Parlement européen
2014-2019

TEXTES ADOPTÉS

P8_TA(2019)0156

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

Résolution du Parlement européen du 12 mars 2019 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 (2019/2575(RSP))

Le Parlement européen,

– vu la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen[1],

– vu 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[2],

– vu la directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil[3],

– 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 le 13 septembre 2017 par la Commission (règlement sur la cybersécurité) (COM(2017)0477),

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

– vu l'adoption de la nouvelle loi sur le renseignement national par le Congrès national du

1 JO L 321 du 17.12.2018, p. 36.
2 JO L 194 du 19.7.2016, p. 1.
3 JO L 218 du 14.8.2013, p. 8.

peuple chinois le 28 juin 2017,

– vu les déclarations du Conseil et de la Commission du 13 février 2019 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,

– vu l'adoption par le gouvernement australien de mesures, entrées en vigueur le 18 septembre 2018, réformant la sécurité du secteur des télécommunications,

– 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 investissements directs étrangers dans l'Union européenne[1],

– vu ses résolutions antérieures sur l'état des relations entre l'Union européenne et la Chine, notamment celle du 12 septembre 2018[2],

– vu la communication de la Commission du 14 septembre 2016 intitulée «Un plan d'action pour la 5G en Europe» (COM(2016)0588),

– vu sa résolution du 1er juin 2017 sur la connectivité internet pour la croissance, la compétitivité et la cohésion: société européenne du gigabit et 5G[3],

– vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)[4],

– vu le règlement (UE) nº 1316/2013 du Parlement européen et du Conseil du 11 décembre 2013 établissant le mécanisme pour l'interconnexion en Europe, modifiant le règlement (UE) nº 913/2010 et abrogeant les règlements (CE) nº 680/2007 et (CE) nº 67/2010[5],

– vu la proposition de règlement du Parlement européen et du Conseil établissant le programme pour une Europe numérique pour la période 2021-2027, présentée par la Commission le 6 juin 2018 (COM(2018)0434),

– vu l'article 123, paragraphes 2 et 4, de son règlement intérieur,

A. considérant que l'Union doit promouvoir son programme en matière de cybersécurité afin qu'elle puisse exploiter son potentiel pour devenir un acteur de premier plan en matière de cybersécurité et l'utiliser au profit de son industrie;

B. considérant que certaines vulnérabilités des réseaux 5G pourraient être exploitées pour compromettre des systèmes informatiques, ce qui pourrait potentiellement nuire gravement à l'économie au niveau européen et national; qu'une approche fondée sur l'analyse des risques dans l'ensemble de la chaîne de valeur est nécessaire pour réduire

---

1 Textes adoptés de cette date, P8_TA(2019)0121.
2 Textes adoptés de cette date, P8_TA(2018)0343.
3 JO C 307 du 30.8.2018, p. 144.
4 JO L 119 du 4.5.2016, p. 1.
5 JO L 348 du 20.12.2013, p. 129.

ces risques à leur minimum;

C. considérant que le réseau 5G constituera l'épine dorsale de notre infrastructure numérique, en étendant la possibilité de connecter divers équipements aux réseaux (internet des objets, etc.), et sera source de nouveaux avantages et de nouvelles opportunités pour la société et les entreprises dans de nombreux domaines, y compris des secteurs essentiels de l'économie, comme les transports, l'énergie, la santé, la finance, les télécommunications, la défense, l'espace et la sécurité;

D. considérant que la mise en place d'un mécanisme approprié pour relever les défis en matière de sécurité donnerait à l'Union la possibilité de prendre activement des mesures pour fixer des normes pour la 5G;

