Des réseaux 5G sûrs: Questions-réponses sur la boîte à outils de l'UE

Bruxelles, le 29 janvier 2020

Pourquoi la cybersécurité des réseaux 5G est-elle importante?

Le 5G, catalyseur majeur des futurs services numériques, jouera un rôle essentiel dans le développement l'économie et de la société numériques dans les années à venir. Depuis la médecine personnalisée jusqu'à une agriculture de précision en passant par les réseaux énergétiques intelligents et la mobilité connectée, la 5G affectera probablement tous les aspects de la vie des citoyens de l'Union. Dans le même temps, du fait de leur architecture moins centralisée, d'une puissance de calcul intelligente de pointe, de la nécessité de disposer d'un plus grand nombre d'antennes et d'une dépendance accrue envers les logiciels, les réseaux 5G offrent davantage de points d'entrée potentiels pour des assaillants. Il est donc de la plus haute importance de garantir la sécurité des futurs réseaux 5G de l'UE.

Si le déploiement sûr de la 5G incombe pour une large part aux opérateurs et la sécurité nationale est du ressort des États membres, la sécurité des réseaux est une question stratégique pour l'ensemble de l'UE. Une approche coordonnée fondée sur des mesures de sécurité solides au niveau national et à l'échelon de l'UE aidera l'Europe à rester l'une des régions phares pour le déploiement de la 5G.

Qu'est-ce que la «boîte à outils» de la 5G sur la cybersécurité?

L'objectif de la boîte à outils de l'UE pour la cybersécurité de la 5G est de définir une approche européenne coordonnée fondée sur un ensemble commun de mesures visant à atténuer les principaux risques en matière de cybersécurité des réseaux 5G qui ont été recensés dans le rapport sur l'évaluation coordonnée des risques dans l'UE. Elle vise également à donner des orientations pour la sélection et la hiérarchisation des mesures qui devraient faire partie des plans d'atténuation des risques tant au niveau national qu'à l'échelon de l'UE. Le but ultime est de créer un cadre solide et objectif de mesures de sécurité qui garantira un niveau adéquat de cybersécurité des réseaux 5G dans toute l'UE, dans le cadre d'approches coordonnées entre les États membres. L'approche adoptée respecte pleinement l'ouverture du marché unique; elle est fondée sur les risques et uniquement motivée par des raisons de sécurité.

Quelles sont les principales conclusions de la boîte à outils?

La boîte à outils recommande un ensemble d'actions essentielles pour les États membres et/ou la Commission.

Les États membres sont convenus de veiller à ce que les mesures soient mises en place (y compris des pouvoirs appropriés pour les autorités nationales) pour réagir de manière adéquate et proportionnée aux risques déjà répertoriés ainsi qu'aux risques potentiels futurs. En particulier, ils sont convenus de veiller à être à même de restreindre, interdire, conformément à une approche fondée sur les risques, la fourniture, le déploiement et l'exploitation des équipements de réseau 5G, et/ou d'imposer des exigences et conditions spécifiques applicables à ces activités. En particulier, ils devraient:

- **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 pour l'UE (par exemple, les fonctions de réseau de base, les fonctions de gestion et d'orchestration et les fonctions de réseau d'accès);
- veiller à ce que chaque opérateur se dote d'une stratégie multi-fournisseur appropriée pour **éviter ou limiter toute dépendance majeure** 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.

La boîte à outils recommande que la Commission, conjointement avec les États membres, contribue 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:

o en tirant pleinement parti des outils et instruments de l'UE existants, en particulier le filtrage des investissements directs étrangers (IDE) 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

o 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.

Où en est la mise en œuvre de la boîte à outils sur la sécurité de la 5G dans les États membres? *

- Le 24 juillet 2020, les États membres de l'UE, avec le soutien de la Commission et de l'ENISA, l'Agence de l'Union européenne pour la cybersécurité, ont publié un rapport sur les progrès accomplis dans la mise en œuvre de la boîte à outils commune de mesures d'atténuation des risques, qui a été adoptée par les États membres et approuvée par une communication de la Commission en janvier 2020.

