Parlement européen
2019-2024

Commission des affaires étrangères

2023/2072(INI)

5.9.2023

PROJET DE RAPPORT

sur les implications en matière de sécurité et de défense de l'influence de la Chine sur les infrastructures critiques dans l'Union européenne
(2023/2072(INI))

Commission des affaires étrangères

Rapporteur: Klemen Grošelj

PR_INI

SOMMAIRE

Page

PROPOSITION DE RÉSOLUTION DU PARLEMENT EUROPÉEN 3

PROPOSITION DE RÉSOLUTION DU PARLEMENT EUROPÉEN

sur les implications en matière de sécurité et de défense de l'influence de la Chine sur les infrastructures critiques dans l'Union européenne
(2023/2072(INI))

Le Parlement européen,

– vu le traité sur le fonctionnement de l'Union européenne,

– vu le titre V du traité sur l'Union européenne, et notamment son chapitre 2, section 2, sur les dispositions concernant la politique de sécurité et de défense commune,

– vu la «boussole stratégique en matière de sécurité et de défense – pour une Union européenne qui protège ses citoyens, ses valeurs et ses intérêts, et qui contribue à la paix et à la sécurité internationales», approuvée par le Conseil le 21 mars 2022 et entérinée par le Conseil européen le 25 mars 2022,

– vu la déclaration de Versailles adoptée le 11 mars 2022 lors d'une réunion informelle des chefs d'État ou de gouvernement,

– vu la communication conjointe de la Commission et du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité du 20 juin 2023 sur la stratégie européenne de sécurité économique (JOIN(2023)0020),

– vu la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil (directive sur la résilience des entités critiques)[1],

– vu la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2)[2],

– vu la recommandation du Conseil du 8 décembre 2022 relative à une approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques,

– vu le communiqué du sommet de Vilnius publié par les chefs d'État et de gouvernement de l'OTAN participant à la réunion du Conseil de l'Atlantique Nord qui s'est tenue à Vilnius le 11 juillet 2023,

[1] JO L 333 du 27.12.2022, p. 164.
[2] JO L 333 du 27.12.2022, p. 80.

– vu le règlement (UE) 2023/XXXX du Parlement européen et du Conseil du [date] établissant un cadre de mesures pour renforcer l'écosystème européen des semi-conducteurs (règlement sur les semi-conducteurs)[3],

– vu la proposition de règlement du Parlement européen et du Conseil relatif aux exigences horizontales en matière de cybersécurité applicables aux produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020, présentée par la Commission le 15 septembre 2022 (COM(2022)0454),

– vu l'article 54 de son règlement intérieur,

– vu l'avis de la commission du commerce international,

– vu le rapport de la commission des affaires étrangères (A9-0000/2023),

A. considérant que la récente communication conjointe sur une stratégie européenne en matière de sécurité économique vise à réduire au minimum les risques découlant de certains flux économiques dans un contexte de tensions géopolitiques accrues et d'une accélération des évolutions technologiques, tout en préservant un maximum d'ouverture et de dynamisme économiques;

B. considérant que la directive sur la résilience des entités critiques et la directive SRI 2 fournissent un cadre juridique complet pour renforcer la résilience physique et numérique des infrastructures critiques, y compris celles liées à l'énergie, aux transports, à la santé, aux infrastructures numériques, à l'eau et à l'alimentation;

C. considérant que, depuis la publication de la recommandation du Conseil du 8 décembre 2022, des actions ciblées ont déjà été lancées pour garantir une réponse commune de l'Union aux incidents, notamment en renforçant la coordination avec l'OTAN par l'intermédiaire de la task force UE-OTAN sur la résilience des infrastructures critiques intégrée dans le dialogue structuré OTAN-UE sur la résilience;

D. considérant que les politiques coercitives et la détermination croissante de la République populaire de Chine (RPC), y compris sa position agressive à l'égard de Taïwan, ainsi que les conséquences sociales et économiques de la pandémie de COVID-19 et de la guerre d'agression menée par la Russie contre l'Ukraine ont mis en lumière les vulnérabilités de l'Union et rappelé la nécessité de «réduire les risques» de ses relations avec la RPC et d'autres pays tiers non démocratiques;

E. considérant que l'acquisition par la Chine d'infrastructures critiques, en particulier dans le voisinage de l'Union, y compris dans les Balkans occidentaux, représente un risque croissant du point de vue du lien entre commerce et sécurité;

F. considérant que le partenariat stratégique sino-russe continue de se développer, notamment dans les domaines des transferts de technologie et de capacités militaires;

[3] JO L XXX.

