Consiglio dell'Unione europea

**Bruxelles, 3 dicembre 2025**
**(OR. en)**

**16389/25**

**POLCOM 368**
**FDI 58**
**COMER 182**
**RECH 543**
**TELECOM 457**
**COMPET 1297**
**DUAL USE 58**
**RELEX 1623**
**ENER 647**
**ENV 1330**
**IND 580**
**INDEF 179**
**CYBER 364**
**PROCIV 176**

**NOTA DI TRASMISSIONE**

| | |
|---|---|
| Origine: | Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice |
| Data: | 3 dicembre 2025 |
| Destinatario: | Thérèse BLANCHET, segretaria generale del Consiglio dell'Unione europea |
| Oggetto: | COMUNICAZIONE CONGIUNTA AL PARLAMENTO EUROPEO E AL CONSIGLIO<br>Rafforzare la sicurezza economica dell'UE |

Si trasmette in allegato, per le delegazioni, il documento JOIN(2025) 977 final.

All.: JOIN(2025) 977 final

COMMISSIONE
EUROPEA

ALTO RAPPRESENTANTE
DELL'UNIONE PER
GLI AFFARI ESTERI E
LA POLITICA DI SICUREZZA

Bruxelles, 3.12.2025
JOIN(2025) 977 final

# COMUNICAZIONE CONGIUNTA AL PARLAMENTO EUROPEO E AL CONSIGLIO

## Rafforzare la sicurezza economica dell'UE

## *1. Introduzione*

L'uso sempre più frequente e mirato di **strumenti economici per promuovere obiettivi strategici** è diventato una caratteristica distintiva del panorama geopolitico attuale. Dai dazi destabilizzanti alla strumentalizzazione delle dipendenze fino all'applicazione arbitraria di misure di difesa commerciale, i principali soggetti coinvolti utilizzano leve economiche per perseguire i loro obiettivi strategici e geopolitici, mettendo a rischio la sicurezza, l'ordine pubblico, la competitività e l'economia dell'UE.

I rischi per la sicurezza economica dell'UE non sono nuovi, ma si sono recentemente intensificati: le vulnerabilità sono ora più visibili, più pressanti e più difficili da ignorare. Tra tali rischi figurano:

- una crescente **instabilità nel contesto globale del commercio e degli investimenti**, caratterizzata dall'aumento di misure commerciali perturbanti e di restrizioni alle esportazioni volte a strumentalizzare le dipendenze;
- una proliferazione di **pratiche predatorie** che prendono di mira le catene di approvvigionamento e le tecnologie critiche, compromettendo la nostra base industriale, alcune delle quali (come le sovraccapacità finanziate dallo Stato) creano nuove dipendenze;
- il continuo deterioramento del panorama della sicurezza, anche nel contesto del protrarsi della **guerra di aggressione** della Russia **nei confronti dell'Ucraina** e dell'aumento degli attacchi ibridi.

La **strategia europea per la sicurezza economica** del 2023 ha definito la risposta iniziale dell'UE a tali sfide[1]. Ha delineato una serie di azioni, basate su valutazioni dei rischi, volte a rafforzare la sicurezza economica dell'UE attraverso la **promozione** della competitività, la **protezione** dai rischi e **partenariati** con attori che condividono le nostre preoccupazioni. Tali tre pilastri rimangono al centro del nostro approccio alla sicurezza economica e la Commissione, unitamente agli Stati membri, si adopera per integrarli in qualsiasi considerazione e azione a livello di politiche. Inoltre la sicurezza economica è essenziale affinché l'UE mantenga i suoi valori, i suoi principi e il benessere dei suoi cittadini, nonché al fine di rafforzare la nostra indipendenza economica.

Tuttavia, dall'adozione della strategia del 2023, la necessità che l'UE agisca con maggiore coraggio, rapidità e unità è diventata ancora più impellente. La presente comunicazione delinea un uso più strategico e assertivo degli strumenti dell'Unione, a integrazione degli obiettivi strategici originari, al fine di sostenere la sicurezza economica dell'Europa, che riguarda la capacità dell'Unione di garantire la sicurezza, insieme ad altri obiettivi, attraverso un'economia forte, dinamica e resiliente, anticipando, scoraggiando e rispondendo a minacce potenziali o effettive legate alle relazioni economiche dell'UE con il resto del mondo. L'UE può conseguire tale obiettivo, in particolare assicurandosi di rimanere all'avanguardia in termini di tecnologie, industrie e servizi critici. Ciò rispecchia un **cambiamento di paradigma**, che comporta il passaggio da una posizione reattiva a un utilizzo più proattivo e

[1] JOIN(2023) 20 final.

sistematico del nostro pacchetto di strumenti. Inoltre, in alcuni casi, l'UE, i suoi Stati membri e l'industria dovranno essere sempre più pronti ad accettare i costi economici a vantaggio di una riduzione delle vulnerabilità e di una maggiore sicurezza complessiva.

Tale invito ad agire contempla il **miglioramento** della raccolta, del monitoraggio e dell'analisi delle informazioni, nonché della capacità di anticipare le minacce emergenti; il **dissuadere** paesi terzi dall'utilizzare le dipendenze dell'Unione come arma; la **riduzione** della nostra esposizione nei confronti di paesi terzi che potrebbero strumentalizzare tali dipendenze; e la **prevenzione** di tentativi di minare le nostre azioni di riduzione dei rischi.

È importante sottolineare che il presente invito ad agire riconosce altresì la necessità di **sfruttare i punti di forza dell'UE** in termini, tra l'altro, di peso senza precedenti del mercato unico dell'UE, delle nostre capacità tecnologiche e industriali e dell'accesso ai finanziamenti e ai programmi dell'UE. Figurano in questo contesto l'individuazione delle opportunità economiche dell'UE e dei settori in cui altri dipendono dall'UE. La presente comunicazione invoca pertanto un **approccio integrato esteso a tutta l'amministrazione e alle imprese**, **una migliore governance** nonché **una cooperazione ancora più stretta con partner che condividono gli stessi principi e, se del caso, un'azione congiunta.** Il presente documento è complementare alla strategia globale dell'UE per l'Unione della preparazione. La sicurezza economica dell'UE è sostenuta da quella dei suoi Stati membri ed è inoltre intrinsecamente legata alle sue relazioni di più ampio respiro con il mondo e, pertanto, alla politica estera e di sicurezza comune, che sarà utilizzata in modo più sistematico per sostenere gli obiettivi dichiarati.

Su questi presupposti, ancorata a un'analisi basata sui rischi, la presente comunicazione si concentra sui sei settori ad alto rischio delineati nella sezione 3, applica gli strumenti a nostra disposizione e illustra il modo in cui questi ultimi possono essere ulteriormente migliorati.

## *2. Un approccio proattivo alla sicurezza economica*

L'UE dispone di un'ampia serie di strumenti che contribuiscono alla sua sicurezza economica. Per rafforzare quest'ultima, è ora necessario che li utilizzi in modo **più strategico, efficiente e proattivo**. Sebbene non sia stata originariamente sviluppata tenendo conto della sicurezza economica, la maggior parte di questi strumenti è tuttavia estremamente pertinente al fine di compiere progressi in relazione agli obiettivi di sicurezza economica dell'Unione.

Un elenco non esaustivo degli strumenti chiave è riportato nella *figura 1* e la loro applicazione coordinata è ulteriormente illustrata nella *sezione 3*.

