COMMISSION
EUROPÉENNE

Bruxelles, le 29.1.2020
COM(2020) 50 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS

Sécurité du déploiement de la 5G dans l'UE – Mise en œuvre de la boîte à outils de l'UE

1. ***Introduction***

Les réseaux de télécommunications de cinquième génération (5G) sont appelés à jouer un rôle essentiel dans le développement de la société et de l'économie européennes. Ils devraient offrir de vastes perspectives économiques et constituer une base importante pour la transformation verte et la mutation numérique dans des domaines tels que les transports, l'énergie, l'industrie manufacturière, la santé, l'agriculture et les médias.

Par conséquent, la 5G pourrait avoir une incidence sur pratiquement tous les aspects de la vie des citoyens de l'UE. La cybersécurité des réseaux 5G est donc essentielle non seulement pour protéger nos économies, nos sociétés et nos processus démocratiques, mais aussi pour permettre une transformation numérique fiable dans l'intérêt de tous les citoyens de l'UE.

La dépendance de nombreux services critiques à l'égard des réseaux 5G rendrait les conséquences de perturbations systémiques et généralisées particulièrement graves. En outre, les écosystèmes numériques étant interconnectés, les répercussions au-delà des frontières nationales pourraient être considérables. Garantir la cybersécurité des réseaux 5G revêt donc une importance stratégique pour l'Union, à l'heure où le nombre de cyberattaques ne cesse de croître et alors que ces attaques, plus sophistiquées que jamais, émanent d'une grande variété d'acteurs malveillants, en particulier des acteurs étatiques ou soutenus par un État extérieurs à l'UE. En ce qui concerne la sécurité des infrastructures critiques telles que les réseaux 5G, la démarche choisie consiste à définir, pour la première fois, une approche européenne commune. Cette approche est totalement compatible avec l'ouverture du marché intérieur de l'UE, pour autant que les exigences de l'UE en matière de sécurité soient respectées.

Dans ses conclusions du 22 mars 2019, le Conseil européen a appelé à une approche concertée en matière de sécurité des réseaux 5G. Le 26 mars 2019, la Commission a adopté la recommandation (UE) 2019/534 sur la cybersécurité des réseaux 5G[1]. Cette recommandation invitait les États membres à mener à bien des évaluations nationales des risques, à établir un bilan des mesures nationales, à travailler ensemble au niveau de l'UE sur une évaluation coordonnée des risques et à élaborer une «boîte à outils» de mesures d'atténuation. La présente communication fait partie intégrante de la stratégie numérique européenne globale de la Commission demandée par le Conseil européen.

2. ***Déploiement de la 5G dans l'UE***

Le déploiement d'une infrastructure de réseau 5G en Europe est capitale pour la stratégie industrielle et la compétitivité européennes. La Commission a affirmé que le déploiement des technologies de réseau 5G était un catalyseur essentiel pour les futurs services numériques. En 2016, elle a adopté le plan d'action pour la 5G en Europe, qui vise à faire en sorte que l'Union dispose des infrastructures de connectivité nécessaires à sa transformation numérique à partir de 2020, et que celles qui sont requises pour déployer la 5G dans les zones urbaines et le long des principaux axes de transport soient disponibles d'ici à 2025.[2]. La communication sur la société du gigabit fixe comme ambition un accès à la connectivité mobile des données sur l'ensemble du territoire[3], et notamment dans les zones rurales et isolées.

[1] Recommandation (UE) 2019/534 sur la cybersécurité des réseaux 5G; JO L 88 du 29.3.2019, p. 42.

[2] COM(2016) 588 du 14 juin 2016: «Un plan d'action pour la 5G en Europe».

[3] COM(2016) 587 «Connectivité pour un marché unique numérique compétitif – Vers une société européenne du gigabit».

En ce qui concerne l'assignation des fréquences, les États membres ont attribué 16 % des bandes pionnières pour la 5G[4]. Des consultations pour un certain nombre de procédures d'assignation devraient avoir lieu dans les prochains mois, eu égard à l'obligation légale de délivrer toutes les autorisations nécessaires à l'utilisation de toutes les bandes pionnières pour la 5G d'ici à la fin de l'année.

L'Europe est l'une des régions les plus avancées du monde en ce qui concerne le lancement commercial des services 5G[5]. Aujourd'hui, on estime que les premiers services 5G devraient être disponibles dans 138 villes européennes d'ici à la fin de 2020. Les premiers réseaux 5G sont fondés sur la 4e génération actuelle (4G) des technologies de réseau et les services 5G, principalement fournis au grand public, prennent soit la forme d'une amélioration de la 4G en termes de capacité et de vitesse, soit celle d'une alternative sans fil rentable aux réseaux fixes[6].

En ce qui concerne les possibilités offertes dans le domaine des nouveaux services d'entreprise à entreprise, par exemple dans les secteurs de l'énergie, de l'alimentation et de l'agriculture, des soins de santé, de la production ou des transports, l'Europe est bien avancée, avec un investissement de l'ordre d'1 milliard d'euros, dont 300 millions d'euros au titre du partenariat public-privé 5G dans le cadre du programme Horizon 2020. Cet investissement comprend plus de 160 essais à grande échelle de 5G recensés en Europe, dont dix corridors autoroutiers transfrontaliers pour l'expérimentation à grande échelle de services 5G de mobilité connectée et automatisée. Les essais portent, notamment, sur des applications fondées sur la 5G dans des domaines aussi divers que les soins de santé durables, la mobilité automatisée, l'agriculture efficace sur le plan des ressources, les réseaux électriques intelligents et l'industrie 4.0. En outre, la BEI a fourni, avec le soutien du Fonds européen pour les investissements stratégiques (EFSI), des prêts destinés à accélérer la recherche et le développement dans la technologie 5G.

