

Bruxelles, le 24 juin 2022
(OR. en)

10307/22

TELECOM 276
CYBER 225
COMPET 506
MI 483
FIN 699

RÉSULTATS DES TRAVAUX

Origine:	Secrétariat général du Conseil
en date du:	16 juin 2022
Destinataire:	délégations
N° doc. préc.:	9616/22
Objet:	Rapport spécial n° 03/2022 de la Cour des comptes européenne intitulé " <i>Déploiement des réseaux 5G au sein de l'UE: des retards et des questions de sécurité encore sans réponse</i> " - Conclusions du Conseil (16 juin 2022)

Les délégations trouveront en annexe les conclusions du Conseil sur le rapport spécial n° 03/2022 de la Cour des comptes européenne intitulé "Déploiement des réseaux 5G au sein de l'UE: des retards et des questions de sécurité encore sans réponse", adoptées par le Conseil "Emploi, politique sociale, santé et consommateurs" lors de sa 3882^e session, tenue le 16 juin 2022.

CONCLUSIONS DU CONSEIL

**sur le rapport spécial n° 03/2022 de la Cour des comptes européenne
intitulé:**

***"Déploiement des réseaux 5G au sein de l'UE: des retards et des questions de sécurité encore
sans réponse"***

LE CONSEIL DE L'UNION EUROPÉENNE,

RAPPELANT

– ses conclusions visant l'amélioration de l'examen de rapports spéciaux établis par la Cour des comptes dans le cadre de la décharge¹;

1. PREND NOTE du rapport spécial n° 03/2022 de la Cour des comptes européenne intitulé: *"Déploiement des réseaux 5G au sein de l'UE: des retards et des questions de sécurité encore sans réponse"*², qui couvre, dans l'ensemble, la période allant de 2016 à mai 2021;
2. SOULIGNE l'importance stratégique du déploiement rapide de réseaux 5G de haute qualité au sein de l'UE afin de favoriser des modèles d'entreprise et des services publics innovants essentiels au fonctionnement du marché intérieur;
3. SOULIGNE que les retards dans l'attribution des fréquences peuvent être imputables à différentes raisons et que la situation en matière de déploiement de la 5G peut avoir évolué dans certains États membres depuis la collecte et le traitement des données. Par conséquent, SOULIGNE qu'il importe d'utiliser des données vérifiées et qu'il est nécessaire que les conclusions soient fondées sur des critères/une méthodologie clairs;

¹ 7515/00 + COR 1.

² WK 5636/22 INIT.

4. RAPPELLE ses conclusions 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 dans lesquelles il INVITAIT 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 afin de définir des méthodes et des outils communs efficaces pour atténuer les risques liés aux réseaux 5G³;
5. RAPPELLE la forte approche collaborative des États membres et de la Commission qui a conduit à l'adoption de la boîte à outils de l'UE pour la cybersécurité de la 5G⁴, qui fournit un cadre de mesures visant à atténuer les menaces pour la sécurité liées aux réseaux 5G en vue de promouvoir un niveau adéquat de cybersécurité de ces réseaux dans le marché intérieur;
6. SOULIGNE qu'il importe que les États membres parviennent à mettre en œuvre la boîte à outils de l'UE pour la cybersécurité de la 5G, en particulier pour ce qui est d'appliquer les restrictions pertinentes aux fournisseurs à haut risque pour les actifs essentiels définis comme critiques et sensibles dans les évaluations coordonnées des risques au niveau de l'UE⁵;
7. SOULIGNE que la boîte à outils de l'UE pour la cybersécurité de la 5G constitue un instrument souple fondé sur les risques pour relever les défis recensés en matière de sécurité, qui permet de traiter les aspects liés à la cybersécurité de la 5G de manière rapide et efficace, tout en respectant les compétences des États membres et leur responsabilité exclusive en matière de sécurité nationale, conformément à l'article 4, paragraphe 2, du traité sur l'Union européenne, y compris dans le domaine de la cybersécurité;

³ ST 14517/19.

⁴ [Cybersecurity of 5G networks EU Toolbox of risk mitigating measures](#) (Cybersécurité des réseaux 5G – Boîte à outils de l'UE pour les mesures d'atténuation des risques), approuvé par le groupe de coopération SRI.

⁵ [Conclusions](#) de la réunion extraordinaire du Conseil européen des 1^{er} et 2 octobre 2020, EUCO 13/20.

8. RAPPELLE l'exigence formulée par la Commission dans sa communication intitulée "Façonner l'avenir numérique de l'Europe"⁶, selon laquelle toute entreprise fournissant des services aux citoyens de l'UE devrait accepter et respecter les règles de l'UE;
9. PREND NOTE des conclusions et des recommandations figurant dans le rapport spécial et POINTE en particulier ce qui suit:
- les États membres ne font pas tous référence aux objectifs de la Commission dans leurs stratégies nationales relatives à la 5G ou dans leurs programmes nationaux dans le domaine du haut débit;
 - le code des communications électroniques européen (CCEE)⁷ n'a pas encore été transposé dans tous les États membres;
 - les fréquences pour les réseaux 5G n'ont pas été attribuées ou n'ont pas été entièrement attribuées dans tous les États membres;
 - selon la boîte à outils, la probabilité qu'un équipementier soit soumis à l'ingérence du gouvernement d'un État non-membre de l'UE constitue un autre facteur important pour déterminer son profil de risque; les critères permettant d'évaluer cette ingérence potentielle comprennent les caractéristiques du cadre juridique du pays tiers, y compris la question de savoir si celui-ci garantit un niveau suffisant de protection des données;
10. PREND NOTE des réponses de la Commission qui accompagnent le rapport spécial⁸ et de l'acceptation par la Commission des recommandations figurant dans le rapport spécial;
11. INVITE les États membres et la Commission à prêter attention aux recommandations du rapport spécial et les encourage à tenir compte de ces recommandations lors de l'élaboration de leurs politiques relatives au développement de leurs réseaux 5G, tout en assurant la sécurité de ces réseaux par l'application et le développement ultérieur de la boîte à outils pour la cybersécurité de la 5G, à la lumière des nouveaux problèmes de sécurité découlant des tendances et évolutions technologiques dans la chaîne d'approvisionnement 5G;

⁶ [Communication-shaping-europes-digital-future-feb2020_fr.pdf \(europa.eu\)](#)

⁷ Directive (EU) 2018/1972.

⁸ [COM-Réponses-SR-22-03_FR.pdf \(europa.eu\)](#)

12. INVITE la Commission à collaborer avec les États membres pour recommander des politiques et des mesures visant à atteindre les objectifs européens en matière de connectivité et de couverture 5G de toutes les zones peuplées de l'Union d'ici à 2030, tout en tenant compte des facteurs géopolitiques et économiques cruciaux — tels que l'agression de la Fédération de Russie contre l'Ukraine – susceptibles d'entraver les progrès vers la réalisation de ces objectifs et d'avoir des conséquences importantes en termes de coordination transfrontalière des États membres avec les pays tiers;
 13. INVITE la Commission, avec le soutien de l'ENISA, et les États membres à poursuivre la coopération coordonnée au niveau de l'UE sur les mesures de sécurité pour la 5G et le suivi de la mise en œuvre de la boîte à outils pour la cybersécurité de la 5G et à évaluer la nécessité d'une approche plus homogène de l'utilisation de ses éléments.
-