*Figura 1- Elenco non esaustivo degli strumenti a sostegno della sicurezza economica*


Al fine di promuovere la sicurezza economica dell'UE, la Commissione utilizzerà tali strumenti, in coordinamento con gli Stati membri, come segue:

- gli **strumenti in materia di commercio e concorrenza** saranno utilizzati al fine di ridurre gradualmente l'esposizione dell'UE ai rischi ed evitare che gli obiettivi di riduzione dei rischi dell'UE siano compromessi. Figurano in questo contesto l'ampliamento delle opportunità di diversificazione e quindi la nostra sicurezza in senso più ampio nell'ambito degli accordi commerciali dell'UE, un uso strategico del pacchetto di strumenti in materia doganale e la lotta alle distorsioni causate da sovvenzioni estere, tanto all'interno del mercato unico quanto in relazione a importazioni sovvenzionate o oggetto di dumping;
- gli strumenti in materia di **resilienza e cibersicurezza** si concentreranno sulla preparazione alle situazioni di emergenza e sulla loro gestione, nonché sulla riduzione dell'esposizione alle minacce esterne, quali le minacce informatiche;

- gli **strumenti in materia di sicurezza e ordine pubblico** saranno utilizzati al fine di ridurre l'esposizione eccessiva dell'UE ai rischi, tra l'altro, per garantire il normale funzionamento della società, sostenendo nel contempo azioni volte a sviluppare la sua posizione in termini di tecnologie e industrie critiche e a evitare che i suoi obiettivi di riduzione dei rischi siano compromessi;
- le **misure anticoercizione e restrittive** mireranno a scoraggiare e ad affrontare le situazioni in cui paesi terzi tentano di attuare azioni di coercizione nei confronti dell'UE, nonché a proteggere le imprese dell'UE da misure extraterritoriali imposte da paesi terzi e, se del caso, a innescare un cambiamento di comportamento del paese interessato;
- **i finanziamenti e le restrizioni** attraverso strumenti dell'UE quali lo strumento di vicinato, cooperazione allo sviluppo e cooperazione internazionale (Global Gateway), Orizzonte Europa, NextGenerationEU, InvestEU, il programma Europa digitale, il meccanismo per collegare l'Europa, gli strumenti di assistenza preadesione (IPA), i piani di crescita per i Balcani occidentali e la Moldova, nonché lo strumento per l'Ucraina, EU4Health e il futuro Fondo europeo per la competitività dovrebbero rafforzare la sicurezza economica dell'UE o, come minimo, non indebolirla, in linea con le norme dei programmi;
- **iniziative settoriali** saranno invece utilizzate per sviluppare le capacità e le competenze strategiche proprie dell'UE nei settori ad alto rischio individuati nel processo di valutazione dei rischi.

Una stretta cooperazione e uno stretto coordinamento con i paesi che attribuiscono un'importanza analoga alla sicurezza economica e a un ordine mondiale basato su regole sono più importanti che mai. L'UE si adopererà per rafforzare la **cooperazione internazionale in merito a questioni di sicurezza economica**, in particolare con **partner fidati**, anche attraverso **dialoghi mirati sulla sicurezza economica condotti sia a livello bilaterale che in contesti plurilaterali**. Tale cooperazione sosterrà un'azione congiunta in merito a interessi o preoccupazioni comuni in materia di sicurezza economica. Approfondirà inoltre la comprensione collettiva dei rischi, contribuirà ad anticipare le minacce, consentirà l'elaborazione di misure di attenuazione volte a **ridurre al minimo le esternalità negative** e contribuirà alla creazione e al mantenimento di catene di approvvigionamento affidabili e resilienti in settori strategici chiave, così come a evitare impatti negativi sui nostri partner internazionali che condividono gli stessi principi.

La Commissione cercherà di cooperare con paesi terzi, a livello bilaterale, attraverso il G7 e in contesti quali

***Diffusione di norme in materia di sicurezza economica***

Traendo spunto dai lavori del G7 in materia di commercio basato su norme, la Commissione incoraggerà lo sviluppo e l'impiego di norme in materia di sicurezza economica. Tali norme saranno:

→ incentrate su azioni volte a diversificare le catene di approvvigionamento critiche creando le condizioni per l'ingresso di nuovi fornitori nel mercato o limitando l'accesso da parte dei fornitori dominanti;

→ guidate dai principi di trasparenza, interoperabilità e conformità rispetto alle norme internazionali;

→ mirate e ad hoc, tenendo conto dei rischi specifici, degli impatti economici e delle realtà commerciali di ciascuna catena di approvvigionamento.

I lavori si concentreranno in via prioritaria sulle materie prime critiche e sulle catene di approvvigionamento dei semiconduttori, esplorando nel contempo ulteriori opportunità di collaborazione in altri settori.

l'accordo globale e progressivo di partenariato transpacifico e altri consessi pertinenti. Collaborerà con i partner allo sviluppo e alla diffusione di norme in materia di sicurezza economica per catene di approvvigionamento resilienti. Nel contesto di una cooperazione più stretta può figurare l'**impiego coordinato di strumenti** e la creazione di coalizioni con partner che condividono obiettivi di sicurezza economica analoghi o si trovano ad affrontare sfide simili.

Occorre inoltre tenere adeguatamente conto della pertinenza della **politica di vicinato e di allargamento** dell'UE e dell'incidenza sulla stessa. I rischi e le opportunità per la sicurezza economica dell'UE saranno integrati nell'attuazione, da parte della Commissione, delle politiche e dei programmi che coinvolgono tali regioni. I paesi candidati sono sulla buona strada per diventare futuri Stati membri dell'UE. Il loro allineamento alla politica di sicurezza economica e la loro graduale integrazione nel mercato unico sono essenziali al fine di garantire un'adesione riuscita, rafforzando nel contempo la capacità dell'UE di affrontare i rischi esistenti così come quelli nuovi. Di conseguenza è importante che i paesi candidati rispecchino l'approccio dell'UE in materia di sicurezza economica e, se del caso, si allineino gradualmente alla legislazione dell'UE pertinente per gli obiettivi di sicurezza economica.

## ***3. Compiere progressi in relazione alla sicurezza economica dell'Europa: settori ad alto rischio***

La strategia del 2023 ha avviato valutazioni dei rischi riguardanti la resilienza delle catene di approvvigionamento e la sicurezza energetica, le infrastrutture critiche, la strumentalizzazione delle dipendenze economiche, la sicurezza tecnologica e la fuga di tecnologie. Quattro tecnologie critiche (intelligenza artificiale, tecnologie quantistiche, semiconduttori e biotecnologie) sono già state valutate. Sulla base di tale lavoro, la Commissione ha individuato **sei settori ad alto rischio** nei quali concentrerà i propri sforzi nell'immediato e a breve termine, in stretta collaborazione con gli Stati membri, l'industria e partner fidati. Allo stesso tempo, la Commissione continuerà a monitorare gli sviluppi e, ove necessario, a valutare i nuovi settori ad alto rischio emergenti e ad intervenire in tali settori.

