Questions et réponses – la Commission recommande une approche européenne commune de la sécurité des réseaux 5G

Strasbourg, le 26 mars 2019

.

Pourquoi le déploiement des réseaux 5G est-il crucial pour l'Europe?

Les réseaux de cinquième génération (5G) formeront l'épine dorsale de nos sociétés et de nos économies, reliant des milliards d'objets et systèmes, y compris dans des secteurs critiques comme l'énergie, les transports, les banques et la santé, ainsi que des systèmes de contrôle industriel qui véhiculent des informations sensibles et étayent des dispositifs de sécurité. Les processus démocratiques comme les élections s'appuient de plus en plus sur les infrastructures numériques et les réseaux 5G. Cet état de fait souligne qu'il convient de déceler toute vulnérabilité et rend la recommandation présentée aujourd'hui par la Commission d'autant plus pertinente dans la perspective des élections au Parlement européen de mai.

La 5G est également un atout majeur de la compétitivité de l'Europe sur le marché mondial. Les recettes produites par la 5G dans le monde devraient représenter l'équivalent de 225 milliards d'euros en 2025. Les retombées de l'introduction de la 5G dans quatre secteurs industriels clés, à savoir l'automobile, la santé, les transports et l'énergie, pourraient représenter 114 milliards d'euros par an.

Le déploiement de la 5G relève de la responsabilité des États membres qui, aux côtés des opérateurs, prennent des décisions majeures pour le préparer. Une procédure d'enchères relative à au moins une bande de fréquences est prévue pour 2019 dans 11 États membres: l'Autriche, la Belgique, la Tchéquie, la France, l'Allemagne, la Grèce, la Hongrie, l'Irlande, les Pays-Bas, la Lituanie et le Portugal. Six autres États membres devraient suivre en 2020: l'Espagne, Malte, la Lituanie, la Slovaquie, la Pologne et le Royaume-Uni.

À l'échelle de l'Union, le plan d'action pour la 5G fixe les dates cibles de 2020 pour le lancement commercial dans tous les États membres et de 2025 pour le déploiement complet dans les villes et le long des principaux axes de transport. Selon le dernier rapport de l'observatoire 5G de la Commission, les opérateurs européens sont en concurrence avec d'autres régions du monde à la pointe qui se préparent à un lancement commercial de la 5G cette année. L'Europe est un leader mondial dans les activités d'essai 5G, principalement grâce au partenariat public-privé 5G de la Commission; elle compte 139 essais, principalement dans des secteurs verticaux essentiels, répertoriés dans 23 États membres.

Le code des communications électroniques européen soutiendra le déploiement et l'adoption des réseaux 5G, notamment en ce qui concerne l'assignation des radiofréquences, les incitations à l'investissement et l'établissement de conditions-cadres favorables, tandis que les règles adoptées récemment en matière d'internet ouvert offrent une sécurité juridique en ce qui concerne le déploiement des applications 5G. Du côté du secteur privé, les acteurs du marché planifient leurs investissements dans les infrastructures et mettent en place des partenariats pour que les solutions technologiques passent de la phase d'essai au déploiement commercial.

Pourquoi faut-il évaluer les risques liés aux futurs réseaux 5G?

Une fois déployés, les réseaux 5G constitueront l'épine dorsale d'un large éventail de services essentiels au fonctionnement du marché intérieur et au maintien et à l'exercice de fonctions sociétales et économiques vitales, dans les domaines de l'énergie, des transports, des banques et de la santé, ainsi que des systèmes de contrôle industriel, par exemple. L'organisation de processus démocratiques tels que les élections s'appuiera aussi de plus en plus sur les infrastructures numériques et les réseaux 5G.

Toute vulnérabilité des réseaux 5G pourrait être exploitée pour mettre en péril ces systèmes et infrastructures numériques – ce qui pourrait causer de graves préjudices – ou pour voler ou espionner des données à grande échelle. Le fait que de nombreux services critiques dépendent des réseaux 5G rendrait particulièrement graves les conséquences de perturbations systémiques et étendues. Dès lors, une approche solide fondée sur les risques s'avère nécessaire, plutôt qu'une approche reposant

essentiellement sur des mesures d'atténuation ex post.

Les États membres ont fait part de leurs préoccupations concernant les risques potentiels pour la sécurité liés aux réseaux 5G et ont étudié ou pris des mesures pour faire face à ces risques; ils ont également affirmé, dans les conclusions du Conseil européen du 22 mars 2019, qu'ils attendaient avec intérêt une approche concertée au niveau de l'UE.