Le code des communications électroniques européen (ci-après le «code»)[7], qui s'appliquera à partir du 21 décembre 2020, constitue un point de départ important pour établir un climat propice aux investissements pour les réseaux 5G et au-delà. En outre, des programmes de financement public, tels que le volet numérique du mécanisme pour l'interconnexion en Europe[8] ou les fonds d'investissement et structurels européens, seront également essentiels pour soutenir le déploiement futur des réseaux 5G, notamment en reliant les communautés aux services fondés sur la 5G, tels que les écoles, les hôpitaux, les villes et les administrations locales.

[4] http://www.5GObservatory.eu

[5] http://www.5GObservatory.eu

[6] Certaines des nouvelles fonctionnalités de la 5G seront introduites de manière échelonnée. Lors de la première étape du déploiement, (à court ou très court terme), les réseaux 5G seront principalement des réseaux non autonomes pour lesquels seul le réseau d'accès radio sera en technologie 5G. Les autres fonctionnalités de réseau continueront à reposer sur les cœurs de réseaux 4G existants, qui offriront aux utilisateurs finaux des performances accrues en matière de haut débit mobile. Au cours des étapes suivantes (court/moyen terme jusqu'à long terme), le déploiement de réseaux 5G autonomes, y compris les fonctions de cœur de réseau 5G, nécessitera et entraînera, à terme, une modification beaucoup plus importante de l'architecture du réseau.

[7] Directive (UE) 2018/1972 du Parlement européen et du Conseil établissant le code des communications électroniques européen (refonte).

[8] Proposition de règlement du Parlement européen et du Conseil du 6 juin 2018 établissant le mécanisme pour l'interconnexion en Europe et abrogeant les règlements (UE) nº 1316/2013 et (UE) nº 283/2014; [COM(2018) 438]

Compte tenu des possibilités stratégiques qui s'offrent à l'Europe dans le domaine des services 5G dans divers secteurs, il est primordial que les opérateurs et les fournisseurs de services investissent dans des solutions avancées en matière de réseaux et de services 5G. Celles-ci nécessiteront non seulement de nouveaux réseaux radio 5G, mais aussi de nouveaux cœurs de réseaux 5G dits «autonomes», afin de fournir des fonctionnalités avancées de la 5G, telles que le découpage en tranches de réseau[9] et le traitement des données à la périphérie[10].

La Commission continuera de soutenir pleinement le déploiement de la 5G dans l'UE, notamment en collaborant avec les États membres et les parties prenantes pour saisir les possibilités offertes par la 5G Les aspects sanitaires pertinents seront dûment pris en compte, sur la base du principe de précaution[11], en coopération avec les organisations internationales concernées et la communauté scientifique.

3. Évaluation coordonnée au niveau de l'UE des risques liés à la cybersécurité des réseaux 5G

Tous les États membres, réunis au sein du groupe de coopération SRI[12], ont mené à bien leur propre évaluation nationale des risques liés à leurs infrastructures de réseau 5G et ont transmis les résultats à la Commission et à l'ENISA, l'Agence de l'Union européenne pour la cybersécurité, au début du mois de juillet 2019.

Sur la base de ces évaluations nationales des risques, le groupe de coopération SRI, composé de représentants des États membres, de la Commission et de l'ENISA, a publié le 9 octobre 2019 un rapport sur l'évaluation coordonnée au niveau de l'UE des risques liés à la cybersécurité des réseaux 5G[13]. Ce rapport inventorie les principales menaces et acteurs malveillants, les actifs les plus sensibles et les principales vulnérabilités (techniques et autres) concernant les réseaux 5G. Il recense aussi un certain nombre de catégories de risques revêtant une importance stratégique du point de vue de l'UE, illustrées par des scénarios de risque concrets, correspondant à des combinaisons pertinentes des différents paramètres (vulnérabilités, menaces et acteurs de la menace) pour les différents actifs (voir appendice).

En complément de ce rapport et à titre de contribution supplémentaire à la boîte à outils, l'ENISA a réalisé un inventaire complet des menaces[14], consistant en une analyse détaillée de certains aspects techniques, et recensant notamment les actifs de réseau et les menaces auxquelles ceux-ci sont exposés.

L'évaluation coordonnée des risques au niveau de l'UE met en lumière un certain nombre d'aspects importants pour les réseaux 5G. Plus précisément:

---

[9] Le découpage en tranches d'un réseau 5G permet un degré élevé de séparation entre différentes couches de service sur le même réseau physique, ce qui accroît les possibilités d'offrir des services différenciés sur l'ensemble du réseau.

[10] Le traitement des données à la périphérie est une forme d'architecture distribuée consistant à rapprocher les opérations de traitement et de stockage de l'information de l'endroit où elles sont nécessaires afin d'améliorer les temps de réponse et d'économiser de la bande passante.