**Panoramica dei sei settori ad alto rischio**

3.1. Rafforzare la resilienza delle catene di approvvigionamento e contrastare le dipendenze ad alto rischio da beni e servizi critici

**Indicatori non cumulativi di dipendenza ad alto rischio:**
*- il 60 % o oltre dell'approvvigionamento dell'UE è controllato da un unico paese terzo o da operatori di un unico paese terzo;*
*- i fattori produttivi/servizi hanno un valore sistemico per l'economia dell'UE in ragione del loro ruolo in molteplici settori, ad esempio in quelli delle materie prime critiche e dei semiconduttori;*
*- i fattori produttivi/servizi sono fondamentali per l'industria della difesa/le capacità strategiche dell'UE o per catene di approvvigionamento di tecnologie critiche specifiche, quali le tecnologie per l'energia pulita;*
*- il paese terzo ha già strumentalizzato o minacciato di strumentalizzare le dipendenze economiche, ad esempio attraverso restrizioni all'esportazione;*
*- esiste già una sovraccapacità non di mercato o la stessa è in fase di creazione.*

**Il rischio.** Le economie moderne sono profondamente interconnesse e dipendono da un'ampia gamma di fattori produttivi, beni intermedi e servizi essenziali forniti dai partner a livello mondiale. In alcuni casi l'offerta è altamente concentrata, spesso in paesi che non condividono gli stessi interessi strategici e che hanno la capacità e la volontà di intensificare e strumentalizzare tali dipendenze. Tali rischi per le catene di approvvigionamento dell'UE sono particolarmente evidenti nella nostra dipendenza da **materie prime critiche, materiali trasformati e avanzati, componenti di tecnologie pulite** specifici e da **semiconduttori tradizionali**, nonché nei settori dei **servizi finanziari,** dei **prodotti farmaceutici,** dell'**aeronautica** e delle **tecnologie digitali e spaziali**. Sono rilevabili altresì nel **settore agroalimentare**, nel contesto del quale la visione per l'agricoltura e l'alimentazione[2] sottolinea la necessità di ridurre le dipendenze strategiche, in particolare quando l'UE dipende da un numero limitato di partner per le importazioni di mangimi, additivi per mangimi e concimi.

Le dipendenze ad alto rischio possono: i) essere **strumentalizzate** per fini coercitivi (ad esempio materie prime critiche, semiconduttori tradizionali, materiali avanzati, prodotti energetici, minacce di disabilitazione di determinati servizi); ii) creare una **vulnerabilità economica sistemica** o un rischio sistemico per l'ordine pubblico e la protezione della salute pubblica in caso di crisi (ad esempio dispositivi di protezione individuale, approvvigionamento di medicinali critici, forniture alimentari); iii) creare il rischio di perturbazioni intersettoriali su vasta scala (ad esempio penetrazione nelle reti di

***Esempio di applicazione: semiconduttori tradizionali***

**Rischio**: la dipendenza strutturale da un unico fornitore di un paese terzo per la fabbricazione di chip essenziali a basso margine mette a rischio diverse industrie europee. Tali semiconduttori costituiscono una parte fondamentale di molteplici catene di approvvigionamento.

**Uso di strumenti**: la Commissione collaborerà con partner fidati al fine di diversificare le fonti di approvvigionamento e cercherà di incoraggiare un'intensificazione della produzione all'interno dell'UE. L'imminente revisione del regolamento sui chip stabilirà misure efficaci di attenuazione. La cibersicurezza dei semiconduttori tradizionali importati utilizzati in applicazioni connesse alla sicurezza dovrebbe essere ulteriormente valutata nel contesto del regolamento sulla ciberresilienza.

[2] COM(2024) 75 del 19 febbraio 2025.

telecomunicazione, affidamento su un unico fornitore di servizi cloud, messa fuori uso di servizi digitali); iv) **incidere sulla competitività dell'UE, rallentando le transizioni verde e digitale** in caso di interruzione dell'approvvigionamento (ad esempio batterie, magneti permanenti, prodotti e componenti delle tecnologie pulite, materiali avanzati); v) incidere sull'autonomia degli Stati membri nello sviluppo e nell'impiego di **capacità militari**; o vi) minacciare la sovranità alimentare dell'UE.

**Obiettivo.** La Commissione e gli Stati membri cercheranno di **ridurre al minimo il potenziale di perturbazioni a breve termine**, mettendo nel contempo in atto misure volte a **ridurre progressivamente le attuali dipendenze ad alto rischio presenti nel mercato unico e a contrastare i tentativi di crearne di nuove**. Utilizzerà i suoi strumenti per monitorare la catena di approvvigionamento, creare un quadro per sostenere la diversificazione dell'approvvigionamento e prevenire l'indebolimento dell'azione dell'UE affrontando le distorsioni della concorrenza nel mercato unico. Anche le azioni nel contesto della transizione verso l'economia circolare svolgeranno un ruolo importante.

La Commissione adotterà le misure necessarie per garantire che le sue catene di approvvigionamento alternative non siano compromesse da pratiche di dumping e manipolazione dei prezzi.

La Commissione fornirà assistenza agli Stati membri nell'utilizzo completo ed efficace degli strumenti esistenti, in particolare i criteri di resilienza che dovranno essere applicati dagli Stati membri a partire da gennaio 2026 negli appalti pubblici, nelle aste e nei regimi di sostegno pubblico nel contesto del regolamento sull'industria a zero emissioni nette.

La Commissione adotterà inoltre misure volte a sviluppare **la capacità e le competenze interne dell'UE** e a diversificare l'approvvigionamento **attraverso la cooperazione con i partner, anche basandosi sulla sua vasta rete di accordi commerciali e su altre forme bilaterali e plurilaterali di cooperazione**. Figureranno in questo contesto la considerazione della produzione di determinati prodotti critici nei paesi candidati e nei nostri paesi partner più in generale, anche con regioni quali il Medio Oriente e il Nord Africa. Ciò rafforzerà la resilienza delle catene di approvvigionamento diversificate dell'UE e offrirà ulteriori opportunità alle imprese dell'UE. La Commissione continuerà a individuare e a monitorare costantemente le vulnerabilità delle catene di approvvigionamento e le **dipendenze ad alto rischio** attraverso il suo processo di valutazione dei rischi e il dialogo con gli Stati membri e l'industria.

3.2. Attrarre investimenti in entrata a valore aggiunto che rafforzino la sicurezza economica dell'UE

**Il rischio.** Gli investimenti in entrata rafforzano la resilienza e la competitività dell'UE creando posti di lavoro, sviluppando le capacità industriali, facendo leva sui finanziamenti e sulla dimensione di scala, sostenendo l'innovazione e il trasferimento di tecnologie. Tuttavia talune forme di investimenti in entrata possono comportare rischi, tra i quali figurano: i) i rischi relativi a **sicurezza e ordine pubblico**, compreso l'accesso a dati sensibili (ad esempio geolocalizzazione, dati biometrici, segreti commerciali), l'accesso a infrastrutture critiche, l'accesso a tecnologie a duplice uso e ad altre tecnologie critiche; e ii) i **rischi relativi alla**

**resilienza economica**, quali dipendenze più profonde o un singolo punto di vulnerabilità nelle catene di approvvigionamento critiche controllato da soggetti ad alto rischio o da paesi terzi che compromettono i nostri interessi in materia di sicurezza economica (ad esempio batterie, materie prime critiche, software e componenti), che rendono l'UE vulnerabile alle perturbazioni economiche o alla strumentalizzazione; e iii) **sfide in termini di bassa competitività**, quali la mancanza di trasferimento tecnologico, la limitata creazione di valore aggiunto (ad esempio solo linee di assemblaggio), l'assunzione di lavoratori dal paese che investe e quindi l'impatto, tra l'altro, sul mercato del lavoro locale.

**Obiettivo.** La Commissione si concentrerà sulla necessità di garantire che l'UE rimanga aperta agli investimenti esteri e attraente per gli stessi. Cercherà di trovare un equilibrio tra tale apertura, ove necessario ai fini della sicurezza economica dell'UE, e la necessità di evitare di aggravare le dipendenze o di crearne di nuove. È inoltre fondamentale preservare la capacità di innovazione delle imprese dell'UE, anche attraverso l'acquisizione estera di proprietà intellettuale chiave da leader emergenti, e garantire la sicurezza dell'approvvigionamento e la continuità del servizio. La Commissione utilizzerà i propri strumenti e le proprie iniziative per definire e attuare misure mirate, quali l'imposizione di condizioni per gli investimenti in entrata, che incoraggino il trasferimento di tecnologie per i soggetti siti in paesi che compromettono deliberatamente la nostra sicurezza economica.