- Selon le rapport, des progrès satisfaisants ont déjà été atteints pour certaines des mesures de la boîte à outils, notamment dans les domaines suivants:

O Les **pouvoirs des autorités réglementaires nationales pour réglementer la sécurité 5G** ont été renforcés ou sont sur le point de l'être dans une large majorité d'États membres, y compris en ce qui concerne les pouvoirs de réglementer l'acquisition d'équipements et de services de réseau par les opérateurs.

o Des mesures visant à **restreindre la participation des fournisseurs sur la base de leur profil de risque** sont déjà en place dans quelques États membres et à un stade avancé de préparation dans beaucoup d'autres. Le rapport invite les autres États membres à aller de l'avant et à achever ce processus dans les mois à venir. En ce qui concerne la portée exacte de ces restrictions, le rapport souligne qu'il importe d'examiner le réseau dans son ensemble et d'en aborder les éléments essentiels, ainsi que d'autres éléments critiques et très sensibles, y compris les fonctions de gestion et le réseau d'accès radio, et d'imposer des restrictions concernant d'autres actifs essentiels, comme les zones géographiques définies, le gouvernement ou d'autres entités critiques.

O Les **exigences en matière de sécurité et de résilience des réseaux pour les opérateurs de téléphonie mobile** font l'objet d'un réexamen dans une majorité d'États membres. Le rapport souligne qu'il importe de veiller à ce que ces exigences soient renforcées, qu'elles suivent les pratiques les plus avancées et que leur mise en œuvre par les opérateurs soit effectivement contrôlée.

- D'autre part, certaines mesures sont à un stade moins avancé de mise en œuvre. En particulier, d'après le rapport:

O Des progrès sont nécessaires d'urgence pour atténuer le **risque de dépendance vis-à-vis de fournisseurs à haut risque**, également en vue de réduire les dépendances au niveau de l'Union. Cette démarche devrait se fonder sur un inventaire exhaustif de la chaîne d'approvisionnement des réseaux et suppose un suivi de l'évolution de la situation.

O Des défis ont été recensés dans la **conception et l'imposition de stratégies multifournisseurs appropriées pour les opérateurs individuels ou au niveau national** en raison de difficultés techniques ou opérationnelles (par exemple, le manque d'interopérabilité, la taille du pays, etc.).

o En ce qui concerne le **filtrage des investissements directs étrangers**, il conviendrait de prendre des mesures pour en instaurer sans délai le mécanisme dans les 13 États membres qui n'en ont pas encore, en vue notamment de l'entrée en application, en octobre 2020, du cadre de l'UE pour le filtrage des investissements. Ces mécanismes de filtrage devraient être appliqués aux investissements dont l'évolution risque d'affecter la chaîne de valeur de la 5G, en tenant compte des objectifs de la boîte à outils.

Que devraient faire les autorités nationales pour faire avancer la mise en œuvre de la boîte à outils?*

- **Achever le processus de mise en œuvre** au niveau national, tout en accordant une **attention particulière aux éléments** mis en évidence dans le rapport d'avancement;
- **échanger davantage d'informations sur les défis, les meilleures pratiques et les solutions** pour la mise en œuvre des mesures de la boîte à outils;
- continuer **à suivre et à évaluer la mise en œuvre de la boîte à outils**;
- poursuivre la coopération avec la Commission pour appliquer les mesures de la boîte à outils, notamment dans le domaine de la **normalisation et de la certification**, des instruments de défense commerciale et des règles de la concurrence, afin d'éviter les distorsions du marché de l'offre des réseaux de 5G et
- **investir dans les capacités de l'UE** en matière de technologies 5G et post-5G et garantir que les projets de réseaux de 5G bénéficiant d'un financement public tiennent compte des risques pour la cybersécurité.

Quels sont les différents types de mesures répertoriés dans la boîte à outils?

Pour chacun des neuf domaines de risque recensés dans le rapport sur l'évaluation coordonnée des risques pour l'UE, la boîte à outils contient des plans d'atténuation des risques. Ces plans prévoient des combinaisons possibles de mesures stratégiques.

- Les **mesures stratégiques** répertoriées dans la boîte à outils vont de mesures concernant des pouvoirs réglementaires accrus pour les 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 (par exemple le risque d'ingérence d'acteurs étatiques extérieurs à l'UE ou soutenus par un État), à l'évaluation du profil des fournisseurs et la promotion d'initiatives pour soutenir le développement de fournisseurs durables et diversifiés dans le domaine de la 5G.
- Les **mesures techniques** répertoriées dans la boîte à outils vont du contrôle d'accès strict et de la gestion, exploitation et surveillance sûres des réseaux à l'utilisation de la certification pour les composants et/ou processus des réseaux 5G.
- Les **actions de soutien** englobent les actions dans le domaine des normes 5G visant à renforcer les capacités d'essai et d'audit, améliorer les efforts de coordination en cas d'incident ou veiller à ce que les risques liés à la cybersécurité soient pleinement pris en compte dans les projets 5G financés par l'UE. Ces actions de soutien peuvent permettre, favoriser et renforcer l'efficacité des mesures stratégiques et techniques.

