



Bruxelles, le 3 décembre 2019
(OR. en)

14517/19

TELECOM 372
CYBER 323
COMPET 769
MI 815
CONSOM 320

RÉSULTATS DES TRAVAUX

Origine:	Secrétariat général du Conseil
en date du:	3 décembre 2019
Destinataire:	délégations
Objet:	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 - Conclusions du Conseil (3 décembre 2019)

Les délégations trouveront en annexe les 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, adoptées par le Conseil "Transports, télécommunications et énergie" lors de sa session du 3 décembre 2019.

**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**

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le potentiel des réseaux 5G pour l'économie européenne, le marché unique de l'UE et les citoyens européens,

1. RECONNAÎT que la 5G est une évolution des réseaux 4G et que la 5G augmentera le potentiel en matière de fourniture de services du réseau mobile [...] et favorisera, dans le même temps, des modèles d'entreprise et des services publics innovants dans de multiples secteurs, tout en offrant d'autres possibilités aux citoyens européens, aux opérateurs de télécommunications, aux entreprises, y compris les PME, au secteur public ainsi qu'à d'autres parties prenantes.
2. RAPPELLE que l'Union a élaboré un cadre juridique pour traiter et atténuer les risques liés à la 5G en matière de cybersécurité, notamment la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen (CCEE) et la 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 (directive SRI).
3. ADMET la nécessité d'atteindre les objectifs ambitieux du plan d'action pour la 5G adopté par la Commission en 2016 et de la déclaration ministérielle de Tallinn sur la 5G, ainsi que de la feuille de route correspondante approuvée par les États membres en 2017 sur la base des objectifs de la société du gigabit.

4. SOULIGNE que les réseaux 5G prendront place parmi les infrastructures essentielles pour l'exercice et le maintien de fonctions sociétales et économiques vitales et feront partie d'un large éventail de services essentiels au fonctionnement du marché intérieur, y compris sa transformation numérique et, à cet égard, INSISTE sur l'importance de la souveraineté technologique européenne et de la promotion, à l'échelle mondiale, de l'approche de l'UE en matière de cybersécurité des réseaux de communications électroniques de demain.
5. MET EN ÉVIDENCE la nécessité d'assurer le déploiement, rapide et fondée sur la demande, des réseaux 5G et de veiller à ce que la 5G constitue un atout essentiel pour la compétitivité et la durabilité européennes, ainsi qu'un catalyseur majeur des futurs services numériques et une priorité dans le cadre du marché unique européen. Dans ce contexte, le Conseil FAIT RESSORTIR également l'importance de la coopération des États membres pour l'adoption des réseaux 5G dans les zones transfrontalières qui les séparent.
6. RECONNAÎT la nécessité de sensibiliser le public aux possibilités offertes par la 5G et d'accroître les compétences parmi les développeurs et au sein de différentes organisations d'utilisateurs, et de veiller à ce que le secteur public ait un rôle à jouer pour encourager l'adoption de la 5G, en montrant l'exemple, et incite toutes les parties prenantes concernées à pratiquer le partage d'informations et d'expériences en vue de soutenir un déploiement réussi de la 5G, y compris en ce qui concerne les questions relatives aux mesures de valeurs limites en matière de champs électromagnétiques.
7. ENCOURAGE la Commission et les États membres à prendre les mesures nécessaires pour faire de l'UE un marché de premier plan pour le déploiement des réseaux 5G et le développement de solutions fondées sur la 5G qui favorisent la croissance et l'innovation, améliorent la vie quotidienne des citoyens et des entreprises, ouvrent la voie à de nouveaux services et à de nouvelles applications, tout en offrant davantage de possibilités à l'ensemble de la société dans des secteurs et industries essentiels tels que l'énergie, les soins de santé, l'agriculture, la finance et la mobilité,

vu les défis posés par les réseaux 5G,

8. INSISTE sur le fait qu'il importe de préserver la sécurité et la résilience des réseaux et services de communications électroniques, en particulier en ce qui concerne la 5G, en suivant une approche fondée sur les risques.
9. SOULIGNE que si le déploiement des réseaux 5G se traduira par de nouvelles possibilités, les profonds changements que les technologies 5G apporteront aux réseaux, aux appareils et aux applications, ainsi que les préoccupations accrues qui, en ce qui concerne l'intégrité et la disponibilité des réseaux 5G, s'ajouteront aux questions de confidentialité et de respect de la vie privée, font que l'UE et les États membres doivent accorder une attention particulière à la promotion de la cybersécurité de ces réseaux et de tous les services qui dépendent des communications électroniques.
10. SALUE les efforts conjoints déployés au niveau européen pour préserver la sécurité des réseaux 5G en se fondant en particulier sur la recommandation de la Commission sur la cybersécurité des réseaux 5G, et MET L'ACCENT sur l'importance d'une approche coordonnée et d'une mise en œuvre effective de la recommandation afin d'éviter une fragmentation du marché unique.
11. SE FÉLICITE de l'évaluation coordonnée des risques au niveau européen qui a été publiée le 9 octobre 2019 et constitue la première suite donnée à la recommandation.
12. MET EN ÉVIDENCE que les changements technologiques introduits par la 5G augmenteront la surface d'exposition globale et feront qu'une attention particulière devra être accordée aux profils de risque des différents fournisseurs.
13. FAIT RESSORTIR que, outre les risques techniques liés à la cybersécurité des réseaux 5G, des facteurs non techniques, tels que le cadre juridique et politique auquel les fournisseurs peuvent être soumis dans les pays tiers, devraient aussi être pris en considération.