***Esempio: veicoli elettrici a batteria***

**Rischio:** la posizione dominante di determinati fornitori di veicoli elettrici a batteria e lo stretto controllo sulle tecnologie necessarie per la produzione di tali veicoli rischiano di compromettere il ruolo chiave del settore automobilistico nell'economia dell'UE, mentre tali fornitori traggono vantaggio dal mercato dell'UE. Vi sono inoltre rischi intrinseci in termini di cibersicurezza associati ai veicoli connessi.

**Uso di strumenti**: la Commissione sta valutando le modalità per incoraggiare investimenti a valore aggiunto, anche attraverso il ricorso a iniziative in materia di politica commerciale e di concorrenza. Continuerà inoltre a monitorare i flussi commerciali e a utilizzare il suo pacchetto di strumenti di attenuazione dei rischi per ridurre i rischi degli elementi di connettività, sostenere gli investimenti nella prossima generazione di tecnologie per veicoli elettrici a batteria affinché l'Europa rimanga resiliente e competitiva e, ove necessario, limitare l'esposizione a soggetti ad alto rischio in relazione ai pertinenti componenti connessi dei veicoli elettrici a batteria. La Commissione incentiverà inoltre la condivisione della tecnologia e del relativo know-how in grado di rafforzare gli obiettivi di sicurezza economica dell'UE.

3.3. Sostenere una base industriale vivace della difesa e dello spazio e altri settori industriali ad alto rischio

**Il rischio.** La guerra di aggressione della Russia nei confronti dell'Ucraina, le crescenti tensioni geopolitiche e l'azione politica volta a strumentalizzare le dipendenze commerciali evidenziano l'importanza di investire in una vivace base industriale interna, in particolare nei settori della difesa e dello spazio, nonché in settori strategici a duplice uso, quali i trasporti (ad esempio l'aviazione, l'aeronautica, la cantieristica navale e i porti), quindi in una base industriale che alimenta l'economia dell'UE e ne sostiene l'autonomia strategica. Tra i rischi in questo settore figurano: i) investimenti (interni) insufficienti; ii) bassi volumi di produzione associati a un approvvigionamento insufficiente di tecnologia nazionale per infrastrutture istituzionali; iii) politiche e pratiche non di mercato di paesi terzi che comportano distorsioni

sui mercati globali e regionali; iv) controlli sulle esportazioni ingiustificati o sproporzionati imposti da paesi terzi su prodotti e tecnologie europei (extraterritorialità dei regimi di esportazione dei paesi terzi); v) perdita della proprietà e del controllo a causa di acquisizioni estere, anche, in alcuni casi, attraverso acquisizioni di portafoglio; vi) un quadro normativo rigido e mercati dei capitali frammentati che non agevolano il flusso di fondi né promuovono le start-up e le scale-up attive nel settore delle tecnologie ad alto rischio/ad alto rendimento con capacità a duplice uso.

***Esempio di applicazione: componenti chiave per droni e sistemi antidrone***

**Rischio**: dipendenza da fornitori di paesi terzi per componenti chiave di droni, batterie e sistemi antidrone; ciclo di innovazione estremamente breve al fine di mantenere l'efficacia operativa delle soluzioni basate su droni, sulla base di una effettiva esperienza sul campo di battaglia (misurato in mesi, talvolta in settimane).

**Uso di strumenti**: la Commissione utilizzerà i propri strumenti nell'ambito dei programmi industriali europei nel settore della difesa al fine di garantire la capacità produttiva nell'UE e l'accorciamento dei cicli di innovazione per le tecnologie relative ai droni sulla base di una effettiva esperienza operativa. Continuerà a rafforzare la cooperazione e lo scambio di informazioni su base volontaria tra gli organismi pertinenti (ad esempio agenzie nazionali per gli appalti, organizzazioni internazionali per gli appalti - Organizzazione congiunta per la cooperazione in materia di armamenti (OCCAR), Agenzia europea per la difesa (AED), NATO) e nell'ambito degli strumenti/delle azioni dei programmi per l'industria europea della difesa. Al fine di garantire la resilienza delle catene di approvvigionamento, stabilirà una mappatura mirata delle catene di approvvigionamento per prodotti e attrezzature specifici, compresi i prodotti a duplice uso, e sosterrà la produzione attraverso coinvestimenti.

Taluni componenti in settori critici quali la difesa provengono da soggetti ad alto rischio, il che potrebbe impedire l'accesso e l'uso di **materiale di difesa, tecnologie a duplice uso e mezzi di mobilità militare** in caso di situazioni di tensione geopolitica. Inoltre è fondamentale che l'UE mantenga una forza lavoro altamente qualificata e non rimanga indietro rispetto alla curva dell'innovazione nelle tecnologie alla base di settori strategici. Attenuare in maniera proficua tali rischi mobilitando rapidamente strumenti mirati ed efficaci è essenziale per le capacità militari e di difesa nell'UE.

**Obiettivo.** La Commissione utilizzerà i suoi strumenti per mantenere e sviluppare capacità e competenze di produzione strategiche nell'UE, in particolare: i) promuovendo **investimenti** pubblici e privati e, se del caso, riducendo i rischi a essi associati; ii) **sostenendo la domanda** (incentivi) anche attraverso l'aggregazione o l'acquisto in comune; iii) **impedendo la ricollocazione** di capacità e settori strategici; iv) **eliminando gradualmente i soggetti potenzialmente ostili** dal settore della difesa e da altre catene di approvvigionamento critiche, anche limitando l'approvvigionamento di tecnologie critiche di difesa e spaziali soggette a restrizioni da paesi terzi; v) attenuando le **minacce poste dagli investimenti esteri diretti** nelle imprese che forniscono prodotti o tecnologie critici; vi) **sostenendo lo sviluppo di tecnologie, componenti e materiali critici** nell'UE secondo obiettivi a lungo termine, nonché gli appalti nazionali per tali risorse per le infrastrutture istituzionali; vii) garantendo che **le start-up e le** altre **imprese** dell'UE dispongano delle condizioni necessarie per espandersi, ad

esempio attraverso finanziamenti adeguati e un trattamento tariffario favorevole temporaneo per determinati fattori produttivi, nonché un ecosistema favorevole dei mercati dei capitali.

La priorità sarà sostenere la **base industriale della difesa e dello spazio**. Sebbene l'attenzione immediata si concentrerà sulle specifiche situazioni ad alto rischio individuate nel contesto del processo di valutazione dei rischi, la Commissione monitorerà attentamente, dal punto di vista della sicurezza economica, tutti i settori chiave quali quelli delle tecnologie pulite, dell'energia e delle industrie circolari e ad alta intensità energetica, dell'agroalimentare, del digitale e dell'elettronica, dell'aviazione (compresa l'aeronautica), della cantieristica navale, dell'industria automobilistica e della sanità.