[11] Recommandation 1999/519/CE du Conseil du 12 juillet 1999 relative à la limitation de l'exposition du public aux champs électromagnétiques (de 0 Hz à 300 GHz)

[12] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union. Le groupe de coopération SRI a été créé par la directive SRI pour assurer la coopération stratégique et l'échange d'informations entre les États membres de l'UE dans le domaine de la cybersécurité.

[13] https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

[14] ENISA Threat landscape for 5G networks: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

a) Les changements technologiques introduits par la 5G vont accroître la surface d'attaque globale et le nombre de points d'entrée potentiels pour les assaillants:

- du fait de l'amélioration de la fonctionnalité en périphérie de réseau et du caractère moins centralisé de l'architecture par rapport aux générations précédentes de réseaux mobiles, certaines fonctions des cœurs de réseaux peuvent être intégrées dans d'autres parties des réseaux, ce qui rend les équipements correspondants plus vulnérables (par exemple les stations de base ou les fonctions MANO);

- la part croissante du logiciel dans les équipements 5G entraîne une augmentation des risques liés aux processus de développement et de mise à jour des logiciels, crée de nouveaux risques d'erreurs de configuration et confère un rôle plus important dans l'analyse de sécurité aux choix effectués par chaque opérateur de réseau mobile durant la phase de déploiement du réseau.

b) Ces nouvelles caractéristiques technologiques donneront davantage de poids à la dépendance des opérateurs de réseau mobile à l'égard de fournisseurs tiers et au rôle de ces derniers dans la chaîne d'approvisionnement 5G.

Cela aura pour conséquence d'accroître le nombre de chemins d'attaque qui pourraient être exploités par des acteurs malveillants, en particulier des acteurs étatiques ou soutenus par un État extérieurs à l'UE, ayant les capacités (intention et ressources) de mener des attaques contre les réseaux de télécommunications des États membres de l'UE, ainsi que la gravité potentielle des conséquences de ces attaques.

Dans ce contexte d'exposition accrue aux attaques facilitées par des fournisseurs tiers, le profil de risque individuel des fournisseurs revêtira une importance bien particulière, notamment lorsqu'un fournisseur a une présence significative sur certains réseaux ou dans certaines zones.

c) Une forte dépendance à l'égard d'un seul fournisseur augmente la vulnérabilité à une éventuelle défaillance de ce fournisseur et l'ampleur des conséquences de cette dernière. Elle aggrave également les conséquences potentielles des faiblesses ou vulnérabilités et de leur exploitation possible par des acteurs malveillants, en particulier lorsque la dépendance concerne un fournisseur qui présente un niveau de risque élevé.

d) Si certains des nouveaux cas d'utilisation prévus pour la 5G se concrétisent, les réseaux 5G finiront par représenter une part importante de la chaîne d'approvisionnement de nombreuses applications informatiques critiques, et dans ce cas, les incidences ne se limiteront pas aux exigences en matière de confidentialité et de protection de la vie privée, mais l'intégrité et la disponibilité de ces réseaux deviendront aussi des préoccupations majeures de sécurité nationale et constitueront un défi majeur de sécurité pour l'UE.

Source: Évaluation coordonnée des risques au niveau de l'UE

Le rapport sur l'évaluation coordonnée des risques au niveau de l'UE conclut en outre que tous ces défis créent un nouveau paradigme de sécurité qui impose de réévaluer le cadre actuel d'action et de sécurité applicable au secteur de la 5G et à son écosystème, et fait de l'adoption de mesures d'atténuation une nécessité impérative pour les États membres.

Pour remédier efficacement aux risques recensés et renforcer la sécurité et la résilience des réseaux 5G, il convient d'adopter une approche globale, ce qui suppose de mettre en place un ensemble de mesures clés accompagnées d'actions de soutien ayant la même finalité. L'évaluation coordonnée a servi de base pour définir des mesures d'atténuation pouvant être appliquées aux niveaux national et européen.

Dans ses conclusions du 3 décembre 2019, le Conseil a soutenu les conclusions de l'évaluation coordonnée des risques et a souligné l'importance d'une approche coordonnée et d'une mise en œuvre effective de la recommandation afin d'éviter la fragmentation du marché unique[15]. À cet effet, le Conseil a invité les États membres, la Commission et l'ENISA à prendre toutes les mesures nécessaires, dans le cadre de leurs compétences, pour assurer la sécurité et l'intégrité des réseaux de communications électroniques, en particulier les réseaux 5G, et à continuer de consolider une approche coordonnée pour s'attaquer aux défis en matière de sécurité liés aux technologies 5G.

4. Boîte à outils de l'UE pour la cybersécurité 5G

Le 29 janvier 2020, le groupe de coopération SRI a présenté la boîte à outils de l'UE, une panoplie de mesures destinées à atténuer les risques[16]. Elle apporte une réponse à tous les risques recensés dans le rapport d'évaluation coordonnée des risques.