Pourquoi agir au niveau européen pour sécuriser les réseaux 5G?

Vu le caractère interconnecté et transnational des infrastructures numériques et la nature transfrontière des menaces, toute vulnérabilité dans les réseaux 5G ou toute cyberattaque qui ciblerait les futurs réseaux dans un État membre affecterait l'Union dans son ensemble. C'est pourquoi des mesures concertées prises tant au niveau national qu'au niveau européen doivent garantir un niveau élevé de cybersécurité.

La cybersécurité des réseaux 5G est une question d'importance stratégique pour l'Union, à l'heure où les cyberattaques se multiplient et sont plus sophistiquées que jamais, et où il devient de plus en plus indispensable de protéger les droits de l'homme et les libertés fondamentales en ligne.

Lors de leur réunion du 22 mars 2019, les chefs d'État et de gouvernement de l'UE ont déclaré qu'ils attendaient avec intérêt la recommandation de la Commission relative à une approche concertée en matière de sécurité des réseaux 5G. Dans sa résolution sur les menaces pour la sécurité liées à la présence technologique croissante de la Chine dans l'Union, le Parlement européen invite également la Commission et les États membres à prendre des mesures au niveau de l'Union.

De plus, la cybersécurité des réseaux 5G est essentielle pour garantir l'autonomie stratégique de l'Union, comme indiqué dans la communication conjointe intitulée «Les relations UE-Chine – Une vision stratégique». Les investissements étrangers dans des secteurs stratégiques, les acquisitions d'actifs, de technologies et d'infrastructures critiques dans l'UE, la participation à l'élaboration de normes de l'UE et la fourniture d'équipements critiques peuvent présenter des risques pour la sécurité de l'UE. Cela vaut en particulier pour les infrastructures critiques telles que les réseaux 5G, qui seront essentiels pour notre avenir et doivent être totalement sécurisés.

Comment la coordination de l'UE se déroulera-t-elle? Quelles sont les étapes à franchir?

1. Au niveau national

Chaque État membre devrait procéder à une évaluation nationale des risques liés aux infrastructures des réseaux 5G d'ici à la fin du mois de juin 2019. Sur cette base, les États membres devraient actualiser les exigences de sécurité existantes pour les fournisseurs de réseaux et les assortir de conditions garantissant la sécurité des réseaux publics, en particulier lorsqu'ils octroient des droits d'utilisation dans les bandes de fréquences destinées à la 5G. Parmi ces mesures devrait figurer l'obligation renforcée, pour les fournisseurs et les opérateurs, de garantir la sécurité des réseaux. Les évaluations des risques et les mesures nationales devraient tenir compte de différents facteurs, tels que les risques techniques et les risques liés au comportement des fournisseurs ou des opérateurs, y compris ceux de pays tiers. Les évaluations nationales des risques joueront un rôle central dans la mise en place d'une évaluation coordonnée des risques au niveau de l'UE.

Les États membres de l'UE ont le droit d'exclure de leurs marchés, pour des raisons de sécurité nationale, des entreprises qui ne respectent pas leurs normes et leur législation.

2. Au niveau de l'UE

Les États membres devraient échanger des informations entre eux et, avec le soutien de la Commission et de l'Agence de l'Union européenne pour la cybersécurité (ENISA), ils procéderont à une évaluation coordonnée des risques au plus tard le 1er octobre 2019. Sur cette base, les États membres s'accorderont sur un ensemble de mesures d'atténuation pouvant être prises au niveau national. Ces mesures d'atténuation peuvent inclure des exigences de certification, des essais, des contrôles, ainsi que le recensement des produits ou fournisseurs jugés potentiellement non sûrs. Ces travaux seront menés par le groupe de coopération des autorités compétentes, institué par la directive sur la sécurité des réseaux et des systèmes d'information, avec l'aide de la Commission et de l'ENISA. Ils devraient étayer l'action des États membres au niveau national et fournir des orientations à la Commission en vue d'éventuelles mesures supplémentaires au niveau de l'UE. En outre, les États membres devraient établir des exigences de sécurité spécifiques qui pourraient s'appliquer dans le cadre des marchés publics liés aux réseaux 5G, et notamment des exigences obligatoires concernant la mise en œuvre de

systèmes de certification de cybersécurité.