3.4. Sviluppare e mantenere la leadership in tutte le tecnologie critiche

**Il rischio.** Taluni paesi terzi e talune imprese hanno dimostrato interesse ad acquisire il controllo della tecnologia e del know-how nascenti o avanzati dell'UE. In alcuni casi, azioni di questo tipo sono state volte a compromettere la capacità dell'Unione di competere nel settore della tecnologia in questione. Tali azioni perseguono detto obiettivo, ad esempio, mediante acquisizioni, cooperazione in materia di ricerca e sviluppo, ingegneria inversa o spionaggio industriale. Ciò avviene anche sottraendo artificiosamente quote di mercato alle imprese più innovative, il che a sua volta si traduce in minori entrate a disposizione di tali imprese per investimenti in attività di ricerca e sviluppo all'avanguardia. Nel lungo termine, i risultati economici, la sicurezza e la posizione geopolitica dell'UE dipenderanno dal mantenimento e dallo sviluppo delle nostre capacità tecnologiche. Di conseguenza è di importanza strategica preservare le capacità dell'UE in tutte queste tecnologie, rafforzando gli appositi strumenti di finanziamento dell'UE e affrontando la sicurezza tecnologica e la fuga di tecnologie. Allo stesso tempo, occorre prestare particolare attenzione all'attuazione e all'applicazione sempre più frammentate dei controlli delle esportazioni di prodotti a duplice uso.

***Esempio di applicazione: tecnologie quantistiche***

**Rischio**: soggetti stranieri sostenuti dallo Stato o ad alto rischio cercano di accedere al calcolo quantistico, alla comunicazione quantistica e al know-how e alle infrastrutture di rilevamento quantistico dell'UE attraverso investimenti, acquisizioni o partenariati in materia di ricerca e sviluppo, accelerando usi militari/di intelligence sensibili all'estero ed erodendo la sovranità tecnologica dell'UE.

**Uso di strumenti**: la Commissione continuerà a mappare i principali soggetti/le principali infrastrutture del settore delle tecnologie quantistiche dell'UE e a monitorare gli investimenti esteri, i partenariati e i flussi di proprietà intellettuale al fine di alimentare il controllo degli investimenti esteri diretti, il controllo delle esportazioni e le valutazioni dei rischi per la sicurezza della ricerca. Utilizzerà i propri strumenti per indagare in merito a investimenti che comportano rischi e per collaborare con gli Stati membri al fine di coordinare risposte rapide a tentativi di acquisizioni ostili o a casi di fughe di informazioni. Al fine di sostenere gli obiettivi di sicurezza economica, per ciò che attiene ai componenti e ai servizi quantistici critici darà priorità ai finanziamenti e ai fornitori dell'UE o che condividono gli stessi principi, e limiterà la dipendenza da fornitori quantistici/cloud ad alto rischio in settori sensibili. Cercherà inoltre di garantire che i soggetti sottoposti a un'indebita influenza straniera non possano accedere a progetti quantistici sensibili.

**Obiettivo.** La Commissione utilizzerà i propri strumenti per sostenere un contesto quadro positivo per lo sviluppo di tecnologie critiche nell'UE e prevenire azioni che compromettono gli sforzi dell'UE affrontando le distorsioni. Monitorerà gli sviluppi del mercato e fornirà ulteriore sostegno alla ricerca e all'innovazione nell'UE da parte di start-up e scale-up, imprese consolidate, organizzazioni di ricerca e innovazione e da parte del mondo accademico. Si concentrerà sul garantire la diffusione industriale e la valorizzazione dei risultati in materia di ricerca, sviluppo e innovazione nel contesto della base industriale del mercato unico. Il 28º regime, che fornisce alle imprese un unico corpus di norme armonizzato a livello di UE per la costituzione di imprese, la governance, la mobilità e l'accesso ai finanziamenti, rafforzerà la resilienza economica dell'UE consentendo operazioni transfrontaliere più sicure e catene di approvvigionamento più solide e diversificate.

La Commissione promuoverà la sicurezza delle attività di ricerca e innovazione e adotterà le misure di accompagnamento necessarie per attenuare il rischio di fuga di tecnologie o know-how, ad esempio attraverso acquisizioni predatorie, la cooperazione in materia di ricerca e sviluppo e gli investimenti nei mercati strategici ed emergenti dell'UE in relazione a destinazioni o settori sensibili, continuando nel contempo a promuovere partenariati internazionali fidati per la ricerca e l'innovazione che sono fondamentali per gli obiettivi di sicurezza economica dell'Unione. Esaminerà come garantire che le imprese e le organizzazioni di ricerca e innovazione nell'UE possano espandersi ed evitare acquisizioni/trasferimenti di proprietà dovuti esclusivamente a opportunità di finanziamento insufficienti da fonti fidate. Allo stesso tempo, la Commissione cercherà di impedire l'accesso di soggetti ad alto rischio alle azioni sostenute dall'Unione nel settore delle tecnologie critiche, che potrebbero essere strumentalizzate contro l'UE.

***Esempio: apparecchiature di rilevamento presso le frontiere dell'UE (porti, aeroporti, frontiere terrestri, ecc.)***

**Rischio**: mancanza di prassi comuni in tutta l'UE, dipendenza da un unico fornitore o da un numero limitato di fornitori, accesso non autorizzato (anche attraverso canali autorizzati, ad esempio la manutenzione) che incide sulle prestazioni delle apparecchiature di rilevamento e sull'integrità e/o sulla riservatezza delle relative informazioni sensibili, vulnerabilità ai malware che potrebbe compromettere le relative informazioni, i relativi sistemi o le relative reti oppure creare distorsioni in tali contesti attraverso le apparecchiature in questione.

**Uso di strumenti**: sulla base della valutazione del rischio di cibersicurezza a norma della direttiva NIS2, la Commissione cercherà di attenuare i rischi rilevati attraverso l'individuazione di fornitori ad alto rischio, il ricorso a sistemi di certificazione della cibersicurezza, il rafforzamento delle norme in materia di cibersicurezza e l'integrazione di requisiti di sicurezza nelle gare d'appalto. La Commissione valuterà il ruolo potenziale delle sovvenzioni estere nel conferire un vantaggio competitivo a determinati fornitori.

3.5. Impedire l'accesso a informazioni e dati sensibili che potrebbero compromettere la sicurezza economica dell'UE

**Il rischio.** Paesi terzi ottengono accesso a informazioni/dati sensibili dell'UE o dei suoi Stati membri a seguito di attività di spionaggio industriale, della loro fornitura di hardware o software utilizzati in determinati prodotti (ad esempio veicoli connessi, 5G/altri sistemi di telecomunicazione, infrastrutture delle reti elettriche, piattaforme di sequenziamento del DNA) o a causa della loro proprietà e del loro

controllo di determinate imprese in possesso di informazioni/dati sensibili (ad esempio operatori portuali, aeroportuali e del traffico, reti finanziarie, modelli di intelligenza artificiale, portali di dati, telecomunicazioni, dati personali o informazioni di mercato sensibili). Si rilevano evidenti implicazioni per la sicurezza e l'ordine pubblico, ulteriormente aggravate da potenziali impatti economici, ad esempio legati alla frammentazione delle catene di approvvigionamento. Nel settore dell'energia, ad esempio, tale rischio si estende all'acquisizione da parte di investitori di paesi terzi di imprese dell'UE che detengono tecnologie avanzate per il monitoraggio e il trattamento di dati operativi provenienti da infrastrutture energetiche critiche.

**Obiettivo.** Ridurre e, ove possibile, eliminare il rischio di accesso da parte di soggetti ad alto rischio e di soggetti collegati a informazioni/dati sensibili dell'UE o dei suoi Stati membri, limitando in tal modo potenziali impatti negativi sull'economia e sulla sicurezza dell'UE. Si presterà inoltre attenzione al rischio potenziale rappresentato dai lavoratori stranieri in settori strategici e dagli studenti stranieri coinvolti nell'istruzione superiore, anche nei settori della scienza, della tecnologia, dell'ingegneria e della matematica (STEM), in linea con le procedure pertinenti.

