Parlement européen
2014-2019

Document de séance

B8-0153/2019

6.3.2019

PROPOSITION DE RÉSOLUTION

déposée à la suite de déclarations du Conseil et de la Commission

déposée conformément à l'article 123, paragraphe 2, du règlement intérieur

sur les menaces pour la sécurité liées à la présence technologique croissante de la Chine dans l'UE et les actions possibles à l'échelle de l'UE pour les réduire (2019/2575(RSP))

Tiziana Beghin, Dario Tamburrano, Isabella Adinolfi, Rolandas Paksas
au nom du groupe EFDD

B8-0153/2019

Résolution du Parlement européen sur les menaces pour la sécurité liées à la présence technologique croissante de la Chine dans l'UE et les actions possibles à l'échelle de l'UE pour les réduire
(2019/2575(RSP))

Le Parlement européen,

– vu les communications de la Commission du 14 septembre 2016 intitulées «Connectivité pour un marché unique numérique compétitif – Vers une société européenne du gigabit» (COM(2016)0587) et «Un plan d'action pour la 5G en Europe» (COM(2016)0588),

– vu la proposition modifiée de règlement du Parlement européen et du Conseil concernant l'accès des produits et services des pays tiers au marché intérieur des marchés publics de l'Union et établissant des procédures visant à faciliter les négociations relatives à l'accès des produits et services originaires de l'Union aux marchés publics des pays tiers, présentée par la Commission le 29 janvier 2016 (COM(2016)0034),

– vu la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant les mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union[1] (directive SRI),

– vu la proposition de règlement du Parlement européen et du Conseil relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) nº 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité, présentée par la Commission le 13 septembre 2017 (règlement sur la cybersécurité) (COM(2017)0477),

– vu la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen[2],

– vu la proposition de règlement du Parlement européen et du Conseil établissant le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination, présentée par la Commission le 12 septembre 2018 (COM(2018)0630),

– vu la procédure de règlement des différends de l'OMC du 1er juin 2018 (affaire WT/DS549/6) relative à certaines mesures que la Chine avait imposées en matière de transfert de technologie étrangère en Chine,

– vu sa position adoptée en première lecture le 14 février 2019 sur la proposition de règlement du Parlement européen et du Conseil établissant un cadre pour le filtrage des

[1] JO L 194 du 19.7.2016, p. 1.
[2] JO L 321 du 17.12.2018, p. 36.

investissements directs étrangers dans l'Union européenne[3],

– vu les négociations en cours entre l'Union européenne et la Chine en vue de la conclusion d'un accord global sur les investissements,

– vu l'article 123, paragraphe 2, de son règlement intérieur,

A. considérant que les évolutions récentes dans le domaine des TIC, dont les télécommunications de 5e génération (5G), ont donné naissance à de nouvelles possibilités de production, de distribution et de déploiement de biens et de services ainsi que d'interaction entre les appareils et entre les citoyens, les administrations publiques et d'autres acteurs socioéconomiques, et qu'elles sont donc susceptibles de dynamiser l'économie européenne;

B. considérant que la cybersécurité des TIC, la protection des informations sensibles, le respect des droits individuels et la protection contre les menaces informatiques extérieures sont des conditions indispensables pour garantir la souveraineté technologique des citoyens de l'Union et, à terme, assurer la prospérité et soutenir la démocratie dans l'Union européenne;

C. considérant que la recherche et les essais relatifs à la 5G ont beaucoup de mal à tenir le rythme face à la pression étrangère en faveur du déploiement et de la commercialisation de la 5G alors que plusieurs études scientifiques ont fait part d'inquiétudes et d'incertitudes à propos de sa sécurité et de son innocuité, notamment en matière de risques de pollution électromagnétique pour la santé humaine et l'environnement;

D. considérant que la cybersécurité des réseaux 5G constitue un défi nouveau et complexe en raison de la nature virtualisée et décentralisée de la 5G et de sa chaîne de valeur fragmentée et hautement spécialisée, qui concerne autant la production que la distribution, l'installation, la configuration, l'exploitation, la maintenance et les mises à jour logicielles; qu'il faut que l'Union européenne comble le manque de cybersécurité de ses infrastructures critiques dans les secteurs des télécommunications, de l'énergie, des transports, de la santé, de la défense et de la sécurité, notamment;

E. considérant que la sécurité et l'innocuité des réseaux 5G ne peuvent pas être assurées par les fabricants et les opérateurs de réseaux, mais passent par l'action coordonnée effective de toutes les autorités nationales et internationales concernées;

F. considérant que l'Union européenne est en mesure de se poser en chef de file du développement des technologies de cybersécurité en soutenant les entreprises européennes de ce secteur et en encourageant toutes les modifications qu'il y a lieu d'apporter à la chaîne de valeur pour réduire la dépendance de l'Union à l'égard des technologies étrangères;

G. considérant que l'Union européenne a défini un ensemble de mesures visant à garantir la cybersécurité, dont la directive SRI et le règlement sur la cybersécurité, qu'il y a lieu de mettre en œuvre rapidement et de surveiller en permanence afin qu'ils gardent toute

[3] Textes adoptés de cette date, P8_TA(2019)0121.

leur efficacité en procédant aux réexamens et aux mises à jour nécessaires;

H. considérant que la présence des fournisseurs de technologies provenant de Chine et d'autres pays tiers est de plus en plus marquée sur le marché européen de la 5G, notamment les entreprises ou les sociétés peu transparentes qui appartiennent à l'État;