E. considérant que des préoccupations ont été formulées au sujet d'équipementiers de pays tiers qui pourraient présenter un risque pour la sécurité de l'Union en raison de la législation de leur pays d'origine, en particulier après l'adoption des lois chinoises sur les renseignements nationaux, qui instaurent l'obligation pour tous les citoyens, entreprises et autres entités de coopérer avec le gouvernement afin de préserver la sécurité nationale, la notion de sécurité nationale faisant l'objet d'une définition particulièrement large; qu'il n'existe aucune garantie que de telles obligations n'aient pas d'application extraterritoriale, et que les réactions face à la législation chinoise ont varié d'un pays à l'autre, allant d'une évaluation de la sécurité à une interdiction pure et simple;

F. considérant qu'en décembre 2018, l'autorité nationale tchèque en matière de cybersécurité a émis un avertissement contre les menaces pour la sécurité que représentent les technologies fournies par les sociétés chinoises Huawei et ZTE; que, par la suite, en janvier 2019, les autorités fiscales tchèques ont exclu Huawei d'un appel d'offres pour la mise en place d'un portail fiscal;

G. considérant qu'une enquête approfondie est nécessaire pour découvrir si les appareils concernés, ou tout autre appareil ou fournisseur, présentent des risques pour la sécurité en raison de la présence de «portes dérobées» vers les systèmes;

H. considérant que les solutions devraient être coordonnées et traitées à l'échelon de l'Union pour éviter d'être confrontés à des niveaux de sécurité différents et à d'éventuelles failles dans la cybersécurité, une coordination mondiale étant par ailleurs nécessaire pour apporter une réponse forte à ce problème;

I. considérant que les avantages du marché unique vont de pair avec l'obligation de respecter les normes de l'Union et son cadre juridique, et que les fournisseurs ne devraient pas faire l'objet de différences de traitement en fonction de leur pays d'origine;

J. considérant que le règlement sur le filtrage des investissements directs étrangers, qui devrait entrer en vigueur d'ici à la fin de 2020, renforce la capacité des États membres à filtrer les investissements étrangers sur la base de la sécurité et de l'ordre public, et établit un mécanisme de coopération qui permet à la Commission et aux États membres de coopérer à l'évaluation des risques en matière de sécurité, notamment en matière de cybersécurité, que présentent les investissements étrangers sensibles, et couvre également les projets et programmes présentant un intérêt pour l'Union, tels que les

réseaux transeuropéens de télécommunications et Horizon 2020;

1. estime que l'Union doit se poser en chef de file de la cybersécurité à l'aide d'une approche commune fondée sur l'utilisation efficiente et efficace des connaissances d'expert de l'Union, des États membres et de l'industrie, étant donné qu'un patchwork de décisions nationales divergentes nuirait au marché unique numérique;

2. se dit vivement préoccupé par les informations récentes selon lesquelles le matériel 5G mis au point par les entreprises chinoises contiendrait des portes dérobées incorporées permettant aux fabricants et aux autorités chinoises d'accéder, sans y être autorisés, aux données et aux télécommunications privées à caractère personnel échangées dans l'Union;

3. s'inquiète également de la présence éventuelle de points faibles importants dans le matériel 5G développé par ces fabricants s'il venait à être installé lors du déploiement des réseaux 5G dans les années à venir;

4. souligne que les enjeux de sécurité des réseaux et du matériel sont semblables dans le monde entier et invite l'Union à tirer des enseignements de l'expérience disponible pour pouvoir garantir les normes les plus élevées de cybersécurité; invite la Commission à élaborer une stratégie qui mette l'Europe en tête dans le domaine des technologies de la cybersécurité et qui vise à réduire la dépendance de l'Europe vis-à-vis des technologies étrangères dans le domaine de la cybersécurité; estime que si le respect des exigences de sécurité ne peut être garanti, il convient d'appliquer des mesures adéquates;

5. invite les États membres à informer la Commission de toute mesure nationale qu'ils entendent adopter afin de coordonner la réponse de l'Union et ainsi garantir des normes de cybersécurité particulièrement élevées dans l'ensemble de l'Union et rappelle qu'il importe de s'abstenir de mettre en place des mesures unilatérales disproportionnées qui fragmenteraient le marché unique;