3.6. Prevenire e attenuare le perturbazioni delle infrastrutture critiche dell'UE che incidono sulla sua economia

**Il rischio.** Le infrastrutture critiche dell'UE, comprese le infrastrutture critiche dei trasporti, dei sistemi spaziali, dell'energia e delle comunicazioni, in particolare quelle individuate come strategiche per la mobilità militare, sono perturbate da soggetti stranieri, il che potrebbe comportare effetti a cascata sull'economia europea. L'accento sarà posto sulla garanzia della stabilità dei servizi forniti. Le perturbazioni potrebbero verificarsi attraverso attacchi fisici, informatici o ibridi, compreso il sabotaggio di intere strutture o di loro parti/sottocomponenti. Tali perturbazioni potrebbero inoltre essere collegate alle catene di approvvigionamento delle tecnologie dell'informazione e della comunicazione, che forniscono componenti o servizi critici alla base delle infrastrutture critiche. Vi è inoltre il rischio di preposizionamento di paesi terzi e operatori ad alto rischio nelle infrastrutture critiche dell'UE al fine di ottenere la capacità di perturbarle (quando e se necessario). Inoltre esiste un rischio reputazionale e di credibilità se determinate infrastrutture sono soggette a minacce o vengono effettivamente colpite. Infine vi è il rischio che paesi terzi assumano un ruolo guida nella definizione di norme internazionali, il che può incidere sulle infrastrutture critiche.

*Esempio: invertitori solari*

**Rischio**: crescente dipendenza da un unico fornitore; rischi informatici: manipolazione dei parametri di produzione dell'energia elettrica, impedimento della produzione di energia elettrica, accesso ai dati operativi, infiltrazione tra i soggetti coinvolti nella catena di approvvigionamento.

**Uso di strumenti**: la Commissione continuerà a valutare i rischi informatici attraverso una valutazione coordinata nel quadro della direttiva NIS2 (che si concluderà nel 2026). Su tale base attuerà misure di attenuazione incentrate tanto sul rafforzamento della preparazione (ad esempio il regolamento sulla preparazione ai rischi nel settore dell'energia elettrica e la direttiva sui soggetti critici) quanto sulla gestione delle vulnerabilità individuate, ad esempio attraverso: la certificazione e la normazione nel contesto del regolamento sulla ciberresilienza e criteri diversi dal prezzo nel contesto del regolamento sull'industria a zero emissioni nette. La Commissione monitorerà gli sviluppi del mercato e cercherà di prevenire o attenuare gli investimenti ad alto rischio. La Commissione continuerà a valutare il ruolo delle sovvenzioni estere che possono falsare la parità di condizioni nei mercati dell'energia solare, in particolare attraverso importazioni sovvenzionate.

**Obiettivo.** In linea con le pertinenti strategie dell'UE in materia di difesa, sicurezza interna e preparazione, l'obiettivo consiste nell'applicare le norme esistenti al fine di ridurre il rischio di fuga di dati/spionaggio e di perturbazioni fisiche e informatiche, in particolare: i) **limitando la proprietà/il controllo/la gestione** di infrastrutture critiche europee **da parte di soggetti ad alto rischio**; ii) aumentando le misure di **protezione fisica**; iii) **limitando le vulnerabilità informatiche**; e iv) **limitando le dipendenze da singoli fornitori o da fornitori ad alto rischio**, nonché le vulnerabilità nascoste, gli accessi nascosti (*backdoor*) o le potenziali perturbazioni sistemiche dell'approvvigionamento di tecnologie dell'informazione e della comunicazione, in particolare in caso di dipendenza (*lock-in*) tecnologica o dipendenza da determinati fornitori; v) **riservando le capacità di produzione critiche dell'UE** potenzialmente in grado di espandersi in caso di perturbazioni della catena di approvvigionamento globale o di crisi sanitarie; vi) **facendo sì che** la Commissione **impedisca l'accesso da parte di soggetti ad alto rischio alle azioni sostenute dall'Unione**, comprese quelle sostenute da istituti e strumenti finanziari pubblici; vii) sostenendo lo **sviluppo di fornitori affidabili di sottocomponenti critici** nell'UE e in paesi terzi fidati, affinché vi siano alternative valide; viii) sostenendo **iniziative faro** nel settore della difesa e in settori correlati (sorveglianza del fianco orientale, iniziativa europea di difesa antidrone).

### *4. Azioni volte a rafforzare la sicurezza economica dell'UE*

L'accesso a informazioni di qualità e la loro analisi approfondita costituiscono il punto di partenza per una politica e un processo decisionale dell'UE in materia di sicurezza economica efficaci e ben informati. Il sistema di valutazione dei rischi avviato dalla strategia del 2023 rimarrà al centro di tali sforzi. Le valutazioni esistenti saranno aggiornate, approfondite e integrate da nuove valutazioni in relazione a tutte le tecnologie critiche e alle rispettive catene di approvvigionamento.

La Commissione svilupperà ulteriormente la propria capacità di raccolta di informazioni sulla sicurezza economica. Accelererà la **mappatura delle dipendenze strategiche lungo le catene del valore che comportano vulnerabilità per l'economia dell'Unione** e rafforzerà **il**

**monitoraggio e l'anticipazione delle azioni di paesi terzi** volte a creare nuove dipendenze o a sostenere quelle esistenti.

Inoltre il successo della politica dell'UE in materia di sicurezza economica dipenderà da **un maggiore coordinamento tanto a livello di UE quanto con gli Stati membri**. Figurano in questo contesto la costruzione di una comprensione comune delle minacce alla sicurezza economica, l'individuazione di rischi concreti e lo sviluppo di misure di attenuazione. Ciò dovrebbe essere sostenuto da migliori flussi di informazioni, da una piena comprensione dei costi e dei benefici dell'azione dell'UE e dalla volontà di agire congiuntamente ove necessario, ponendo l'UE in una posizione di forza. La Commissione ha adottato le necessarie misure organizzative interne. Ma ciò richiede anche un modo nuovo di lavorare con gli Stati membri, e in misura sempre maggiore tra gli Stati membri e al loro interno, in particolare per quanto concerne i settori politici che sono sempre più strategici ma che sono stati tradizionalmente decentrati, quali la ricerca e l'innovazione.

L'UE continuerà a dialogare strettamente con l'**industria**, garantendo uno scambio sicuro di informazioni e un impegno più strutturato. L'industria svolge un ruolo di primo piano nel contesto della sicurezza economica dell'UE. Le imprese devono diventare più resilienti e diversificare le loro catene di approvvigionamento critiche, in particolare eliminando completamente la dipendenza da un unico fornitore ad alto rischio. È inoltre fondamentale che integrino nei loro modelli imprenditoriali i costi derivanti da una maggiore diversificazione, riconoscendo i benefici che la resilienza ai rischi geopolitici apporta. Deve trattarsi di un **processo bidirezionale** e di **una responsabilità che deve essere condivisa tra il settore pubblico e quello privato**, consentendo ai responsabili delle politiche di migliorare la capacità di valutazione delle minacce e di intelligence aziendale dell'UE e di dotarla degli strumenti per agire, aiutando nel contempo l'industria a perseguire misure di attenuazione a livello di impresa.