La boîte à outils de l'UE inventorie et décrit un ensemble de mesures stratégiques et techniques assorties de mesures de soutien destinées à renforcer leur efficacité, qui peuvent être mises en place afin d'atténuer les risques recensés. Les **mesures stratégiques** comprennent des mesures relatives au renforcement des pouvoirs réglementaires des autorités en matière d'examen des procédures de marché et de déploiement liés aux réseaux, des mesures spécifiques pour pallier les risques relatifs aux vulnérabilités non techniques, ainsi que des initiatives envisageables pour promouvoir une chaîne d'approvisionnement et de valeur durable et diversifiée dans le domaine de la 5G, en vue d'éviter des risques systémiques de dépendance à long terme. Les **mesures techniques** comprennent des mesures visant à renforcer la sécurité des réseaux et équipements 5G en s'attaquant aux risques liés aux technologies, aux processus, et aux facteurs humains et physiques. En outre, pour chacun des domaines de risque recensés dans l'évaluation coordonnée des risques au niveau de l'UE, la boîte à outils prévoit des **plans d'atténuation des risques** fondés sur les mesures dont l'efficacité est maximale.

Parmi celles-ci, les conclusions associées à la boîte à outils de l'UE, approuvées par le groupe de coopération SRI, contiennent des recommandations relatives à la mise en œuvre, par tous les États membres et par la Commission, de l'ensemble de **mesures clés** suivant:

Conclusions associées à la boîte à outils de l'UE

La boîte à outils de l'UE contient une série de mesures et d'actions qui, si elles sont correctement combinées et effectivement mises en œuvre, constituent la base d'une approche coordonnée dans ce domaine. En effet, compte tenu du large éventail de domaines de risque

[15]Conclusions du Conseil sur l'importance de la 5G pour l'économie européenne et sur la nécessité d'atténuer les risques pour la sécurité liés à la 5G. 14517/19, 3 décembre 2019 (en anglais) https://www.consilium.europa.eu/media/41595/st14517-en19.pdf

[16] Cybersécurité des réseaux 5G - Boîte à outils de l'UE: mesures destinées à atténuer les risques, 29 janvier 2020. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

recensés dans l'évaluation coordonnée des risques au niveau de l'UE et de leur diversité, utiliser un seul type de mesure ne sera pas suffisant. Il faudra plutôt avoir recours à une combinaison appropriée d'une série de mesures pour traiter l'ensemble des principaux domaines de risque.

Sur la base de l'évaluation des plans d'atténuation possibles et du recensement des mesures présentant l'efficacité maximale, les recommandations que contient la boîte à outils sont les suivantes:

1. Tous les États membres devraient veiller à ce que des mesures soient prises (notamment des compétences conférées aux autorités nationales) pour réagir de manière appropriée et proportionnée aux risques actuellement recensés et futurs, et faire en sorte, en particulier, qu'ils soient en mesure d'imposer des restrictions, des interdictions et/ou des exigences ou conditions spécifiques, suivant une approche fondée sur les risques, en ce qui concerne la fourniture, le déploiement et l'exploitation d'équipements de réseau 5G sur la base d'une série de motifs liés à la sécurité.

Ils devraient notamment:

- *renforcer les **exigences de sécurité** pour les opérateurs de réseau mobile (contrôles d'accès stricts, règles concernant la sécurité de l'exploitation et de la surveillance, limitation de l'externalisation de certaines fonctions, etc.);*

- *évaluer les profils de risque des fournisseurs; en conséquence, **appliquer des restrictions pertinentes pour les fournisseurs considérés comme à haut risque - y compris les exclusions nécessaires pour atténuer effectivement les risques - pour les actifs essentiels** définis comme critiques et sensibles dans l'évaluation coordonnée des risques au niveau de l'UE (par exemple, les fonctions de cœur de réseau, les fonctions de gestion et d'orchestration de réseau et les fonctions de réseau d'accès);*

- *veiller à ce que chaque opérateur se dote d'une stratégie multifournisseur appropriée pour **éviter ou limiter toute forte dépendance** à l'égard d'un seul fournisseur (ou de fournisseurs présentant un profil de risque similaire), garantir un équilibre suffisant entre les fournisseurs au niveau national et **éviter la dépendance à l'égard des fournisseurs considérés comme à haut risque**; cela nécessite également d'éviter toute situation d'enfermement propriétaire; notamment en promouvant une interopérabilité accrue des équipements.*

2. La Commission européenne, agissant conjointement avec les États membres, devrait contribuer à:

- *maintenir une **chaîne d'approvisionnement et de valeur durable et diversifiée dans le domaine de la 5G**, en vue d'éviter une dépendance à long terme, notamment:*

  - *en tirant pleinement parti des outils et instruments de l'UE existants, en particulier le filtrage des éventuels **investissements directs étrangers** concernant les actifs clés pour la 5G et en évitant les **distorsions** du marché de l'offre de la 5G dues à d'éventuelles pratiques de dumping ou subventions; et*

  - *en continuant à renforcer les **capacités de l'UE dans les technologies 5G et post-5G** en faisant appel aux programmes et aux financements de l'UE pertinents;*

 faciliter la coordination entre les États membres dans le domaine de ***la normalisation*** *afin d'atteindre des objectifs spécifiques en matière de sécurité et élaborer des* ***systèmes de certification pertinents à l'échelle de l'UE*** *afin de promouvoir des produits et des processus plus sûrs.*