6. réaffirme que toute entité qui fournit du matériel ou des services dans l'Union, quel que soit son pays d'origine, doit se conformer aux obligations en matière de droits fondamentaux et à la législation de l'Union et des États membres, y compris le cadre juridique en matière de respect de la vie privée, de protection des données et de cybersécurité;

7. invite la Commission à évaluer la solidité du cadre juridique de l'Union afin d'apporter une réponse aux inquiétudes concernant la présence de matériel vulnérable dans les secteurs stratégiques et les infrastructures de base; demande instamment à la Commission de présenter des initiatives, y compris des propositions législatives s'il y a lieu, pour remédier en temps utile à toute défaillance détectée étant donné que l'Union est dans un processus constant d'identification et de correction des problèmes de sécurité et d'amélioration de la résilience en matière de cybersécurité dans l'Union;

8. invite instamment les États membres qui n'ont pas encore transposé intégralement la directive sur la sécurité des réseaux et des systèmes d'information (directive SRI) à le faire sans attendre et demande à la Commission de suivre étroitement cette transposition pour ainsi veiller à ce que ses dispositions soient correctement appliquées et respectées et que les citoyens européens soient mieux protégés des menaces extérieures et intérieures sur la sécurité;

9. demande instamment à la Commission et aux États membres de veiller à ce que les mécanismes de signalement introduits par la directive SRI soient correctement appliqués; fait observer que la Commission et les États membres devraient consacrer une attention approfondie à tout incident de sécurité ou toute réaction inappropriée des fournisseurs afin de remédier aux lacunes constatées;

10. invite la Commission à étudier la nécessité d'élargir le champ d'application de la directive SRI à de nouveaux secteurs et services d'importance critique qui ne sont pas couverts par une législation spécifique;

11. salue et appuie l'accord conclu sur le règlement sur la cybersécurité et le renforcement du mandat de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) pour mieux aider les États membres à lutter contre les menaces et les attaques en matière de cybersécurité;

12. demande instamment à la Commission de charger l'ENISA d'accorder la priorité à la définition d'un système de certification du matériel 5G afin de veiller à ce que le déploiement de la 5G dans l'Union réponde aux normes de sécurité les plus élevées et résiste aux portes dérobées ou à d'autres failles importantes qui mettraient en danger la sécurité des réseaux de télécommunications et des services correspondants dans l'Union; recommande d'accorder une attention particulière aux processus, produits et logiciels communément utilisés qui ont, de par leur ampleur, une incidence importante sur la vie quotidienne des citoyens et l'économie;

13. se félicite des propositions relatives aux centres de compétences en matière de cybersécurité et à un réseau de centres nationaux de coordination, conçues pour aider l'Union à garder et à développer les capacités technologiques et industrielles nécessaires pour sécuriser son marché unique numérique; rappelle toutefois que la certification ne devrait pas exclure les autorités compétentes et les opérateurs du processus d'examen de la chaîne d'approvisionnement afin de garantir ainsi l'intégrité et la sécurité des équipements qu'ils intègrent dans les environnements critiques et les réseaux de télécommunications;

14. rappelle que la cybersécurité exige des normes élevées en matière de sécurité; demande un réseau qui soit sécurisé par défaut et dès la conception; invite instamment les États membres à explorer avec la Commission tous les moyens disponibles pour garantir un niveau élevé de sécurité;

15. invite la Commission, en coopération avec l'ENISA, à préconiser des stratégies destinées à éviter les cybermenaces et les vulnérabilités lors de l'acquisition de matériel et de services 5G divers, par exemple, en diversifiant les matériels fournis ou en prévoyant des procédures de marchés publics multiphases;

16. réaffirme sa position sur le programme pour une Europe numérique qui impose des exigences de sécurité et le contrôle de la Commission sur les entités établies dans l'Union européenne mais contrôlées depuis des pays tiers, en particulier pour les actions liées à la cybersécurité;

