les intérêts de la défense et de la sécurité nationale, l'exploitation sur le territoire national des appareils qui par leurs fonctions présentent un risque pour l'intégrité, la sécurité et la continuité de l'exploitation du réseau[25].

L'autorisation est octroyée pour une durée maximale de huit ans « *pour un ou plusieurs modèles les versions de dispositifs matériels ou logiciels précisés par l'opérateur dans son dossier de demande d'autorisation*[26] ». Les services du Premier ministre doivent leur répondre sous deux mois et l'absence de réponse vaut refus : les équipements doivent être retirés[27]. Le renouvellement de l'autorisation fait l'objet d'un dossier de demande de renouvellement, qui est remis au moins deux mois avant l'expiration de l'autorisation en vigueur[28].

L'arrêté du 6 décembre 2019 a enfoncé le clou du cercueil du libre arbitre sur le choix des équipementiers par les opérateurs, en listant les catégories d'appareils soumis à l'article L34-11 du code des postes et des communications électroniques :

Description de l'appareil	**Dénomination de la fonction réseau associée dans les standards 3GPP**
Appareils, ou stations de base, assurant la communication radioélectrique avec les équipements terminaux et l'allocation des ressources radioélectriques	New Radio Base Station (en-gNodeB et gNodeB)
Appareils assurant l'authentification et l'autorisation d'accès au réseau des équipements terminaux	Access and Mobility management Function (AMF) et Authentication Server Function (AUSF)
Appareils assurant l'acheminement des communications des équipements terminaux vers des réseaux tiers	User Plane Function (UPF)
Appareils assurant la gestion des sessions et des connexions des équipements terminaux	Session Management Function (SMF)
Appareils assurant la mise en œuvre et le contrôle des politiques d'accès au réseau	Policy Control Function (PCF)
Appareils assurant la répartition des équipements terminaux et de leurs communications entre les différentes tranches isolées constituant le réseau radioélectrique mobile	Network Slice Selection Function (NSSF)
Appareils assurant l'enregistrement, l'autorisation et la continuité des services au sein du réseau	Network Repository Function (NRF)
Appareils permettant l'exposition des informations du réseau et sa configuration par des appareils externes au réseau	Network Exposure Function (NEF)
Appareils assurant le stockage des données cryptographiques et identifiants relatifs aux abonnés	Unified Data Management (UDM)
Appareils assurant l'interconnexion du réseau mobile avec d'autres réseaux	Security Edge Protection Proxy (SEPP)

[25] Article L. 34-11.-I du Code des Postes et des Communications électroniques.
[26] Ibid.
[27] Ibid.
[28] Ibid.

La réception de ces nouvelles mesures par l'industrie

La loi n°2019-810 du 1er août 2019 a fait grincer des dents les opérateurs français, ceux-ci se voyant astreints à déposer une demande pour chaque équipements 5G installés depuis février 2019. La liste des catégories de matériels concernés n'a été dévoilée que plus tard, par arrêté, ajoutant une période d'incertitude.

Ces nouvelles mesures législatives ont d'ailleurs été publiquement décriées par les opérateurs, Bouygues Telecom et SFR, envisageant même de contester la loi via une question prioritaire de constitutionnalité adressée au Conseil Constitutionnel.

Dans un entretien aux « Echos » en date du 31 janvier 2020, Arthur Dreyfuss, le président de la Fédération française des télécoms est revenu sur la loi n°2019-810 du 1er août 2019 :

« Cette loi, qui devait clarifier la situation, a plongé les opérateurs dans un nuage d'incertitude qui les empêche de faire leur métier, celui de déployer des réseaux numériques performants pour les Français, les entreprises, les collectivités ou les administrations [...] On ne peut pas utiliser la sécurité comme prétexte à des décisions dictées en réalité par des enjeux commerciaux et diplomatiques qui nous dépassent. Et je ne peux pas laisser dire que les opérateurs n'auraient pas conscience des enjeux de sécurité , comme on l'a entendu. Nous employons en France plus de 15.000 ingénieurs et techniciens télécoms qui travaillent quotidiennement à assurer la sécurité des réseaux. Nous sommes comptables devant nos clients - particuliers, entreprises et administrations. Il n'y a jamais eu de problème de sécurité sur nos infrastructures[29] ».