3. Afin de garantir que cette approche coordonnée résiste à l'épreuve du temps, il convient de prolonger le mandat du groupe de travail ad hoc du groupe de coopération SRI, ainsi que la coopération avec les autres organes et entités concernés, afin, notamment:

 de réexaminer périodiquement, avec le soutien de la Commission et de l'ENISA, les ***évaluations des risques au niveau national et au niveau de l'UE*** *concernant la sécurité des réseaux 5G et post-5G, en continuant à développer et à aligner la méthode d'évaluation suivie et en l'adaptant à l'évolution de la technologie 5G;*

 d'assurer un ***suivi et une évaluation détaillés et réguliers de la mise en œuvre*** *de la boîte à outils sur la base de rapports structurés des États membres;*

 de coordonner et soutenir la mise en œuvre des ***actions de soutien*** *qui nécessitent une coopération au niveau de l'UE, notamment en ce qui concerne l'élaboration de lignes directrices et l'échange de bonnes pratiques sur les différentes mesures;*

 de soutenir la poursuite éventuelle de la coordination au niveau de l'UE, le cas échéant, afin, notamment, de renforcer la convergence en ce qui concerne les ***exigences de sécurité technique et organisationnelle applicables aux opérateurs de réseau***.

Source: Boîte à outils de l'UE

Les conclusions associées à la boîte à outils démontrent que les États membres sont déterminés à faire face ensemble aux défis posés par la sécurité des réseaux 5G. Il s'agit d'un point essentiel pour la sécurité au sein des États membres et dans l'ensemble de l'UE, pour les économies nationales ainsi que pour le marché intérieur de l'UE et la souveraineté technologique de l'Europe. Tant l'évaluation coordonnée des risques au niveau de l'UE que la boîte à outils témoignent de la grande qualité des travaux menés conjointement au sein du groupe de coopération SRI, qui ont bénéficié d'une forte collaboration entre les représentants de tous les États membres, la Commission et l'ENISA.

La boîte à outils permet la mise en œuvre d'une approche commune de la cybersécurité des réseaux 5G dans l'UE, favorisant ainsi la cohérence dans l'ensemble du marché intérieur par des politiques et une coordination au niveau de l'UE, ainsi que l'exercice des compétences des États membres, notamment en matière de sécurité nationale. Les mesures et les plans d'atténuation qu'elle prévoit permettent à l'UE d'apporter une réponse appropriée, efficace et proportionnée aux défis communs de la cybersécurité des réseaux 5G.

La Commission salue la publication de la boîte à outils de l'UE sur la cybersécurité des réseaux 5G et souscrit pleinement à l'ensemble des conclusions exposées ci-dessus.

Elle invite les États membres et les institutions, agences et autres organismes concernés de l'Union:

i) à assurer la mise en œuvre rapide de stratégies d'atténuation des risques efficaces et appropriées dans l'ensemble de l'UE conformément aux recommandations figurant dans la boîte à outils de l'UE, et

ii) à prendre toutes les mesures supplémentaires nécessaires pour assurer la coordination au niveau de l'Union, notamment en poursuivant les travaux menés au sein du groupe de coopération SRI et en créant un mécanisme fiable pour suivre la mise en œuvre de la boîte à outils de l'UE, de manière à garantir l'efficacité des mesures et le bon fonctionnement du marché intérieur.

5. Mise en œuvre de la boîte à outils

La détermination des États membres à utiliser pleinement la boîte à outils est une condition essentielle pour assurer une approche européenne crédible et efficace de la sécurité des réseaux 5G. S'il appartiendra aux États membres de décider de la pertinence d'une mesure donnée en fonction des circonstances nationales, il est absolument essentiel qu'un **ensemble de mesures clés soit établi dans chaque État membre, conformément aux recommandations du groupe de coopération SRI (voir plus haut les conclusions associées à la boîte à outils) et, pour certaines de ces mesures, au niveau de l'UE,** afin de parer aux risques constatés.

La Commission reste pleinement disposée à accompagner les prochaines phases des travaux et invite les États membres:

- à prendre, **pour le 30 avril 2020 au plus tard,** des mesures concrètes et quantifiables pour mettre en œuvre l'ensemble de mesures clés selon les recommandations figurant dans les conclusions associées à la boîte à outils de l'UE;

- à élaborer, **pour le 30 juin 2020 au plus tard,** un rapport du groupe de coopération SRI sur l'état d'avancement de la mise en œuvre, dans chaque État membre, de ces mesures clés, en se fondant sur les rapports et le suivi réguliers assurés notamment au sein du groupe de coopération SRI, avec l'aide de la Commission et de l'ENISA.

5.1. Une approche concertée et fondée sur les risques à l'égard des fournisseurs de 5G

Dans la mesure où l'objectif ultime consiste à garantir la sécurité et la résilience des réseaux 5G et leur viabilité, les États membres se sont accordés sur la nécessité d'analyser le profil de risque de chaque fournisseur et, par conséquent, d'appliquer les restrictions qui s'imposent aux fournisseurs considérés comme présentant un risque élevé pour les actifs clés, et notamment les exclusions nécessaires pour atténuer efficacement ces risques, comme il est indiqué dans la boîte à outils. La Commission est disposée à prêter assistance aux États membres pour la mise en œuvre de ces mesures.

Pour soutenir leur mise en œuvre dans l'ensemble de l'UE, l'évaluation coordonnée des risques au niveau de l'UE et la boîte à outils de l'UE fournissent des orientations concernant 1) l'analyse du profil de risque des fournisseurs[17] et 2) la sensibilité des éléments et des fonctions de réseau[18], ainsi que d'autres actifs. Tant l'évaluation coordonnée des risques au

[17] Point 2.37 de l'évaluation coordonnée des risques au niveau de l'UE.