17. invite les États membres à veiller à ce que les institutions publiques et les entreprises privées contribuant au bon fonctionnement de réseaux d'infrastructures critiques comme les télécommunications, l'énergie, la santé et les système sociaux réalisent des

évaluations adéquates des risques en tenant compte des menaces pour la sécurité liées spécifiquement aux caractéristiques techniques du système qui les concerne ou à la dépendance à l'égard de fournisseurs externes de matériel et de logiciels informatiques;

18. rappelle que le cadre juridique actuel sur les télécommunications commande aux États membres de veiller à ce que les opérateurs de télécommunications respectent l'intégrité et la disponibilité des réseaux publics de communications électroniques, notamment un chiffrement de bout en bout si nécessaire; souligne qu'en vertu du code des communications électroniques européen, les États membres disposent de pouvoirs étendus pour enquêter sur les produits mis sur le marché de l'Union et prendre un large éventail de mesures en cas de non-conformité;

19. invite la Commission et les États membres à 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;

20. rappelle aux États membres l'obligation qui leur incombe en vertu du cadre juridique de l'Union, notamment de la directive 2013/40/UE relative aux attaques contre les systèmes d'information, d'imposer des sanctions aux personnes morales qui se sont rendues coupables d'infractions pénales telles que des attaques contre ces systèmes; souligne que les États membres devraient également recourir à la faculté d'imposer d'autres sanctions à ces entités juridiques, telles que l'interdiction temporaire ou définitive de se livrer à certaines activités commerciales;

21. invite les États membres, les agences de cybersécurité, les opérateurs de télécommunications, les fabricants et les fournisseurs de services d'infrastructures critiques à signaler à la Commission et à l'ENISA tout élément attestant l'existence de portes dérobées ou d'autres failles importantes susceptibles de compromettre l'intégrité et la sécurité des réseaux de télécommunications ou d'enfreindre le droit de l'Union et les droits fondamentaux; demande aux autorités nationales de protection des données et au contrôleur européen de la protection des données d'examiner attentivement les indices de violation de données à caractère personnel de la part de fabricants extérieurs et d'imposer des sanctions adéquates conformément à la législation européenne relative à la protection des données;

22. se félicite de la prochaine entrée en vigueur en vigueur d'un règlement établissant un cadre pour le filtrage des investissements étrangers directs (IED) pour des motifs de sécurité et d'ordre public, et souligne que ce règlement établit pour la première fois une liste de domaines et de facteurs, notamment les communications et la cybersécurité, qui intéressent la sécurité et l'ordre public au niveau de l'Union européenne;

23. invite le Conseil à accélérer ses travaux sur la proposition de règlement «vie privée et communications électroniques»;

24. réaffirme que l'Union européenne doit promouvoir la cybersécurité tout au long de la chaîne de valeur, de la recherche jusqu'au déploiement et à l'adoption de technologies clés, diffuser les informations en la matière et promouvoir l'hygiène informatique et des programmes de formation, notamment sur la cybersécurité, et estime que le programme pour une Europe numérique fait partie des outils efficaces pour y parvenir;

25. prie instamment la Commission et les États membres de prendre les mesures

nécessaires, notamment des programmes d'investissement solides, afin de créer un environnement propice à l'innovation au sein de l'Union, qui devraient être accessibles à toutes les entreprises dans l'économie numérique de l'Union, y compris les petites et moyennes entreprises (PME); insiste, en outre, sur le fait qu'un tel environnement devrait permettre aux fabricants européens de développer de nouveaux produits, services et technologies, ce qui leur permettrait d'être compétitifs;

26. demande instamment à la Commission et aux États membres de tenir compte des demandes susmentionnées lors des discussions à venir sur la future stratégie UE-Chine car c'est à cette condition que l'Union restera compétitive et qu'elle garantira la sécurité de ses infrastructures numériques;

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