La recommandation présentée aujourd'hui s'appuiera sur une **vaste panoplie d'instruments** déjà en place ou adoptés en vue de renforcer la coopération contre les cyberattaques et de donner à l'UE les moyens d'agir collectivement pour protéger l'économie et la société européennes: on citera, notamment, la première législation européenne en matière de cybersécurité, la directive sur la sécurité des réseaux et des systèmes d'information (directive SRI), le règlement sur la cybersécurité approuvé récemment par le Parlement européen et la nouvelle réglementation en matière de télécommunications.

La recommandation aidera aussi les États membres à mettre en œuvre ces nouveaux instruments de manière cohérente en ce qui concerne la sécurité des communications 5G.

Quelles dispositions de l'UE sont déjà en place ou en cours de mise en œuvre pour protéger les futurs réseaux 5G?

L'UE dispose d'une **série d'instruments** pour protéger les réseaux de communications électroniques, notamment la première législation européenne en matière de cybersécurité (directive sur la sécurité des réseaux et des systèmes d'information), le règlement sur la cybersécurité approuvé récemment par le Parlement européen et la nouvelle réglementation en matière de télécommunications.

De plus, les États membres de l'UE peuvent, pour des raisons de sécurité nationale, exclure de leurs marchés des entreprises qui ne respectent pas leurs normes et leur législation.

Règles relatives aux télécommunications: les États membres doivent garantir l'intégrité et la sécurité des réseaux de communications publics, avec l'obligation de veiller à ce que les opérateurs prennent des mesures techniques et organisationnelles pour gérer de manière appropriée d'éventuels risques pesant sur la sécurité des réseaux et des services. Les autorités réglementaires nationales compétentes sont aussi investies de certains pouvoirs, dont celui d'adresser des instructions contraignantes et d'en imposer le respect. En outre, les États membres sont autorisés à assortir l'autorisation générale de conditions relatives à la sécurité des réseaux publics face aux accès non autorisés, afin de protéger la confidentialité des communications.

Outils prévus en matière de cybersécurité: le futur cadre européen de certification de cybersécurité pour les produits, processus et services numériques, que le Parlement européen a approuvé récemment, devrait constituer un instrument d'appui essentiel pour promouvoir des niveaux de sécurité cohérents. Il devrait permettre l'instauration de systèmes de certification de cybersécurité, pour répondre aux besoins des utilisateurs d'équipements et de logiciels liés à la 5G.

Pour favoriser le respect de ces obligations et instruments, l'Union a mis en place un certain nombre d'organes de coopération. L'Agence européenne pour la cybersécurité (ENISA), la Commission, les États membres et les autorités réglementaires nationales ont élaboré, à l'intention de ces dernières, des lignes directrices techniques sur la notification des incidents, les mesures de sécurité ainsi que les menaces et les actifs. Le groupe de coopération institué par la directive sur la sécurité des réseaux et des systèmes d'information réunit les autorités compétentes afin de soutenir et de faciliter la coopération, notamment grâce à la définition d'orientations stratégiques.

Garantir la cybersécurité impose aussi de conserver un niveau suffisant d'autonomie stratégique, en atteignant dans l'UE une masse critique d'investissements dans la cybersécurité et les technologies numériques avancées. La Commission a donc proposé de faire de cet objectif une priorité pour la prochaine période budgétaire de l'UE, notamment dans le cadre de sa proposition de programme pour une Europe numérique, et de créer un nouveau centre européen de compétences en cybersécurité, fonctionnant en réseau, pour la mise en œuvre de projets dans le domaine de la cybersécurité.

Règles relatives aux marchés publics: les règles de l'UE concernant les marchés publics contribuent à une meilleure utilisation de l'argent des contribuables, en garantissant l'attribution de ces marchés au moyen d'appels d'offres concurrentiels, ouverts, transparents et strictement réglementés.

Les directives de l'UE sur les marchés publics ne font pas de distinction entre les opérateurs économiques de l'UE et ceux de pays tiers, mais elles comportent un certain nombre de garde-fous. Elles permettent par exemple aux pouvoirs adjudicateurs de refuser, dans certaines conditions, des offres anormalement basses ou non conformes aux normes de sécurité, de travail ou d'environnement. Elles leur permettent aussi de protéger leurs intérêts essentiels en matière de sécurité et de défense.