[18] Au point 2.21 de l'évaluation coordonnée des risques au niveau de l'UE sont présentées les principales catégories d'éléments et de fonctions et leur degré global de sensibilité, ainsi qu'une liste des éléments clés recensés par les États membres pour chaque catégorie, tandis qu'aux points 2.28 et 2.29 figurent un certain nombre d'autres types d'actifs ou de secteurs sensibles (par exemple, des entités ou des zones géographiques données).

niveau de l'UE que les mesures prévues par la boîte à outils couvrent les risques liés aux fournisseurs d'équipements et de services de réseau 5G. Elles ne couvrent pas les autres produits ou services que ces fournisseurs, ou d'autres, peuvent fournir.

Comme il est indiqué au point 2.37 de l'évaluation coordonnée des risques au niveau de l'UE, les profils de risque des différents fournisseurs peuvent être évalués sur la base de plusieurs facteurs.

Il convient que ladite évaluation se fonde exclusivement sur des considérations de sécurité et des critères objectifs. Pour favoriser une approche coordonnée de la mise en œuvre de ces mesures, la boîte à outils comprend une recommandation invitant les États membres à échanger des informations sur les approches et meilleures pratiques nationales. La Commission considère au demeurant que cette action devrait figurer parmi les premières priorités de la prochaine phase des travaux menés au sein du groupe de coopération SRI en coopération avec la Commission et l'ENISA.

Il importe que les restrictions imposées aux fournisseurs considérés comme présentant un risque élevé, y compris les exclusions nécessaires pour atténuer efficacement les risques, de même que les mesures visant à éviter la dépendance à l'égard de ces fournisseurs, soient prises en temps utile. Une intervention au stade le plus précoce, y compris, dans la mesure du possible, dans le cadre des procédures d'octroi des licences pour les fréquences 5G, renforcera également la prévisibilité pour les acteurs du marché, contribuant par là même à un déploiement rapide des réseaux 5G, et garantira la sécurité à long terme des réseaux 5G et la résilience de la chaîne d'approvisionnement de la 5G.

Dans le même temps, les calendriers de mise en œuvre de ces mesures peuvent différer au niveau national, si ces différences s'avèrent nécessaires et justifiées, notamment en cas de forte dépendance à l'égard d'équipements ou de services de fournisseurs évalués comme présentant un risque élevé (par exemple, en tenant compte des cycles de mise à niveau des équipements, et notamment du passage des réseaux 5G non autonomes aux réseaux 5G autonomes). Les États membres pourraient envisager d'établir des plans de mise en œuvre prévoyant des périodes de transition appropriées pour les opérateurs de réseau concernés. Dans ce cas, les périodes de transition devraient être définies de manière à préserver, voire à renforcer, les incitations à investir dans des équipements de réseau modernes, notamment en accélérant le déploiement de cœurs de réseau 5G à part entière («autonomes») et en remplaçant les équipements 4G existants dans d'autres parties des réseaux (par exemple, dans le réseau d'accès radio), conformément aux objectifs du plan d'action pour la 5G[19].

Par ailleurs, en raison de la complexité des réseaux 5G logiciels, les opérateurs de télécommunications risquent de recourir de plus en plus souvent à des tiers pour l'exécution de certaines tâches, comme la maintenance et la mise à niveau des réseaux et des logiciels 5G, ainsi que d'autres services externalisés, en plus de la fourniture des équipements de réseau. Ainsi qu'il est précisé dans l'évaluation coordonnée des risques au niveau de l'UE, il s'agit là d'une source de risques sérieux pour la sécurité qui demande, dès lors, une vigilance particulière. Il est indispensable de procéder également à une analyse de sécurité approfondie du profil de risque des fournisseurs chargés de ces services, en particulier lorsque les tâches en question ne sont pas réalisées dans l'UE. Des mesures appropriées s'imposent, telles que l'application de restrictions, en particulier dans les parties sensibles des réseaux 5G, ou la

[19] COM(2016) 588 du 14 septembre 2016, «Un plan d'action pour la 5G en Europe».

nécessaire exclusion des entités à haut risque conformément aux mesures d'atténuation prévues par la boîte à outils, afin de préserver l'intégrité à long terme de l'infrastructure 5G.

5.2. Le rôle de la Commission pour accompagner la mise en œuvre de la boîte à outils

La Commission continuera d'accompagner la mise en œuvre de l'approche de l'UE en matière de cybersécurité des réseaux 5G en général, tout en prenant des initiatives ponctuelles en rapport avec les mesures et les objectifs prévus par la boîte à outils lorsqu'elles peuvent apporter une valeur ajoutée. Elle fera pleinement usage de ses compétences et des instruments appropriés, en tant que de besoin, pour répondre aux questions de sécurité qui se posent. De cette manière, et en unissant ses forces avec les États membres et le secteur privé, la Commission entend favoriser les mesures stratégiques contribuant à garantir la souveraineté et l'avance technologiques de l'UE dans le développement futur des technologies de réseau, les technologies de cybersécurité et toutes les composantes dont dépendent généralement notre économie et notre sécurité.

En pratique, la Commission se chargera des tâches suivantes pour garantir la mise en œuvre des mesures d'atténuation correspondantes que prévoit la boîte à outils dans les domaines relevant de sa compétence:

Préservation de la cybersécurité des réseaux 5G et d'une chaîne de valeur diversifiée pour la 5G

-**Coopération en matière de cybersécurité**: continuer de prêter assistance aux États membres pour la mise en œuvre efficace, coordonnée et rapide des mesures nationales par l'intermédiaire du groupe de coopération SRI.