Qu'est-ce qu'un plan d'atténuation des risques?

Pour chacun des neuf domaines de risque recensés dans le rapport sur l'évaluation coordonnée des risques pour l'UE, la boîte à outils contient des plans d'atténuation des risques. Ces plans prévoient des combinaisons possibles de mesures stratégiques et/ou techniques (ainsi que des actions de soutien appropriées) destinées à atténuer un risque en matière de sécurité.

Les mesures contenues dans la boîte à outils sont-elles obligatoires?

La boîte à outils de l'UE pour la cybersécurité 5G est un document élaboré et approuvé par le groupe de coopération SRI, composé de représentants de toutes les autorités nationales, de la Commission et de l'Agence de l'UE pour la cybersécurité. Le développement d'une approche coordonnée de l'UE en matière de cybersécurité pour la 5G s'appuie sur un ferme engagement des États membres et de la Commission à utiliser et à mettre pleinement en œuvre un ensemble essentiel de mesures recommandées. La boîte à outils définit une méthodologie précise et objective pour faire face aux risques répertoriés dans l'évaluation européenne des risques publiée en octobre 2019, tout en respectant les compétences nationales dans ce domaine.

Dans le même temps, le déploiement et l'exploitation des réseaux 5G relèvent de la sécurité nationale. Les États membres peuvent aller au-delà de ce qui est proposé dans la boîte à outils lorsqu'ils en constatent la nécessité.

Comment la boîte à outils de l'UE sera-t-elle mise en œuvre?

Une combinaison appropriée de différents types de mesures est nécessaire pour atténuer efficacement

les risques recensés. En effet, les États membres devront prendre une série de mesures d'atténuation pour faire face efficacement aux risques liés aux réseaux 5G. Les mesures peuvent être mises en œuvre par des actions au niveau national et/ou à l'échelon de l'UE, selon la mesure ou l'action en cause. Certaines mesures peuvent être directement instaurées ou renforcées au niveau national, d'autres peuvent nécessiter une action supplémentaire ou commune à l'échelon de l'UE, de manière compatible avec les compétences respectives des États membres et de l'UE.

La boîte à outils traite-t-elle le risque d'ingérence d'un pays tiers?

La boîte à outils apporte une réponse à tous les risques recensés dans l'évaluation coordonnée des risques pour l'UE, y compris les risques d'ingérence d'un pays tiers par l'intermédiaire de la chaîne d'approvisionnement de la 5G. Elle ne cible aucun fournisseur ni aucun pays en particulier. Afin d'atténuer ce risque particulier, la boîte à outils recommande que tous les États membres prennent les mesures suivantes:

1) évaluer les profils de risque des fournisseurs, notamment selon les critères définis dans l'évaluation coordonnée des risques dans toute l'UE;

2) 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 (par exemple, les fonctions de réseau de base, les fonctions de gestion et d'orchestration et les fonctions de réseau d'accès).

Comment la communication de la Commission complète-t-elle la boîte à outils?

La communication de la Commission approuve la boîte à outils de l'UE et propose une marche à suivre pour avancer dans sa mise en œuvre. En outre, la Commission agira, conformément à la boîte à outils, en recourant, en tant que de besoin, à tous les outils dont elle dispose pour garantir la sécurité de l'infrastructure et de la chaîne d'approvisionnement 5G, notamment:

- la réglementation sur les télécommunications et la cybersécurité, par exemple le soutien au titre des dispositions applicables aux communications électroniques, y compris en envisageant des actes d'exécution relatifs aux mesures de sécurité techniques et organisationnelles;
- la coordination en matière de normalisation, par exemple en ce qui concerne la participation aux organismes de normalisation et la promotion de l'interopérabilité par des interfaces ouvertes;
- la certification à l'échelle de l'UE, au titre du règlement sur la cybersécurité;
- le filtrage des investissements directs étrangers afin de protéger la chaîne d'approvisionnement de la 5G européenne;
- les instruments de défense commerciale: la surveillance du marché et une action visant à protéger les acteurs de l'UE sur le marché de la 5G contre des éventuelles pratiques de distorsion des échanges (dumping ou subventions);
- les règles de concurrence: surveillance du marché afin de garantir des résultats compétitifs, notamment en relation avec d'éventuelles situations d'enfermement propriétaire;
- les marchés publics, en veillant à ce que les aspects liés à la sécurité soient dûment pris en compte lors de l'attribution des marchés publics, ainsi que par l'intermédiaire des programmes de financement de l'UE, et en s'assurant que les bénéficiaires respectent les exigences de sécurité applicables;
- la mise à profit pleine et entière des cadres de réponse aux incidents et de gestion des crises à l'échelon de l'UE, face à des incidents de cybersécurité majeurs;
- des investissements accrus dans la recherche, l'innovation et les technologies du déploiement.

