Parlamento europeo
2019-2024

Commissione per gli affari esteri

2023/2072(INI)

5.9.2023

PROGETTO DI RELAZIONE

sulle implicazioni in materia di sicurezza e di difesa dell'influenza della Cina sulle infrastrutture critiche nell'Unione europea
(2023/2072(INI))

Commissione per gli affari esteri

Relatore: Klemen Grošelj

INDICE

Pagina

PROPOSTA DI RISOLUZIONE DEL PARLAMENTO EUROPEO 3

PROPOSTA DI RISOLUZIONE DEL PARLAMENTO EUROPEO

sulle implicazioni in materia di sicurezza e di difesa dell'influenza della Cina sulle infrastrutture critiche nell'Unione europea
(2023/2072(INI))

Il Parlamento europeo,

– visto il trattato sul funzionamento dell'Unione europea,

– visto il titolo V del trattato sull'Unione europea, in particolare il capo 2, sezione 2, recante disposizioni sulla politica di sicurezza e di difesa comune,

– vista la "Bussola strategica per la sicurezza e la difesa – Per un'Unione europea che protegge i suoi cittadini, i suoi valori e i suoi interessi e contribuisce alla pace e alla sicurezza internazionali", approvata dal Consiglio il 21 marzo 2022 e dal Consiglio europeo il 25 marzo 2022,

– vista la dichiarazione di Versailles, adottata durante la riunione informale dei capi di Stato e di governo l'11 marzo 2022,

– vista la comunicazione congiunta della Commissione e dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza del 20 giugno 2023 sulla "Strategia europea per la sicurezza economica" (JOIN(2023)0020),

– vista la direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio (direttiva CER)[1],

– vista la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2)[2],

– vista la raccomandazione del Consiglio dell'8 dicembre 2022 su un approccio coordinato a livello dell'Unione per rafforzare la resilienza delle infrastrutture critiche,

– visto il comunicato del vertice di Vilnius, rilasciato dai capi di Stato e di governo della NATO che hanno partecipato alla riunione del Consiglio del Nord Atlantico svoltasi a Vilnius l'11 luglio 2023,

– visto il regolamento (UE) 2023/XXXX del Parlamento europeo e del Consiglio, del [data], che istituisce un quadro di misure per rafforzare l'ecosistema europeo dei semiconduttori (regolamento sui chip)[3],

[1] GU L 333 del 27.12.2022, pag. 164.
[2] GU L 333 del 27.12.2022, pag. 80.
[3] GU L XXX.

– vista la proposta della Commissione del 15 settembre 2022 di un regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020 (COM(2022)0454),

– visto l'articolo 54 del suo regolamento,

– visto il parere della commissione per il commercio internazionale,

– vista la relazione della commissione per gli affari esteri (A9-0000/2023),

A. considerando che la recente comunicazione congiunta su una strategia europea per la sicurezza economica si concentra sull'idea di ridurre al minimo i rischi derivanti da determinati flussi economici nel contesto delle crescenti tensioni geopolitiche e dell'accelerazione dei cambiamenti tecnologici, preservando nel contempo la massima apertura e il massimo dinamismo dell'economia;

B. considerando che la direttiva sulla resilienza dei soggetti critici e la direttiva NIS 2 dispongono un quadro giuridico completo per rafforzare la resilienza fisica e digitale delle infrastrutture critiche, comprese quelle relative all'energia, ai trasporti, alla sanità, alle infrastrutture digitali, all'acqua e ai prodotti alimentari;

C. considerando che, a seguito della raccomandazione del Consiglio dell'8 dicembre 2022, sono già in corso azioni mirate per garantire una risposta comune dell'UE agli incidenti, anche rafforzando il coordinamento con la NATO attraverso la task force UE-NATO sulla resilienza delle infrastrutture critiche nel quadro del dialogo strutturato UE-NATO sulla resilienza;

D. considerando che le politiche coercitive e la crescente assertività della Repubblica popolare cinese (RPC), compresa la sua posizione aggressiva nei confronti di Taiwan, come pure le conseguenze sociali ed economiche della pandemia di COVID-19 e della guerra di aggressione della Russia contro l'Ucraina, hanno messo in luce le vulnerabilità dell'UE e riaffermato la necessità di ridurre i rischi connessi alle sue relazioni con la RPC e altri paesi terzi non democratici;

E. considerando che l'acquisizione di infrastrutture critiche da parte della Cina, in particolare nel vicinato dell'UE, compresi i Balcani occidentali, rappresenta un rischio crescente per il nesso tra commercio e sicurezza;

F. considerando che il partenariato strategico tra Cina e Russia continua a espandersi, anche nei settori della tecnologia e dei trasferimenti di capacità militari;

Il cuore del problema: comprendere la strategia di fusione militare-civile della Cina

1. sottolinea che la strategia di fusione militare-civile della Cina consiste in un programma e un piano diretti e guidati dallo Stato per strumentalizzare tutte le leve del potere statale e commerciale al fine di rafforzare e sostenere l'esercito popolare di liberazione, ovvero il braccio armato del partito comunista cinese;