A l'étranger, les réponses diffèrent selon le pays :

A l'international, les mesures mises en place s'inscrivent dans des logiques différentes. Les Etats-Unis ont fait le choix d'interdire deux constructeurs d'antennes chinois de leurs réseaux mobiles 5G, en plus des mesures engagées par l'administration de Donald Trump. Ils espèrent désormais contrebalancer leur absence d'équipementier 5G national via deux stratégies :

- La normalisation d'une initiative nommée OpenRAN, une initiative qui tente d'ouvrir des parties du réseau télécom à un écosystème de petits équipementiers.
- La possibilité de rachat / prise de parts dominante chez Nokia ou Ericsson.

Les États-Unis usent de leur influence pour que leurs décisions sur le marché de la 5G soient aussi appliquées chez leurs alliés et partenaires, menaçant même une réduction du partage des renseignements avec les services des nations qui n'obéiront pas à leur demande, même si cela paraît peu probable d'être appliqué. Cette influence transpire à travers les réunions pour rencontrer différents représentants de nations européennes afin de leur présenter des preuves de l'espionnage, que dénonce les Etats-Unis, effectuées par plusieurs représentants américains dont Robert O'Brien, l'assistant du président pour les affaires de sécurité nationale. Mais les autres nations ont appris à se méfier des États-Unis depuis les fausses preuves sur les armes de destructions massives en Irak, la remise en cause des alliances comme l'OTAN ou encore l'imprévisibilité de l'administration Trump. Ce n'est pas un hasard si la défiance envers les États-Unis s'est accrue et que des pays comme la France poussent désormais pour plus d'autonomie stratégique via une solution européenne.

Au Royaume Uni, dans un premier temps le Gouvernement de sa Majesté avait choisi d'autoriser les vendeurs à hauts risques (HRVs[30]) à hauteur de 35% chez chaque opérateur. Cependant, en juillet 2020, le Gouvernement de sa Majesté a fait marche arrière et désormais les HRvs doivent être enlevés des réseaux d'ici 2027. Le motif est clair, à la suite des nouvelles restrictions du département du commerce américain en mai 2020[31], le NCSC UK (National Cyber Security Centre) et son centre dédié HCSEC (Huawei Cyber Security Evaluation Centre) affirme désormais ne plus être en mesure de contrôler les HRVs.

L'Allemagne n'arrive pas à parler d'une voix unique sur ce sujet et les différentes tentatives de lois proposées ont toutes été avortées. L'Allemagne a un problème de lobbying fort des entreprises du secteur automobile qui dépendent beaucoup du marché des importations chinoises. Ils ont été prompts à se sentir concernés à la suite des déclarations[32] de l'ambassadeur de Chine en Allemagne promettant de potentielles mesures de rétorsions sur le marché automobile allemand si un fournisseur chinois était mis au ban sur le marché allemand.

[29] « S'il interdit Huawei, l'Etat devra indemniser les opérateurs », dit le président de la Fédération française des télécoms, Les Echos, 30 janvier 2020

[30] NCSC advice on the use of equipment from high risk vendors in UK telecoms networks, UK NCSC, 28 janvier 2020

[31] Export Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List, U.S. Bureau of Industry and Security, 19 mai 2020

[32] China Threatens Retaliation Should Germany Ban Huawei 5G, Bloomberg, 15 décembre 2019

Monaco est le premier État à être couvert en 5G entièrement le 9 juillet 2019. A l'aide d'un partenaire chinois, 1er géant des télécommunications au monde, Monaco est désormais couvert via son opérateur Monaco Telecom, détenu majoritairement par Xavier Niel. Intéressant à noter, quand en France, Free aussi détenu par Xavier Niel a choisi Nokia pour ses réseaux 5G.

Conclusion

L'ensemble des mesures de la loi n°2019-810 du 1er août 2019 ont été mises en place pour réduire les risques, elles ne permettront jamais de les faire disparaître. Cependant, supprimer les fournisseurs étrangers à l'Union Européenne ne va pas empêcher l'utilisation de technologies étrangères dans le domaine de la 5G. En effet, une grosse partie[33] des brevets essentiels (SEP) pour la mise en œuvre de la 5G au niveau des antennes appartient au leader mondial, un chinois. De plus, la sécurité des réseaux de télécommunications 5G ne doit pas reposer que sur les équipementiers. Les opérateurs se doivent d'être plus exigeants sur le maintien en condition de sécurité de leurs réseaux historiques, sur la sécurité et les pratiques de leurs fournisseurs ou encore en augmentant les niveaux de sécurité en interne. *La sécurité des réseaux mobiles 5G de demain en dépend.*

[33] Who Owns Core 5G Patents? – A Detailed Analysis of 5G SEPs, GreyB, juin 2020