**Suite donnée à la résolution non législative du Parlement européen sur les menaces pour la sécurité liées à la présence technologique croissante de la Chine dans l’Union et les actions possibles à l’échelle de l’UE pour les réduire**

(Les menaces pour la sécurité liées à la présence technologique croissante de la Chine dans l’Union et les actions possibles à l’échelle de l’UE pour les réduire)

1. **Résolution présentée conformément à l’article 123, paragraphes 2 et 4, du règlement intérieur du Parlement européen**
2. **Numéros de référence**: 2019/2575 (RSP) / B8-0154/2019 / P8\_TA-PROV(2019)0156
3. **Date d’adoption de la résolution:** 12 mars 2019
4. **Commission parlementaire compétente**: s.o.
5. **Analyse/évaluation succincte de la résolution et des demandes qu’elle contient:**

Dans sa résolution, le Parlement européen exprime de profondes inquiétudes quant aux récentes allégations de vulnérabilités intégrées dans les équipements 5G fournis par des fabricants chinois. Il insiste également sur la nécessité d’une approche commune de l’UE face aux menaces en matière de cybersécurité, en particulier en ce qui concerne les infrastructures des réseaux 5G, qui constitueront l’épine dorsale de l’économie numérique. En particulier, le Parlement européen invite les États membres à se coordonner entre eux, avec la Commission et avec l’Agence européenne pour la cybersécurité (ENISA) afin d’éviter un patchwork d’interventions qui nuirait au marché unique numérique.

La résolution souligne la nécessité d’exploiter au maximum les instruments juridiques existants et à venir pour lutter contre les cybermenaces, et mentionne à cet égard la directive SRI, le code des communications électroniques européen, le règlement sur la cybersécurité et la proposition relative au centre et au réseau de compétences en matière de cybersécurité (actuellement en cours de négociation). En particulier, les États membres sont invités à achever sans délai la transposition de la directive SRI, tandis que la Commission est appelée à surveiller étroitement le processus de mise en œuvre.

La résolution invite également la Commission à définir une ligne d’action future qui permette à l’UE de devenir un acteur de premier plan dans le domaine des technologies de cybersécurité et de réduire les dépendances vis-à-vis des technologies étrangères. Dans le cadre de ce processus, la Commission devrait envisager de revoir la solidité du cadre juridique actuel en matière de cybersécurité, y compris l’extension éventuelle du champ d’application de la directive SRI à d’autres secteurs d’importance critique, ainsi que le mandat de l’ENISA afin que celle-ci travaille en priorité sur un système de certification de cybersécurité relatif aux équipements 5G. Enfin, la Commission et les États membres sont invités à tenir compte de la résolution dans le cadre du développement de la future stratégie UE-Chine.

1. **Réponse à ces demandes et aperçu des mesures que la Commission a prises ou envisage de prendre:**

En ce qui concerne la demande générale visant à ce que l’Union adopte une approche commune et se pose en chef de file dans le domaine de la cybersécurité (paragraphes 1 à 4), la Commission poursuit cet objectif au moyen d’un ensemble de politiques concrètes, en particulier le paquet «cybersécurité» de 2017 et ses actions de suivi (telles que le règlement sur la cybersécurité adopté récemment et la proposition relative à un Centre européen de compétences).

En ce qui concerne la directive SRI (paragraphes 8 et 9), la Commission note que la plupart des États membres l’ont transposée en droit national. Elle suit étroitement, par des contrôles approfondis, la mise en œuvre de cette directive, et elle est disposée à soutenir les États membres dans ce processus. Le délai de révision de la directive SRI est fixé à 2021; la Commission, sur la base d’une évaluation approfondie, examinera, parmi les domaines d’amélioration envisageables, s’il est possible d’élargir le champ d’application de la directive SRI à d’autres secteurs d’importance critique (paragraphe 10).

En ce qui concerne la cybersécurité des réseaux 5G (paragraphes 5, 7, 12, 15 et 19), la Commission a dûment tenu compte de la résolution du Parlement européen et, avec le soutien du Conseil européen, a publié, le 26 mars, une recommandation aux États membres. La recommandation, qui était annoncée dans la communication conjointe sur les relations UE-Chine (paragraphe 26), définit une série de mesures opérationnelles:

* au niveau national, les États membres devraient réaliser une évaluation des risques liés aux infrastructures des réseaux 5G d’ici au 30 juin 2019 (et la transmettre à la Commission et à l’ENISA pour le 15 juillet) et, sur la base de cette évaluation, actualiser les exigences en matière de sécurité pour les fournisseurs de réseaux et inclure des conditions pour assurer la sécurité des réseaux publics, en particulier lors de l’octroi de l’utilisation des radiofréquences des bandes 5G;
* au niveau de l’UE, un processus de coordination dans le cadre de la coopération SRI a été lancé le 30 avril 2019. Les États membres, avec le soutien de la Commission et de l’ENISA, devraient procéder à une évaluation coordonnée des risques au niveau européen pour le 1er octobre 2019 au plus tard. Sur cette base, au plus tard le 31 décembre 2019, les États membres devraient convenir d’un train de mesures d’atténuation (boîte à outils) pouvant être utilisées au niveau national et par la Commission pour l’élaboration d’exigences communes.

En outre, les États membres, en collaboration avec la Commission, devraient définir les conditions relatives à la sécurité des réseaux dont doit être assortie l’autorisation générale pour la fourniture de réseaux de communications publics. Ils devraient également participer activement à la mise au point de systèmes européens de certification pour les équipements 5G, en apportant notamment leur appui à la définition de profils de protection spécifiques et, une fois ces systèmes en place, rendre la certification 5G obligatoire. Enfin, les États membres devraient établir des exigences de sécurité spécifiques qui pourraient s’appliquer dans le cadre des marchés publics liés aux réseaux 5G, dont des exigences obligatoires concernant la certification de cybersécurité.

La recommandation prévoit que les travaux de coordination doivent avoir lieu au sein du groupe de coopération rassemblant les autorités compétentes, institué par la directive SRI, avec l’aide de la Commission et de l’ENISA.