- **Règles en matière de télécommunications et de cybersécurité**: offrir son assistance pour la mise en œuvre des mesures prévues dans la boîte à outils concernant les exigences de sécurité, eu égard notamment aux dispositions applicables de la réglementation européenne sur les communications électroniques, et réfléchir à la valeur ajoutée d'éventuels actes d'exécution qui définiraient avec précision des mesures de sécurité techniques et organisationnelles complétant les règles nationales et renforçant l'efficacité et la cohérence des mesures de sécurité imposées aux opérateurs.

- **Normalisation**: prendre des mesures contribuant à maintenir et, s'il y a lieu, à renforcer la participation européenne au sein des divers organismes de normalisation afin de réaliser les objectifs de l'Europe en matière de sécurité et d'interopérabilité. La Commission assurera notamment, en coopération avec les États membres, l'analyse et la promotion des spécifications techniques et des normes nécessaires à l'interopérabilité entre les fournisseurs d'équipements 5G dans différentes parties du réseau, y compris dans les réseaux existants, afin de créer les conditions d'un véritable environnement multifournisseur, par exemple par des interfaces ouvertes et interopérables.

- **Certification**: soutenir la mise au point de mécanismes de certification 5G répondant aux besoins des réseaux 5G au regard du cadre européen de certification en matière de cybersécurité.

- **Filtrage des investissements directs étrangers (IDE)**: soutenir la mise en œuvre du cadre de l'UE pour le filtrage des IDE en cartographiant la chaîne de valeur de la 5G, y compris les actifs de réseau sensibles, et en assurant un suivi régulier des IDE tout au long de la chaîne de

valeur. Conformément au calendrier prévu pour le filtrage des IDE (à partir d'octobre 2020), la Commission contrôlera les investissements étrangers dans le domaine de la 5G conformément aux lignes directrices du règlement (UE) 2019/452, en tenant compte de l'évaluation coordonnée des risques au niveau de l'UE et de la boîte à outils de l'UE.

- **Instruments de défense commerciale**: surveiller toutes les évolutions pertinentes du marché dans l'UE et dans les pays tiers et protéger les acteurs de l'UE sur le marché européen de la 5G par des mesures de défense commerciale contre d'éventuelles pratiques de distorsion des échanges (dumping ou subventions), y compris en lançant, au besoin, des enquêtes préliminaires.

- **Règles de concurrence:** surveiller le fonctionnement des marchés de la fourniture de matériel et de logiciels 5G afin de garantir qu'il se crée une situation concurrentielle, y compris pour prévenir d'éventuels verrouillages contractuels ou technologiques.

- **Programmes de financement de l'UE**: veiller à ce que la participation aux programmes de financement de l'UE dans les domaines technologiques concernés soit subordonnée au respect des exigences de sécurité en utilisant pleinement et en faisant appliquer les conditions de sécurité prévues dans les programmes de R&I, notamment dans Horizon Europe, le programme pour une Europe numérique et le mécanisme pour l'interconnexion en Europe 2, dans les fonds structurels et d'investissement et d'autres programmes pertinents. Une approche similaire devrait également être adoptée dans les programmes et instruments de financement extérieur de l'UE, notamment à l'égard des financements assurés par l'intermédiaire d'institutions financières internationales.

- **Marchés publics:** mettre à profit les marchés publics passés dans le domaine des réseaux 5G pour soutenir les objectifs définis en matière de sécurité, de diversité des fournisseurs et de viabilité à long terme des réseaux 5G; notamment, veiller à ce que les aspects liés à la sécurité soient dûment pris en compte lors de l'attribution de marchés publics en rapport avec les réseaux 5G, conformément aux règles de l'UE régissant les marchés publics.

- **Réaction aux incidents et gestion des crises (plan d'action) et cyberexercices**: mettre pleinement à profit la mise au point du plan d'action de l'UE[20] pour une réaction coordonnée aux incidents et crises de cybersécurité majeurs; de plus, en coopération avec l'ENISA, envisager la réalisation d'un cyberexercice 5G dès que la maturité du marché le permettra.

Et, sous la responsabilité du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité et vice-président de la Commission, ainsi que du Conseil:

- **Cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance (boîte à outils cyberdiplomatique)[21]**: en cas d'actes de cybermalveillance menaçant l'intégrité et la sécurité de l'UE, les États membres sont encouragés à faire usage des mesures pertinentes de politique étrangère et de sécurité commune prévues par la boîte à outils de l'UE en matière de cyberdiplomatie (y compris, le cas échéant, des mesures de restriction) pour encourager la coopération, faciliter l'atténuation des menaces et influencer le comportement des agresseurs potentiels.

[20] Recommandation (UE) 2017/1584 de la Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs.
[21] Conclusions du Conseil du 20 novembre 2017, 9916/17.

De plus, divers programmes contribueront à la réalisation des objectifs consistant à prévenir ou à limiter le risque de dépendance à long terme en promouvant un marché de la 5G diversifié et durable, notamment en maintenant les capacités de l'UE dans la chaîne de valeur de la 5G et en investissant dans l'innovation, conformément aux obligations internationales de l'UE.