Règles relatives au filtrage des investissements directs étrangers: le nouveau règlement entrera en vigueur en avril 2019 et s'appliquera pleinement à partir de novembre 2020. Il constituera un puissant instrument de détection des investissements étrangers dans des actifs, technologies et infrastructures critiques et de sensibilisation à ce sujet. Il permettra aussi d'identifier et de contrer collectivement les menaces pour la sécurité et l'ordre public liées aux acquisitions dans des secteurs

sensibles. Les États membres devraient mettre à profit la période entre l'entrée en vigueur et le début de l'application du règlement pour apporter les modifications nécessaires à leur législation et à leurs pratiques nationales et mettre en place des structures administratives garantissant au niveau de l'UE une coopération efficace avec la Commission, conformément aux mécanismes existants.

Régime de sanctions horizontales pour contrer les cyberattaques: ce nouveau régime, proposé par la Commission et la haute représentante, aura une portée mondiale et permettra à l'UE de réagir avec souplesse, quel que soit le lieu à partir duquel les cyberattaques sont lancées et indépendamment du fait qu'elles soient l'œuvre d'acteurs étatiques ou non étatiques. Ce régime de sanctions, une fois adopté, permettrait à l'Union de réagir aux cyberattaques ayant un «effet important», qui menacent l'intégrité et la sécurité de l'UE, de ses États membres et de leurs citoyens.

Quel est le rôle de l'Agence européenne pour la cybersécurité dans cette coordination?

Le règlement sur la cybersécurité approuvé récemment par le Parlement européen confère un mandat renforcé et permanent à l'agence européenne pour la cybersécurité (Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information, ou ENISA).

L'ENISA apporte déjà son soutien à la Commission en ce qui concerne la sécurité des réseaux de télécommunications. En coopération avec les États membres et les autorités réglementaires nationales, elle a défini, à l'intention de ces dernières, des lignes directrices techniques sur la notification des incidents, les mesures de sécurité ainsi que les menaces et les actifs.

En outre, la recommandation invite l'ENISA à contribuer à la mise au point d'une évaluation coordonnée, au niveau de l'UE, des risques liés aux réseaux 5G.

L'ENISA s'emploiera aussi à élaborer des systèmes de certification paneuropéens, comme le prévoit le règlement sur la cybersécurité.

Quelles sont les prochaines étapes?

- Les États membres devraient mener à bien leur évaluation nationale des risques pour le **30 juin 2019** au plus tard, et actualiser les mesures de sécurité nécessaires. L'évaluation nationale des risques devrait être transmise à la Commission et à l'Agence de l'Union européenne pour la cybersécurité au plus tard le **15 juillet 2019**.
- Parallèlement, les États membres et la Commission entameront des travaux de coordination au sein du groupe de coopération institué par la directive sur la sécurité des réseaux et des systèmes d'information. L'ENISA dressera un inventaire complet des menaces propres aux réseaux 5G qui aidera les États membres à mettre en œuvre, pour le **1er octobre 2019** au plus tard, l'évaluation des risques à l'échelle de l'UE.
- D'ici au **31 décembre 2019**, le groupe de coopération devrait convenir d'une «boîte à outils» de mesures d'atténuation pouvant être prises pour parer aux risques de cybersécurité recensés au niveau national et européen.
- Lorsque le règlement sur la cybersécurité récemment approuvé par le Parlement européen sera entré en vigueur, dans les prochaines semaines, la Commission et l'ENISA prendront toutes les mesures nécessaires pour mettre en place le cadre de certification européen. Les États membres sont encouragés à coopérer avec la Commission et l'ENISA afin de donner la priorité à un système de certification couvrant les réseaux et les équipements 5G.
- D'ici le **1er octobre 2020**, les États membres, en coopération avec la Commission, devraient évaluer les effets de la recommandation en vue de déterminer si des mesures supplémentaires s'imposent. Cette évaluation devrait tenir compte du résultat de l'évaluation coordonnée des risques au niveau européen et de l'efficacité des mesures.

Pour en savoir plus

Recommandation sur la cybersécurité des réseaux 5G

Communiqué de presse

Union de la sécurité: 15 initiatives législatives sur 22 approuvées à ce jour

Communiqué de presse: Les négociateurs de l'Union européenne décident de renforcer la cybersécurité en Europe

Plan d'action pour la 5G

Communiqué de presse: Communication conjointe sur les relations UE-Chine – Une vision stratégique

MEMO/19/1833

Personnes de contact pour la presse:

Nathalie VANDYSTADT (+32 2 296 70 83)
Marietta GRAMMENOU (+32 2 298 35 83)

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