L'enjeu central: comprendre la stratégie chinoise en matière de fusion militaro-civile

1. souligne que la stratégie chinoise de fusion militaro-civile est un programme conçu et mis en œuvre par l'État qui prévoit d'instrumentaliser tous les leviers du pouvoir étatique et de la puissance commerciale afin de renforcer et de soutenir l'Armée populaire de libération (APL), la branche armée du Parti communiste chinois (PCC);

2. observe que le système politique et l'économie de la Chine, orientés par le parti, exigent souvent des entreprises privées qu'elles alignent leurs intérêts commerciaux sur les activités militaires, de répression et d'ingérence politique du PCC; souligne que, par conséquent, les activités internationales des entreprises chinoises aident le PCC à étendre son influence sur les pays étrangers et à fragiliser ses rivaux géopolitiques;

3. considère que la fusion militaro-civile doit être analysée dans un contexte politique et stratégique plus large, en tenant compte de ses interconnexions avec d'autres initiatives, telles que l'initiative «Une ceinture, une route» (y compris la route de la soie du numérique); estime que la visée ultime de la fusion militaro-civile est de faire progresser l'objectif stratégique à long terme de la Chine de devenir la première puissance mondiale;

Conséquences de la stratégie civilo-militaire de la RPC

4. met en garde contre les risques liés à toute forme de participation des entreprises chinoises à des actifs stratégiques de l'Union, en particulier celles entretenant des liens directs ou indirects avec le système militaire chinois; souligne, à cet égard, sa préoccupation quant au transfert de technologie et d'expertise technologique vers l'armée chinoise, qui renforcera la capacité de l'APL à développer la prochaine génération de technologies militaires et pourrait servir à exercer une contrainte sur des partenaires en Asie et dans le monde entier;

5. souligne que la Chine produit 70 % des batteries dans le monde (trois des cinq plus gros groupes de fabrication de batteries se situant sur son territoire), représente 60 % de la production mondiale d'aluminium et 75 % de la production mondiale de silicium, est le raffineur prépondérant de 60 % du lithium, assure 70 % du traitement du cuivre et produit 84 % du nickel et 85 % du cobalt à l'échelle mondiale; souligne que les entreprises minières chinoises sont actives en République démocratique du Congo (cobalt), en Indonésie (nickel), au Chili et en Australie (lithium) et que son quasi-monopole sur la production et la transformation de ces ressources critiques représente non seulement un défi géopolitique aigu pour l'Union, mais aussi un risque énorme pour la défense européenne et d'autres secteurs industriels;

6. rappelle que les communications tant diplomatiques que militaires passent par des câbles sous-marins privés fournis par des entreprises chinoises, telles que HMN Technologies, une entité affiliée aux services de cyberrenseignement de l'APL; se déclare vivement préoccupé par les systèmes de câbles sous-marins servant à la transmission de données exploités par la société chinoise HMN Technologies, qui relient les territoires des États membres de l'Union et la région indo-pacifique, y compris des bases militaires des États membres et de l'OTAN dans la région, ce qui crée des vulnérabilités en matière de sécurité pour la surveillance sous-marine et la collecte de renseignements;

Élaborer des réponses: élargir la boîte à outils pour répondre aux préoccupations en matière de sécurité et de défense

7. alerte sur le fait que la détérioration de l'environnement de sécurité en Europe et dans le monde requiert une réflexion urgente sur la manière de renforcer l'autonomie stratégique de l'Union et de réduire sa dépendance à l'égard de pays comme la RPC qui sont des rivaux systémiques et non des partenaires stratégiques; souligne la nécessité d'empêcher les fuites de technologies émergentes sensibles et de biens essentiels à double usage vers des pays destinataires problématiques qui déploient des stratégies de fusion militaro-civile ou y collaborent;

8. demeure préoccupé par le fait que les infrastructures critiques européennes deviennent de plus en plus vulnérables à l'influence extérieure; salue, à cet égard, les récentes mesures législatives visant à renforcer la résilience des entités critiques dans l'Union; constate toutefois avec inquiétude que la plupart de ces initiatives se limitent à des procédures de filtrage des investissements directs étrangers, ce qui laisse au PCC la possibilité d'accéder à des actifs critiques et d'exercer une influence sur ceux-ci;

9. note que le filtrage des parties prenantes ayant accès aux infrastructures critiques ne saurait se limiter aux investissements directs; demande que les instruments actuels qui s'appliquent aux investissements directs étrangers et aux subventions étrangères soient étendus afin d'y inclure des procédures de filtrage généralisées pour toutes les parties prenantes participant aux projets d'infrastructures critiques de l'Union; invite la Commission, avec le soutien des États membres, à cartographier, suivre et évaluer l'accès de la Chine aux infrastructures critiques dans l'Union; souligne que les États membres sont responsables en dernier ressort de la protection des infrastructures, mais qu'ils n'ont pas systématiquement mis en œuvre les lignes directrices actuelles sur les investissements directs étrangers ni mis en place des mécanismes nationaux de filtrage des investissements;