14. RÉAFFIRME qu'il importe que les États membres tiennent compte de la nécessité de diversifier les fournisseurs de manière à éviter de créer une forte dépendance à l'égard d'un fournisseur unique ou à limiter cette dépendance, étant donné qu'une telle situation augmente l'exposition aux conséquences d'une éventuelle défaillance de ce fournisseur.
15. MET EN LUMIÈRE l'importance que revêt l'évaluation des risques liés aux interdépendances entre les réseaux 5G et les autres systèmes et services publics et privés essentiels.

EN CONSÉQUENCE, LE CONSEIL:

16. FAIT RESSORTIR qu'un déploiement rapide et sûr des réseaux 5G est capital pour renforcer la compétitivité de l'Union et nécessite une approche coordonnée au sein de l'UE, sans préjudice des compétences des États membres en matière de déploiement de réseaux et de sécurité nationale.
17. MET EN AVANT que le renforcement de la confiance dans les technologies 5G est fermement ancré dans les valeurs fondamentales de l'UE, telles que les droits de l'homme et les libertés fondamentales, l'État de droit, la protection de la vie privée, des données à caractère personnel et de la propriété intellectuelle, dans l'engagement en faveur de la transparence, de la fiabilité et de l'inclusion de toutes les parties prenantes et de tous les citoyens, ainsi que dans le renforcement de la coopération internationale.
18. SOULIGNE que la complexité croissante, l'interconnexion et l'évolution rapide de la technologie requiert une approche globale et des mesures de sécurité efficaces et proportionnées, centrées sur la sécurité et la protection de la vie privée dès la conception en tant que parties intégrantes de l'infrastructure 5G et des équipements terminaux.
19. MET EN ÉVIDENCE que la 5G et les autres réseaux de communications électroniques connexes doivent être protégés en permanence tout au long de leur cycle de vie afin de couvrir l'ensemble de la chaîne d'approvisionnement et tous les équipements concernés.

20. **INSISTE** sur la nécessité de relever et de limiter les défis potentiels que représente le déploiement de réseaux et de services 5G pour les services répressifs, y compris, par exemple, en ce qui concerne l'interception légale.
21. **RECONNAÎT** la nécessité de mettre en place des normes et mesures de sécurité communes solides, tenant compte des efforts de normalisation internationale pour la 5G, pour tous les fabricants, opérateurs de communications électroniques et fournisseurs de services concernés, et le fait que les composants principaux, notamment ceux qui sont essentiels pour la sécurité nationale, ne pourront provenir que de parties dignes de confiance.
22. **SOUTIENT** les travaux menés actuellement par l'Agence de l'Union européenne pour la cybersécurité (ENISA) en ce qui concerne le cadre européen de certification en matière de cybersécurité établi par le règlement sur la cybersécurité, qui pourraient améliorer le niveau de cybersécurité des produits, services et processus dans le domaine des technologies de l'information et de la communication.
23. **SOULIGNE** que, si la normalisation et la certification peuvent permettre de relever certains défis en matière de sécurité liés aux réseaux 5G, des mesures de sécurité supplémentaires sont nécessaires pour atténuer efficacement les risques.
24. **SE FÉLICITE** que la Commission, en coopération avec les États membres et le secteur privé, prépare actuellement un partenariat stratégique européen relatif aux réseaux et services intelligents dans le cadre du programme Horizon Europe, avec pour but de promouvoir les investissements, de maintenir et de renforcer la compétitivité, ainsi que de renforcer la recherche, l'innovation et le développement de solutions sûres dans le domaine de la 5G et au-delà.
25. **SALUE** la priorité accordée à la cybersécurité dans la proposition de programme pour une Europe numérique en tant que moyen de renforcer les capacités de l'UE en la matière, ainsi que l'initiative prévue dans le cadre de la proposition de mécanisme pour l'interconnexion en Europe en ce qui concerne les corridors transfrontières RTE-T 5G.

26. INVITE les États membres et la Commission à prendre, avec le soutien de l'ENISA, toutes les mesures nécessaires, dans les limites de leurs compétences, pour assurer la sécurité et l'intégrité des réseaux de communications électroniques, en particulier des réseaux 5G, et continuer à consolider une approche coordonnée pour relever les défis en matière de sécurité liés aux technologies 5G, sur la base des travaux menés conjointement sur la "boîte à outils" en matière de sécurité de la 5G afin de définir des méthodes et des outils communs efficaces pour atténuer les risques liés aux réseaux 5G.
-