2. ritiene che il sistema politico e l'economia cinesi, diretti dal partito, spesso chiedano alle imprese private di allineare i loro interessi commerciali alle attività militari, di repressione e di ingerenza politica del partito comunista cinese; sottolinea che, di conseguenza, le attività internazionali delle imprese cinesi aiutano il partito ad ampliare la sua influenza su paesi stranieri e a danneggiare i rivali geopolitici;

3. ritiene che la fusione militare-civile debba essere intesa in un contesto politico e strategico più ampio, tenendo conto delle sue interconnessioni con altre iniziative, come la Nuova via della seta (compresa la Via della seta digitale); ritiene che l'obiettivo ultimo della fusione militare-civile sia quello di portare avanti l'obiettivo strategico a lungo termine della Cina di diventare la potenza leader a livello mondiale;

Conseguenze della strategia civile-militare della Repubblica popolare cinese

4. avverte riguardo al rischio connesso a qualsiasi forma di partecipazione di imprese cinesi alle risorse strategiche dell'Unione, in particolare per quanto riguarda le imprese che hanno legami diretti o indiretti con il sistema militare cinese; sottolinea, a tale proposito, il suo timore riguardo al trasferimento di tecnologia e competenze tecnologiche all'esercito cinese, il che aumenterebbe la capacità dell'esercito popolare di liberazione di sviluppare la prossima generazione di tecnologia militare, che può essere utilizzata a scopi coercitivi sui partner in Asia e in tutto il mondo;

5. sottolinea che la Cina produce il 70 % delle batterie a livello mondiale (poiché ospita tre dei cinque maggiori giganti della produzione di batterie), rappresenta il 60 % della produzione mondiale di alluminio e il 75 % della produzione di silicio, è il principale raffinatore del 60 % del litio e del 70 % della lavorazione del rame e produce l'84 % del nichel a livello mondiale, nonché l'85 % del cobalto; sottolinea che le imprese minerarie cinesi sono attive nella Repubblica democratica del Congo (cobalto), in Indonesia (nichel), in Cile e in Australia (litio) e che il quasi monopolio cinese nella produzione e nella lavorazione di queste materie prime critiche rappresenta non solo una sfida geopolitica pressante per l'Unione, ma anche un enorme rischio per la difesa europea e altri settori industriali;

6. ricorda che la comunicazione diplomatica e quella militare viaggiano attraverso cavi sottomarini di proprietà privata forniti da imprese cinesi, come la HMN Technologies, un'entità affiliata all'intelligence informatica dell'esercito popolare di liberazione; esprime una profonda preoccupazione per i sistemi di cavi di dati sottomarini gestiti dall'impresa cinese HMN Technologies, che collegano i territori degli Stati membri dell'UE e la regione indo-pacifica, comprese le basi militari degli Stati membri e della NATO nella regione, creando vulnerabilità in materia di sicurezza per quanto riguarda la sorveglianza subacquea e la raccolta di informazioni;

Cercare le risposte: ampliare il pacchetto di strumenti per affrontare le preoccupazioni in materia di sicurezza e di difesa

7. avverte che il deterioramento del clima di sicurezza in Europa e in tutto il mondo richiede una riflessione urgente su come rafforzare l'autonomia strategica dell'UE e ridurre la sua dipendenza da paesi come la Repubblica popolare cinese, che sono rivali sistemici e non partner strategici; sottolinea la necessità di evitare la diffusione di tecnologie emergenti sensibili e di prodotti a duplice uso di importanza fondamentale a

destinatari preoccupanti, che perseguono strategie di fusione militare-civile o collaborano a tali strategie;

8. continua a nutrire preoccupazione per il fatto che le infrastrutture critiche europee sono sempre più vulnerabili alle influenze esterne; elogia, a tale riguardo, le recenti iniziative legislative intese a migliorare la resilienza dei soggetti critici nell'UE; osserva, tuttavia, con preoccupazione che tali iniziative si limitano per lo più alle procedure di controllo degli investimenti esteri diretti, lasciando al partito comunista cinese altri canali aperti attraverso i quali ottenere accesso e influenza per quanto riguarda risorse critiche;

9. osserva che il controllo dei portatori di interessi che hanno accesso a risorse critiche non può limitarsi agli investimenti diretti; chiede che gli attuali strumenti relativi agli investimenti esteri diretti e alle sovvenzioni estere siano ampliati in modo da includervi procedure di controllo generalizzate per tutti i portatori di interessi coinvolti in progetti infrastrutturali critici dell'UE; invita la Commissione, con il sostegno degli Stati membri, a mappare, tracciare e valutare l'accesso della Cina alle infrastrutture critiche nell'UE; sottolinea che gli Stati membri sono, in ultima istanza, responsabili della protezione delle infrastrutture, ma non hanno attuato in modo sistematico gli attuali orientamenti in materia di controllo degli investimenti esteri diretti, né hanno istituito meccanismi di controllo degli investimenti a livello nazionale;