La Commissione, con il sostegno dell'alto rappresentante, intende:

→ migliorare la propria **capacità di raccolta e analisi** delle informazioni portando avanti più rapidamente le valutazioni dei rischi in relazione a specifiche catene di approvvigionamento critiche, infrastrutture critiche e tecnologie critiche e avviando **inviti** periodici **a presentare contributi** al fine di ottenere il contributo dell'industria e dei portatori di interessi in relazione alle vulnerabilità delle catene di approvvigionamento e all'esposizione a pressioni esterne;

→ promuovere **un coordinamento e uno scambio di informazioni** maggiori **con gli Stati membri attraverso la sua rete per la sicurezza economica**. La Commissione utilizzerà la rete al fine di promuovere lo sviluppo di scenari, allineare la comprensione delle minacce, dei rischi e delle possibilità di attenuazione, agevolare lo scambio di informazioni e sostenere l'attuazione, in particolare nell'uso degli strumenti che rientrano nelle competenze degli Stati membri. In tale contesto, la Commissione garantirà la disponibilità di sistemi di informazione adeguati al fine di sostenere lo **scambio rapido e sicuro di informazioni classificate tra e con gli Stati membri** in merito a questioni di sicurezza economica, comprese le valutazioni dei rischi, i soggetti critici e ad alto rischio e le transazioni che destano potenziale preoccupazione. Ciò integrerà il lavoro della rete di

costituzione di scorte dell'UE, che si concentra sulla garanzia dell'approvvigionamento di beni essenziali in situazioni di crisi;

→ creare un **polo di informazione sulla sicurezza economica** nell'ambito del quale, con il sostegno del SEAE, dell'INTCEN/della SIAC[3], della rete delle delegazioni dell'UE e degli Stati membri, nonché degli strumenti di monitoraggio economico del mercato unico esistenti, quali il sistema di monitoraggio SCAN ("*Supply Chain Alert Notification*"), la Commissione individuerà e consoliderà le informazioni disponibili nel contesto di meccanismi pubblici e privati esistenti e coordinerà la raccolta di informazioni supplementari pertinenti per la sicurezza economica. Figureranno in tale contesto un **meccanismo di monitoraggio del mercato** volto a raccogliere informazioni sugli sviluppi nei settori ad alto rischio, comprese informazioni rapide sui flussi commerciali nei settori soggetti a diversificazione al fine di garantire che l'azione dell'UE non sia compromessa. La Commissione consoliderà inoltre le informazioni **sui soggetti ad alto rischio** al fine di sostenere il processo di valutazione dell'ammissibilità ai finanziamenti dell'UE e alla partecipazione a una procedura di investimento o di appalto dell'UE. Inoltre l'autorità doganale europea e il centro doganale digitale dell'UE consentirebbero di **sostenere e far rispettare** in modo efficiente **l'attuazione delle relative iniziative dell'UE in materia di sicurezza economica**, agevolando anche lo scambio di informazioni pertinenti;

→ intensificare **l'impegno strutturato delle delegazioni dell'UE**, in collegamento con le missioni degli Stati membri, altri organismi dell'UE e la comunità imprenditoriale dell'UE presente in paesi terzi, al fine di garantire contributi efficaci alle valutazioni, al monitoraggio e all'attenuazione dei rischi per quanto concerne la sicurezza economica, anche agevolando gli scambi tra imprese e tra imprese e pubblica amministrazione;

→ valutare entro il terzo trimestre del 2026 in che misura il regolamento sulle emergenze e la resilienza nel mercato interno consenta di raccogliere informazioni sulle catene di approvvigionamento a livello di impresa dalle imprese attive nei settori ad alto rischio. Alla luce di tale analisi, la Commissione valuterà la necessità di ulteriori misure;

→ raccomandare agli Stati membri di nominare **consulenti nazionali** di alto livello **per la sicurezza economica** responsabili del coordinamento intergovernativo della valutazione e dell'attenuazione dei rischi per la sicurezza economica. La Commissione promuoverà un coordinamento maggiore delle politiche e azioni congiunte **riunendo regolarmente tali consulenti** e invita altresì il Consiglio dell'UE a prendere in considerazione la possibilità di convocare periodicamente le pertinenti formazioni del Consiglio per discussioni a livello politico;

→ creare un **gruppo di consulenti fidati composto da rappresentanti delle imprese**

[3] Il Centro UE di situazione e di intelligence (INTCEN), attivo in seno al servizio europeo per l'azione esterna, fa parte della capacità unica di analisi dell'intelligence (SIAC) dell'UE e costituisce il centro di intelligence civile dell'UE, che fornisce analisi approfondite ai responsabili delle decisioni presso tutte le istituzioni dell'UE.

**dell'UE** affinché forniscano, tra l'altro, consulenza in merito a rischi specifici e potenziali risposte, oltre a discutere strategie di riduzione dei rischi. La Commissione inviterà periodicamente i rappresentanti dell'industria a partecipare alle discussioni settoriali della rete per la sicurezza economica e, se del caso, a riferire ai commissari europei;

→ istituire un **portale informativo sulla resilienza del commercio** al fine di fornire alle imprese dell'UE informazioni aggiornate, nell'ambito del portale "Access to Markets" (A2M), in merito alle restrizioni all'esportazione e ad altre misure restrittive imposte da paesi terzi, nonché in merito ai potenziali rischi legati alla necessità di rafforzare la resilienza dell'UE;

→ espandere l'**Osservatorio per le tecnologie critiche** al fine di individuare, monitorare e analizzare l'industria spaziale e della difesa e le relative catene di approvvigionamento, includere le tecnologie emergenti e sostenere l'attuazione a livello di UE e nazionale delle tabelle di marcia tecnologiche dell'UE che ne derivano;

→ utilizzare il futuro **centro di competenza sulla sicurezza della ricerca** al fine di promuovere la sicurezza della ricerca e aumentare la resilienza della comunità di ricerca, anche sviluppando una piattaforma per la dovuta diligenza volta a sostenere le università nella scelta dei loro partner internazionali;

→ esaminare le modalità per allineare e **integrare i paesi candidati al nostro approccio alla sicurezza economica**, in particolare nei settori in cui le loro vulnerabilità in termini di sicurezza economica possono rappresentare un rischio per la sicurezza dell'UE.

Basandosi su un'analisi e una governance rafforzate, l'UE può perseguire meglio i propri obiettivi di sicurezza economica i) chiarendo e migliorando la diffusione degli strumenti esistenti e ii) sviluppando strumenti nuovi ove necessario.

Innanzitutto, **la Commissione adeguerà il modo in cui utilizza alcuni dei propri strumenti** al fine di renderli più efficaci nella gestione dei rischi per la sicurezza economica e cercherà di migliorare il coordinamento tra tali strumenti.

**La Commissione adotterà le misure seguenti al fine di migliorare l'uso degli strumenti:**

→ finanziamenti dell'UE:

- in futuro la Commissione **incentiverà nelle proprie attività di finanziamento progetti a sostegno della sicurezza economica dell'UE**;
- in particolare, dovrebbe mobilitare un livello sufficiente di finanziamenti tale da ridurre le dipendenze da tecnologie, componenti e materiali critici, in particolare in settori strategici quali lo spazio e la difesa, anche al fine di attuare pienamente le tabelle di marcia tecnologiche dell'Osservatorio per le tecnologie critiche;
- la Commissione, gli Stati membri e i partner esecutivi dovrebbero cercare di impedire l'accesso da parte di soggetti ad alto rischio alle azioni sensibili sostenute dall'Unione. L'articolo 136 del regolamento finanziario fornisce una base giuridica orizzontale per tutelare la sicurezza e l'ordine pubblico dell'UE quando la

