Procedure file

Informations de base

RSP - Résolutions d'actualité	2019/2575(RSP)	Procédure terminée
Les menaces pour la sécurité liées à la la présence technologique croissante de la Chine dans l'UE et les actions possibles à l'échelle de l'UE pour les réduire Sujet 3.30.06 Technologies de l'information et de la communication, technologies numériques 3.30.07 Cybersécurité, politique cyberespace Zone géographique Chine		

Acteurs principaux

Parlement européen		
Commission européenne	DG de la Commission	Commissaire
	Marché intérieur, industrie, entrepreneuriat et PME	BIEŃKOWSKA Elżbieta

Evénements clés

13/02/2019	Débat en plénière		
12/03/2019	Résultat du vote au parlement		
12/03/2019	Décision du Parlement, 1ère lecture/lecture unique	T8-0156/2019	Résumé
12/03/2019	Fin de la procédure au Parlement		

Informations techniques

Référence de procédure	2019/2575(RSP)
Type de procédure	RSP - Résolutions d'actualité
Sous-type de procédure	Résolution sur déclaration
Base juridique	Règlement du Parlement EP 132-p2
Etape de la procédure	Procédure terminée

Portail de documentation

Proposition de résolution		B8-0153/2019	12/03/2019	EP	
Proposition de résolution		B8-0154/2019	12/03/2019	EP	
Proposition de résolution		B8-0155/2019	12/03/2019	EP	
Proposition de résolution		B8-0159/2019	12/03/2019	EP	
Proposition de résolution		B8-0160/2019	12/03/2019	EP	
Proposition de résolution		B8-0162/2019	12/03/2019	EP	

Proposition de résolution		B8-0164/2019	12/03/2019	EP	
Texte adopté du Parlement, lecture unique		T8-0156/2019	12/03/2019	EP	Résumé
Proposition de résolution commune		RC-B8-0154/2019	12/03/2019		
Réaction de la Commission sur le texte adopté en plénière		SP(2019)444	30/08/2019	EC	

2019/2575(RSP) - 12/03/2019 Texte adopté du Parlement, lecture unique

Le Parlement européen a adopté une résolution sur les menaces pour la sécurité liées à la présence technologique croissante de la Chine dans l'UE et sur les mesures que l'UE pourrait prendre pour les réduire.

La résolution a été déposée par les groupes PPE, S&D, ADLE et Verts/ALE.

Le Parlement a exprimé sa préoccupation face aux récentes allégations selon lesquelles des équipements 5G développés par des entreprises chinoises auraient pu intégrer des « portes dérobées » qui permettraient aux fabricants et aux autorités d'accéder sans autorisation aux données privées et personnelles et aux télécommunications de l'UE. Il s'est également inquiété de la présence potentielle de vulnérabilités majeures dans les équipements 5G développés par ces fabricants.

Les députés ont rappelé qu'en décembre 2018, l'autorité nationale tchèque chargée de la cybersécurité a lancé un avertissement contre les menaces à la sécurité posées par les technologies fournies par les sociétés chinoises Huawei et ZTE, et qu'en janvier 2019, l'administration fiscale tchèque a exclu Huawei d'un appel d'offres pour construire un portail fiscal.

Des inquiétudes ont été exprimées au sujet des fournisseurs d'équipements de pays tiers qui pourraient présenter un risque pour la sécurité de l'UE en raison des lois de leur pays d'origine, en particulier après l'adoption des lois chinoises sur la sécurité d'État, qui imposent à tous les citoyens et entreprises l'obligation de coopérer avec l'État, en rapport avec une définition très vaste de la sécurité nationale. En particulier, les lois chinoises sur la sécurité de l'État ont déclenché des réactions dans divers pays, allant des évaluations de sécurité à l'interdiction pure et simple.