10. si compiace del potenziale insito nella proposta della Commissione relativa a una strategia europea per la sicurezza economica riguardo all'ipotesi di estendere il pacchetto di strumenti dell'UE alle esportazioni o agli investimenti all'estero in una serie ristretta di tecnologie abilitanti fondamentali con applicazioni militari, fra l'altro nei settori dell'informatica quantistica, dei semiconduttori avanzati e dell'intelligenza artificiale; chiede la rapida adozione delle proposte della Commissione e invita gli Stati membri ad attuare pienamente il quadro normativo ampliato dell'UE al fine di escludere le entità che potrebbero contribuire alla fusione militare-civile;

11. si compiace inoltre della proposta della Commissione di prevenire la fuga di tecnologie emergenti sensibili istituendo un elenco di tecnologie a duplice uso sulla base di criteri rigorosamente definiti e lungimiranti, come ad esempio la potenziale natura abilitante e trasformativa di una tecnologia, il rischio di fusione militare-civile e il rischio che la tecnologia sia usata in modo improprio per violare diritti umani; invita la Commissione e gli Stati membri a individuare e attuare quanto prima le pertinenti misure di protezione per tali tecnologie a duplice uso;

12. si compiace dell'adozione del regolamento sui chip, che aumenterà la capacità dell'UE di produrre semiconduttori e creerà una mappa strategica, tra l'altro, delle carenze di capacità nella catena del valore dei semiconduttori nell'UE, limitando così la dipendenza dell'UE da paesi terzi come la Cina; chiede ulteriori proposte intese ad assicurare che le catene di produzione e di approvvigionamento delle infrastrutture e dei materiali critici rimangano all'interno dell'UE;

13. invita la Commissione a proporre un nuovo quadro legislativo per attenuare i rischi per la sicurezza derivanti dai fornitori di sistemi via cavo sottomarini; sottolinea la necessità di impedire ai fornitori di sistemi via cavo, come le imprese cinesi, di condividere i dati

con servizi di intelligence con finalità diverse da quella di proteggere l'infrastruttura da intrusioni esterne o attacchi malevoli;

Nesso tra sicurezza interna ed esterna: rafforzare la resilienza dei partner più stretti dell'UE

14. è consapevole della penetrazione della Repubblica popolare cinese nel mercato e nel grande vicinato dell'UE; invita la Commissione e il Servizio europeo per l'azione esterna (SEAE) a provvedere affinché le misure adottate per rafforzare la resilienza dell'UE di fronte all'influenza cinese siano estese anche ai partner più stretti dell'UE, in particolare ai paesi in via di adesione e a quelli che beneficiano della politica di vicinato dell'UE;

15. ricorda che le forze navali della Repubblica popolare cinese dispongono di strumenti giuridici per garantire che le navi e le infrastrutture civili cinesi possano essere utilizzate a scopi militari e di sicurezza; ritiene che la Cina possa utilizzare le sue infrastrutture commerciali civili per sostenere la presenza dell'esercito popolare di liberazione nei paesi terzi; avverte che la fusione militare-civile fornisce all'esercito popolare di liberazione l'accesso a porti stranieri, consentendogli di preposizionare il supporto logistico per sostenere gli schieramenti navali fino all'Oceano Indiano, al Mar Mediterraneo e all'Oceano Atlantico; sottolinea che i rischi di spionaggio sono più elevati quando le attività commerciali civili cinesi sono dislocate in poli logistici vicini alle basi navali dell'UE e della NATO o agli operatori portuali che hanno firmato accordi per fornire supporto logistico alle imprese europee;

16. osserva che un terzo di tutte le infrastrutture africane costruite dopo il 2010 è stato finanziato e costruito da imprese statali cinesi; sottolinea che, negli ultimi 20 anni, la Cina ha aumentato i propri impegni commerciali, di investimento e di prestito con obblighi contrattuali scarsi o non trasparenti; esprime preoccupazione per il fatto che questo modello cinese è chiaramente attraente per molti paesi che non possono soddisfare i requisiti dell'UE per accedere a livelli di finanziamento equivalenti, ampliando così l'influenza cinese a scapito dei partenariati dell'UE; invita la Commissione e il SEAE a provvedere affinché le norme rigorose dell'UE in materia di investimenti con i partner non ne compromettano le relazioni e l'impegno in materia di sicurezza in quanto partner affidabile e strategico;

17. sottolinea con preoccupazione la strategia della Repubblica popolare cinese volta a costruire una "base di cooperazione per l'economia blu" lungo le coste africane, anche attraverso la costruzione di pescherecci e strutture per la riparazione delle imbarcazioni che possono essere utilizzate anche per scopi militari; sottolinea che vi è una generale mancanza di dettagli e di trasparenza riguardo a tali accordi e licenze con i paesi africani; evidenzia le potenziali conseguenze geopolitiche per l'UE, in particolare nei paesi terzi in cui l'UE è impegnata;

°

° °

18. incarica la sua Presidente di trasmettere la presente risoluzione al vicepresidente della Commissione / alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, al Consiglio e alla Commissione.