10. se félicite du potentiel de la proposition de la Commission relative à une stratégie européenne en matière de sécurité économique pour étendre la boîte à outils de l'Union aux exportations ou aux investissements extérieurs dans un ensemble restreint de technologies clés génériques dotées d'applications militaires, notamment dans les domaines de l'informatique quantique, des semi-conducteurs avancés et de l'intelligence artificielle; demande que les propositions de la Commission soient adoptées rapidement et que les États membres mettent pleinement en œuvre le cadre réglementaire élargi de l'Union afin d'exclure les entités susceptibles de contribuer à la fusion militaro-civile;

11. se félicite en outre de la proposition de la Commission visant à prévenir les fuites de technologies émergentes sensibles en dressant une liste de technologies à double usage, sur la base de critères étroitement définis et prospectifs, tels que le caractère potentiellement habilitant et transformateur d'une technologie, le risque lié à la fusion militaro-civile et le risque que cette technologie soit utilisée abusivement pour violer les droits de l'homme; invite la Commission et les États membres à définir et à mettre en œuvre dans les meilleurs délais les mesures de protection pertinentes pour ces technologies à double usage;

12. se félicite de l'adoption du règlement européen sur les semi-conducteurs, qui renforcera la capacité de l'Union à produire des semi-conducteurs et créera une cartographie stratégique, entre autres, des lacunes capacitaires dans la chaîne de valeur des semi-conducteurs dans l'Union, ce qui permettra de limiter la dépendance de l'Union à l'égard de pays tiers tels que la Chine; appelle de ses vœux de nouvelles propositions visant à sécuriser les chaînes de production et d'approvisionnement des infrastructures et matériaux critiques au sein de l'Union;

13. invite la Commission à proposer un nouveau cadre législatif afin d'atténuer les risques pour la sécurité émanant des fournisseurs de systèmes de câbles sous-marins; souligne la nécessité d'empêcher les fournisseurs de systèmes de câbles, notamment les entreprises chinoises, de partager des données avec des services de renseignement à d'autres fins que la protection des infrastructures contre les intrusions extérieures ou les attaques malveillantes;

Lien entre aspects intérieurs et extérieurs: renforcer la résilience des partenaires les plus proches de l'Union

14. est conscient du fait que la RPC pénètre le marché de l'Union et de son voisinage élargi; invite la Commission et le Service européen pour l'action extérieure (SEAE) à veiller à ce que les mesures prises pour renforcer la résilience de l'Union face à l'influence chinoise soient également étendues aux partenaires les plus proches de l'Union, en particulier aux pays en voie d'adhésion et à ceux qui font partie de la politique de voisinage de l'Union;

15. rappelle que les forces navales de la RPC disposent d'outils juridiques qui leur garantissent de pouvoir utiliser les navires civils et les infrastructures civiles de la Chine à des fins militaires et de sécurité; relève que la Chine peut utiliser ses infrastructures commerciales civiles pour soutenir la présence de l'APL dans les pays tiers; met en garde contre le fait qu'une telle fusion militaro-civile permet à l'APL d'accéder aux ports étrangers, ce qui lui donne la possibilité de prépositionner un soutien logistique afin de soutenir des déploiements navals pouvant s'étendre jusqu'à l'océan Indien, la mer Méditerranée et l'océan Atlantique; souligne que les risques d'espionnage sont les plus élevés lorsque les actifs commerciaux civils chinois sont situés sur des plateformes logistiques proches de bases navales de l'Union et de l'OTAN ou d'opérateurs portuaires qui ont signé des accords visant à fournir un soutien logistique aux entreprises européennes;

16. constate qu'un tiers de l'ensemble des infrastructures africaines construites depuis 2010 a été financé et construit par des entreprises publiques chinoises; souligne qu'au cours des vingt dernières années, la Chine a accru ses engagements en matière de commerce, d'investissement et de prêt, avec des obligations contractuelles peu nombreuses ou opaques; se déclare préoccupé par le fait que ce modèle chinois est clairement attractif pour de nombreux pays qui ne peuvent satisfaire aux exigences de l'Union en matière d'accès à des niveaux de financement équivalents, ce qui accroît l'influence chinoise au détriment des partenariats de l'Union; invite la Commission et le SEAE à veiller à ce que les normes élevées de l'Union en matière d'investissement auprès de ses partenaires ne compromettent pas ses relations et ses engagements en matière de sécurité en tant que partenaire fiable et stratégique;

17. insiste avec inquiétude sur la stratégie de la RPC visant à édifier une «base de coopération en matière d'économie bleue» le long de la côte africaine, y compris par la construction de navires de pêche et d'installations de réparation de navires, qui peuvent également être utilisées à des fins militaires; souligne le manque généralisé de détails et de transparence en ce qui concerne ces accords et ces licences avec les pays africains; insiste sur les conséquences géopolitiques potentielles pour l'Union, en particulier dans les pays tiers où l'Union est engagée;

°

° °

18. charge sa Présidente de transmettre la présente résolution au vice-président de la Commission/haut représentant de l'Union pour les affaires étrangères et la politique de sécurité, au Conseil et à la Commission.