Soulignant qu'il n'y a aucune garantie que ces obligations ne soient pas appliquées de manière extraterritoriale, les députés ont indiqué que les avantages du marché unique découlent de l'obligation de respecter les normes de l'UE et le cadre juridique de l'Union et que, par conséquent, les fournisseurs ne devraient pas être traités différemment en raison de leur pays d'origine.

Le Parlement a invité la Commission à :

- fournir, en coopération avec l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), des orientations sur la manière de lutter contre les cybermenaces et les vulnérabilités lors de l'acquisition d'équipements 5G, par exemple en diversifiant les équipements auprès de différents fournisseurs ou en introduisant des processus d'acquisition multiphase ;

-mandater l'ENISA pour travailler en priorité sur un système de certification des équipements 5G afin de garantir que le déploiement de la 5G dans l'Union réponde aux normes de sécurité les plus élevées et résiste aux portes dérobées ou aux vulnérabilités majeures qui pourraient compromettre la sécurité des réseaux de télécommunications de l'Union. La certification ne devrait toutefois pas exclure les autorités compétentes et les opérateurs du contrôle de la chaîne d'approvisionnement afin de garantir l'intégrité et la sécurité de leurs équipements qui fonctionnent dans des environnements et réseaux de télécommunications critiques ;

- évaluer la solidité du cadre juridique de l'Union afin de répondre aux préoccupations concernant la présence d'équipements vulnérables dans les secteurs stratégiques, et présenter des initiatives, y compris, le cas échéant, des propositions législatives, pour remédier à toute lacune détectée, étant donné que l'Union est constamment en train d'identifier les problèmes de cybersécurité.

Dans le même temps, le Parlement a invité les États membres à informer la Commission de toute mesure nationale qu'ils entendent adopter afin de coordonner la réponse de l'Union. Il a réaffirmé qu'il important de s'abstenir d'introduire des mesures unilatérales disproportionnées qui fragmenteraient le marché unique. Il a souligné la nécessité d'élaborer une stratégie visant à réduire la dépendance de l'Europe à l'égard des technologies étrangères dans le domaine de la cybersécurité.

Le Parlement a exhorté les États membres qui n'ont pas encore transposé intégralement la directive 2016/1148 concernant des mesures visant à assurer un niveau commun élevé de sécurité des réseaux et des systèmes d'information dans l'Union (SRI) à le faire sans délai et à veiller à ce que les mécanismes de notification prévus par la directive SRI soient correctement appliqués. La Commission a été invitée à évaluer la nécessité d'élargir le champ d'application de la directive SRI à d'autres secteurs et services critiques qui ne sont pas couverts par une législation sectorielle spécifique.

Les États membres ont également été invités à :

- veiller à ce que les institutions publiques et les entreprises privées impliquées dans le bon fonctionnement des réseaux d'infrastructures critiques tels que les télécommunications, l'énergie, la santé et les systèmes sociaux entreprennent des évaluations des risques pertinentes qui tiennent compte des menaces à la sécurité spécifiquement liées aux caractéristiques techniques du système concerné ou à la dépendance vis-à-vis de fournisseurs externes de technologies matérielles et logicielles ;

- faire de la sécurité un aspect obligatoire dans toutes les procédures de passation de marchés publics pour les infrastructures concernées, tant au niveau de l'UE qu'au niveau national ;

- imposer des sanctions aux personnes morales qui ont commis des infractions pénales telles que des attaques contre ces systèmes ;

- signaler à la Commission et à l'ENISA toute preuve de portes dérobées ou d'autres vulnérabilités majeures qui pourraient compromettre l'intégrité et la sécurité des réseaux de télécommunications ou enfreindre le droit de l'Union et les droits fondamentaux.

Enfin, le Parlement s'est félicité de l'entrée en vigueur prochaine d'un règlement établissant un cadre pour l'examen analytique des

investissements directs étrangers (IDE), soulignant que ce règlement établit pour la première fois une liste de domaines et de facteurs, dont les communications et la cybersécurité, qui sont pertinents pour la sécurité et l'ordre public au niveau européen.