Promouvoir l'innovation et investir dans la cybersécurité et les technologies pour les infrastructures de réseau:

- **Programmes** de financement de l'UE: accroître les investissements dans la recherche, l'innovation et le déploiement des technologies de réseau et des éléments qui les composent. La Commission a proposé de prévoir près de 3 milliards d'euros d'investissements dans les technologies de cybersécurité au titre du prochain budget de l'UE pour la période 2021-2027. Cette enveloppe comprend la recherche et l'innovation dans le cadre du programme Horizon Europe et l'appui aux capacités de cybersécurité dans le cadre du programme pour une Europe numérique. InvestEU peut également fournir un appui financier à la recherche et au développement dans le domaine de la 5G et soutenir son déploiement.

Par ailleurs, dans le cadre du prochain programme Horizon Europe[22], la Commission a proposé la création d'un partenariat institutionnalisé de l'UE sur l'internet de nouvelle génération et la 6G («Réseaux et services intelligents»), en partenariat avec le secteur privé et en coordination avec les États membres, pour achever le déploiement de la 5G et principalement **pour préparer la 6G**, c'est-à-dire la prochaine génération de technologies mobiles. Plus de 2,5 milliards d'euros d'investissements de l'UE ont été proposés au titre du budget de l'UE (2021-2027), auxquels devraient répondre au moins 7,5 milliards d'euros d'investissements privés dans cette initiative.

- Développement et déploiement industriels: évaluer les lacunes ou défaillances potentielles du marché tout au long de la chaîne de valeur de la 5G qui justifieraient des interventions ciblées dans le cadre du prochain budget à long terme ou d'un éventuel PIIEC (projet important d'intérêt européen commun) en matière de cybersécurité, conformément aux propositions du forum de haut niveau sur les PIIEC. La décision de concevoir et de créer des PIIEC appartient aux États membres et aux entreprises. Les règles de l'UE permettent de les encadrer et la Commission est disposée à faciliter les contacts nécessaires et à fournir des orientations.

[22] Un financement peut également être assuré dans le cadre du MIE 2.0 et du programme pour une Europe numérique.

6. Conclusion

Les réseaux 5G sont porteurs de grandes perspectives pour les Européens, ainsi que pour la société et l'économie européennes. À ce titre, il est essentiel de garantir la sécurité et la résilience des réseaux 5G. Dans le même temps, les menaces qui pèsent sur la cybersécurité (parmi lesquelles le risque d'ingérence d'acteurs étatiques ou soutenus par un État extérieurs à l'UE) sont un défi en constante évolution, dont le poids va croissant à mesure que s'accroît la dépendance à l'égard des technologies et des données. Négliger la cybersécurité nuirait à la confiance placée dans le développement de l'économie et de la société numériques et empêcherait l'UE d'en tirer pleinement profit. Ce défi appelle une réaction elle aussi évolutive et renforcée.

Pour que l'UE puisse assurer sa souveraineté technologique par le maintien et le développement de capacités industrielles, il est essentiel qu'elle se dote d'une approche coordonnée et cohérente de la cybersécurité en ce qui concerne les technologies et les réseaux critiques. La Commission soutiendra pleinement la mise en œuvre de l'approche de l'UE en matière de cybersécurité des réseaux 5G tout en veillant à ce que les marchés de l'UE restent ouverts aux produits et aux services qui respectent les exigences de cybersécurité et de confiance en constante évolution.

À cette fin, il importe que toutes les parties prenantes restent mobilisées pour la sécurité des réseaux 5G, un engagement qui demandera une collaboration suivie entre les États membres, la Commission et l'ENISA.

Dans l'immédiat, comme il est expliqué plus haut, la Commission invite les États à mettre rapidement en œuvre de manière efficace et objective les mesures adoptées dans le cadre de la boîte à outils et à poursuivre leur coopération, avec l'appui de la Commission et de l'ENISA, pour assurer la coordination au niveau de l'UE. En parallèle, la Commission lancera toutes les actions pertinentes relevant de sa compétence pour soutenir la mise en œuvre de la boîte à outils par les États membres et renforcer son impact.

Appendice: Catégories de risque (source: évaluation coordonnée des risques au niveau de l'UE).

	Catégories de risque
Scénarios de risque liés à des mesures de sécurité insuffisantes	*R1: Mauvaise configuration des réseaux*
	R2: Insuffisance des contrôles d'accès
Scénarios de risque liés à la chaîne d'approvisionnement de la 5G	*R3: Faible qualité des produits*
	R4: Dépendance à l'égard d'un seul fournisseur au sein de certains réseaux ou manque de diversité au niveau national:
Scénarios de risque liés au modus operandi des principaux auteurs d'actes malveillants	*R5: Ingérence de l'État dans la chaîne d'approvisionnement de la 5G*
	R6: Exploitation des réseaux 5G par la criminalité organisée ou groupe criminel organisé visant des utilisateurs finaux
Scénarios de risque liés aux interdépendances entre les réseaux 5G et d'autres systèmes critiques	*R7: Perturbation importante d'infrastructures ou de services critiques*
	R8: Défaillance massive des réseaux en raison d'une interruption de l'alimentation électrique ou d'autres systèmes d'appoint
Scénarios de risque liés aux équipements des utilisateurs finaux	*R9: Exploitation de l'internet des objets*