I. considérant que la réciprocité est l'un des meilleurs moyens d'encourager la mise en place de conditions de concurrence équitables à l'échelon mondial;

J. considérant qu'entre le règlement général sur la protection des données et les différentes exigences nationales, les sociétés étrangères sont actuellement confrontées à l'absence de normes européennes en matière de protection des données;

K. considérant que l'Union européenne et la Chine négocient la conclusion d'un accord global sur les investissements depuis 2013; que l'accord proposé contribuerait à résoudre les questions d'accès au marché, à mettre en place un cadre de protection des investissements et à définir des normes de base en matière de travail et d'environnement;

L. considérant que, même s'ils ne permettent de tirer aucune conclusion, des éléments de plus en plus nombreux tendent à prouver l'existence de défaillances de sécurité dans le matériel proposé par des fournisseurs de pays tiers, dont la Chine, et qu'il s'agit d'un risque pour les droits individuels à la vie privée et pour la protection des informations sensibles dans l'Union européenne;

1. souligne que le déploiement et la commercialisation de la 5G devraient se faire conformément au principe de précaution, en incitant tous les acteurs socioéconomiques à en anticiper les retombées éventuelles en matière de sécurité et d'innocuité et à prendre les mesures de précaution proportionnées, notamment la communication rapide des facteurs susceptibles de présenter un risque pour la santé publique ou l'environnement;

2. souligne que les retombées socioéconomiques de la 5G et des technologies qu'elle permet, comme l'internet des objets ou l'intelligence artificielle, doivent être soigneusement évaluées et qu'il convient d'adopter des mesures pour que l'avènement de la société européenne du gigabit ait lieu de façon juste et équitable pour tous et se fonde sur la responsabilité éthique;

3. invite la Commission et les États membres à créer un environnement favorable à l'innovation pour que les fabricants européens puissent développer de nouveaux produits, de nouveaux services et de nouvelles technologies ainsi qu'à aider les entreprises de l'Union à déployer et à commercialiser une 5G sécurisée et sans danger tout en veillant à ce que son potentiel soit accessible à toutes les entreprises de l'économie numérique de l'Union, y compris les petites et moyennes entreprises;

4. rappelle que la cybersécurité est l'un des plus grands défis auxquels l'Union européenne est actuellement confrontée et que toute défaillance dans ce domaine risque de porter préjudice à la vie privée et aux droits fondamentaux des consommateurs et des producteurs de l'Union, d'ébranler la confiance des citoyens à l'égard des produits et services du domaine des TIC et d'avoir, en fin de compte, de graves retombées sur

l'économie; demande un réseau qui soit sécurisé par défaut et dès la conception;

5. invite la Commission et les États membres à coopérer étroitement pour mettre en œuvre la stratégie de l'Union européenne en matière de cybersécurité ainsi qu'à associer mesures européennes et mesures nationales pour limiter le risque de défaillances de sécurité et de violation de données tout au long de la chaîne de valeur; estime que ces mesures pourraient comprendre une certification européenne de cybersécurité, des exigences de configuration, des procédures et des pratiques opérationnelles ainsi que la promotion de l'hygiène informatique et de l'enseignement numérique;

6. estime que l'agence de l'Union européenne chargée de la cybersécurité (l'ENISA – Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information) a un rôle essentiel à jouer dans l'analyse des menaces potentielles émanant de fabricants étrangers, dont la Chine, ainsi que dans la coordination d'une approche commune aux États membres pour éliminer les menaces et les attaques contre la cybersécurité;

7. invite la Commission et les États membres à mettre rapidement en œuvre l'ensemble de mesures relatives à l'économie circulaire ainsi qu'à encourager la gestion des matières premières pendant tout leur cycle de vie et le recyclage des déchets afin d'améliorer l'accès de l'Union européenne aux matières premières critiques, qui sont indispensables aux produits de haute technologies et aux innovations émergentes;

8. estime qu'il est urgent d'adopter une approche de la sécurité et de la protection des données qui soit commune aux États membres afin de s'attaquer aux menaces potentielles pour la sécurité technologique que représentent l'implantation actuelle de fabricants étrangers, notamment chinois, sur le marché de l'Union européenne;

9. invite la Commission et les États membres à analyser et à surveiller, notamment par des tests de résistance, la sécurité des systèmes informatiques faisant largement appel à des technologies de pays tiers;

10. souligne que les fournisseurs de pays tiers ne doivent pas être discriminés en raison de leur pays d'origine, mais que la transparence de ces sociétés, leurs normes de cybersécurité et l'existence d'une réciprocité pour les entreprises européennes dans le pays d'origine doivent être prises en considération afin de garantir des conditions de concurrence équitables;

11. souligne que les fournisseurs et les opérateurs chinois ou d'autres pays tiers ne doivent en aucun cas mettre en péril les droits individuels garantis par le droit de l'Union, même lorsque le droit national de leur pays d'origine prévoit des exigences différentes;

12. invite le Conseil à envisager favorablement la réouverture des discussions sur la nouvelle proposition révisée de la Commission relative à la procédure limitant l'accès des produits étrangers au marché des marchés publics de l'Union lorsqu'il n'existe pas d'accès réciproque;

13. rappelle qu'il importe d'améliorer les négociations avec les pays tiers sur la coopération en matière de réglementation dans le domaine des technologies numériques ainsi que d'assurer une plus grande participation de leur part aux instances internationales de normalisation;

14. charge son Président de transmettre la présente résolution au Conseil et à la Commission.