Quels sont les instruments déjà disponibles à l'échelon de l'UE pour protéger les réseaux 5G?

L'UE dispose déjà d'une série d'instruments pour protéger les réseaux de communications électroniques:

Dans le **cadre réglementaire de l'UE applicable aux télécommunications**, des obligations peuvent être imposées aux opérateurs de télécommunications. Les États membres doivent garantir l'intégrité et la sécurité des réseaux de communications publics, et veiller à ce que les réseaux et services de communication publics prennent des mesures techniques et organisationnelles afin de

gérer les risques pour la sécurité. Ce cadre prévoit également que les autorités réglementaires nationales compétentes ont le pouvoir de donner des instructions contraignantes et contrôler leur respect.

Le **code des communications électroniques européen**, qui remplacera le cadre actuel à partir du 21 décembre 2020, maintient et étend les dispositions du cadre actuel en matière de sécurité et établit des définitions relatives à la sécurité des réseaux et services ainsi qu'aux incidents de sécurité. En outre, ce code prévoit que les mesures de sécurité devraient tenir compte de tous les aspects pertinents de certains éléments dans des domaines tels que la sécurité des réseaux et des installations, le traitement des incidents de sécurité, la continuité des activités, la surveillance, l'audit et les essais ainsi que le respect des normes internationales.

La **directive SRI** impose aux opérateurs de services essentiels dans d'autres domaines (énergie, finance, soins de santé, transport, fournisseurs de services numériques, etc.) de prendre les mesures de sécurité appropriées et de notifier les incidents graves à l'autorité nationale compétente. Cette directive prévoit également une coordination entre les États membres en cas d'incidents transfrontières affectant les opérateurs relevant de son champ d'application. Le programme de travail de la Commission adopté aujourd'hui annonce la révision de la directive avant la fin de 2020.

Le **règlement sur la cybersécurité**, entré en vigueur en juin 2019, établit un cadre européen de certification de cybersécurité pour les produits, processus et services. Une fois en place, les systèmes de certification permettront également aux producteurs de démontrer qu'ils ont intégré des éléments de sécurité spécifiques dès les premiers stades de la conception des produits et aux utilisateurs d'obtenir une assurance de sécurité, pour toute l'Union. Ce cadre constitue un outil de soutien essentiel pour promouvoir des niveaux de sécurité cohérents. Il permet la mise en place de systèmes de certification de cybersécurité pour répondre aux besoins des utilisateurs d'équipements et de logiciels liés à la 5G.

En outre, la Commission accompagnera la mise en œuvre de la boîte à outils de l'UE en matière de cybersécurité de la 5G et agira, comme les États membres lui ont demandé, en recourant à tous les outils dont elle dispose pour garantir la sécurité de l'infrastructure et de la chaîne d'approvisionnement 5G, en tant que de besoin (voir la question précédente).

Quelles sont les prochaines étapes?

Comme recommandé par la coopération SRI et encouragé par la communication de la Commission, les travaux se poursuivront au sein du groupe de coopération SRI afin de suivre la mise en œuvre de la boîte à outils et d'en assurer l'application effective et cohérente.

Le groupe favorisera également l'alignement des approches nationales grâce à de nouveaux échanges d'expériences et un travail en collaboration avec l'Organe des régulateurs européens des communications électroniques (ORECE).

Dans le cadre de la mise en œuvre de la recommandation de la Commission adoptée l'année dernière, les États membres, en coopération avec la Commission, devraient évaluer les effets de la recommandation et déterminer s'il est nécessaire de prendre des mesures supplémentaires **avant le 1er octobre 2020**.

Cette évaluation devrait s'appuyer sur les résultats de l'évaluation coordonnée des risques au niveau de l'UE, publiée en octobre 2019, et tenir compte de l'efficacité des mesures de la boîte à outils.

*Mise à jour le 24/07/2020

QANDA/20/127

Personnes de contact pour la presse:
Johannes BAHRKE (+32 2 295 86 15)
Marietta GRAMMENOU (+32 2 298 35 83)

Renseignements au public: Europe Direct par téléphone au 00 800 67 89 10 11 ou par courriel