Commissione e i partner esecutivi eseguono il bilancio dell'UE. Ciò consente di impedire a soggetti ad alto rischio di beneficiare dei fondi dell'UE e di limitare l'accesso ai fondi dell'UE nei settori strategici e nei settori delle tecnologie e delle infrastrutture critiche da parte di soggetti provenienti da paesi terzi che compromettono gli interessi dell'UE in materia di sicurezza economica. Per fugare eventuali dubbi, i partner esecutivi dovrebbero astenersi dal sostenere progetti che contraddicono quanto sopra, anche in operazioni a proprio rischio. A tal fine, e per garantire un migliore allineamento delle politiche tra i programmi dell'UE e gli obiettivi di sicurezza economica, nel primo trimestre del 2026 saranno messi a disposizione orientamenti, sostenendo così lo sviluppo di un approccio più coeso ed efficace. La Commissione incoraggerà inoltre gli Stati membri, il **gruppo BEI e altre istituzioni finanziarie internazionali/banche e istituti nazionali di promozione che stanno attuando bilanci nazionali o dell'UE** a dare priorità al sostegno alle imprese dell'UE che riducono le dipendenze dall'estero in settori critici, in particolare per specifici progetti, tecnologie critiche e infrastrutture critiche individuati come ad alto rischio. Analogamente, ai fornitori ad alto rischio di paesi terzi dovrebbe essere impedito di accedere ai finanziamenti dell'UE e nazionali qualora sia appurato, sulla base di criteri specifici, che tali paesi terzi compromettono gli interessi dell'UE in materia di sicurezza economica;

→ controllo degli investimenti esteri diretti:

- elaborerà **orientamenti** basati sull'esperienza acquisita nell'attuazione dell'attuale regolamento sul controllo degli investimenti esteri diretti al fine di garantire che le autorità nazionali di controllo adottino un approccio coerente al controllo, anche nei settori strategici. Tali orientamenti stabiliranno inoltre le modalità per tenere conto del potenziale rischio cumulativo di investimenti multipli e saranno integrati da orientamenti sull'interazione tra eventuali prescrizioni a livello di UE e l'applicazione di meccanismi nazionali di controllo nel settore finanziario;

→ controlli delle esportazioni di prodotti a duplice uso:

- svolgerà una **valutazione globale** del regolamento sul controllo delle esportazioni di prodotti a duplice uso. Nell'ambito di tale valutazione, la Commissione esaminerà se detto regolamento consegua i suoi obiettivi nel contesto delle nuove realtà geopolitiche e geoeconomiche, compresi gli impatti del crescente ricorso a controlli unilaterali che possono incidere anche sul mercato unico. La Commissione continuerà inoltre a esaminare, insieme agli Stati membri, come adottare efficacemente controlli europei nei settori tecnologici emergenti in questo nuovo contesto. Durante il processo di valutazione la Commissione garantirà una sensibilizzazione attiva dei portatori di interessi degli Stati membri, dell'industria, degli istituti di ricerca e del mondo accademico;

→ strumenti di difesa commerciale:

- quando viene avviato un caso rilevante ai fini della sicurezza economica dell'UE, **quest'ultima sarà tenuta in considerazione nello svolgimento dell'indagine e**

**nell'elaborazione di eventuali misure**;

→ strumenti per il mercato interno, le autorità doganali e la concorrenza:

- farà pieno uso del **regolamento sulle sovvenzioni estere** al fine di mantenere una concorrenza leale nei settori in cui le sovvenzioni estere determinano distorsioni che comportano rischi per la sicurezza economica;
- incoraggerà gli Stati membri a sfruttare appieno le possibilità esistenti in materia di aiuti di Stato, quali la disciplina degli aiuti di Stato nell'ambito del patto per l'industria pulita, gli orientamenti in materia di aiuti di Stato a finalità regionale, la disciplina sugli aiuti a favore di ricerca, sviluppo e innovazione, il regolamento generale di esenzione per categoria e importanti progetti di comune interesse europeo quali strumenti per rafforzare la resilienza;
- **riesaminerà il ricorso a strumenti doganali strategici (sospensioni tariffarie, contingenti autonomi) per i principali fattori produttivi** al fine di sostenere la competitività delle imprese dell'Unione.

In secondo luogo, la Commissione **elaborerà nuove misure** volte a promuovere la sicurezza economica dell'UE.

**La Commissione intende:**

→ valutare la possibilità di istituire, su base pilota, **un meccanismo di monitoraggio delle start-up a livello di UE volto a individuare le start-up in settori tecnologici critici che sono vulnerabili al rischio di acquisizioni estere ostili**, reindirizzandole verso alternative di investimento dell'UE e altre forme di sostegno (ad esempio consulenza, sviluppo di capacità, incontro con gli investitori). Il meccanismo funzionerebbe in modo coordinato con le iniziative esistenti, quali la strategia dell'UE per le start-up e le scale-up;

→ collaborare con le autorità di controllo al fine di monitorare gli **investimenti di portafoglio** (che non rientrano nell'ambito di applicazione del meccanismo di coordinamento degli investimenti esteri diretti) in settori individuati come ad alto rischio ai fini della sicurezza economica;

→ includere una componente di sicurezza economica per i settori strategici chiave nel futuro **strumento di coordinamento per la competitività**;

→ rafforzare la base industriale e la resilienza delle catene di approvvigionamento dell'UE attraverso l'**atto legislativo su un acceleratore industriale**;

→ come indicato in ResourceEU, sviluppare ulteriormente i **mercati secondari** delle materie prime critiche, anche attraverso l'atto legislativo sull'economia circolare, al fine di agevolare il finanziamento di progetti strategici concernenti materie prime critiche in settori individuati come ad alto rischio ai fini della sicurezza economica;

→ valutare entro il terzo trimestre del 2026 le modalità per **rafforzare la protezione dell'industria contro politiche commerciali sleali e sviluppi negativi del mercato globale, quali l'eccesso di capacità**. In questo contesto la Commissione valuterà

l'efficacia e l'adeguatezza degli strumenti esistenti ed esaminerà la necessità di eventuali nuove misure;

→ rivedere il **regolamento di blocco** al fine di semplificarne l'applicazione e ridurre i costi di conformità per le persone e le imprese dell'UE e creare un deterrente credibile contro l'applicazione extraterritoriale di sanzioni di paesi terzi. Ciò rafforzerà la sicurezza economica europea proteggendo meglio gli operatori dell'UE da misure contrastanti di paesi terzi e garantendo un quadro più prevedibile, efficace e assertivo;

→ esaminare le modalità per incoraggiare le imprese in specifici settori ad alto rischio a garantire che le **forniture provengano da almeno due fornitori diversi** e a limitare l'esposizione a un unico fornitore dominante;

→ esaminare la possibilità di fornire **sostegno finanziario a imprese soggette a decisioni di controllo degli investimenti esteri diretti** in situazioni nelle quali la loro sostenibilità finanziaria potrebbe essere a rischio in assenza di un investimento, fatte salve le norme in materia di aiuti di Stato;

→ nel contesto della revisione delle direttive sugli appalti pubblici, **proporre criteri di preferenza europea in settori strategici specifici** in cui i nostri appalti pubblici stimolano la domanda di leadership industriale europea, aumentano la nostra resilienza e attenuano i rischi per la sicurezza;

→ incentivare le imprese a **ridurre le dipendenze nei settori tecnologici emergenti** nell'ambito del futuro regolamento sui chip 2.0, dell'atto legislativo sui quanti, dell'atto legislativo dell'UE sullo sviluppo del cloud e dell'IA e della strategia della Commissione sui software open source;

→ utilizzare l'imminente revisione del **regolamento sulla cibersicurezza** per introdurre restrizioni a livello di UE all'accesso a infrastrutture critiche da parte di fornitori ad alto rischio.

## ***5. Conclusioni***

L'UE mantiene il proprio fermo impegno a favore di un commercio aperto e basato su regole, delle relazioni in materia di investimenti e della cooperazione internazionale. Continuerà pertanto a sostenere il commercio aperto e gli investimenti con i partner di tutto il mondo e a trarne vantaggio. Allo stesso tempo, nell'attuale contesto geopolitico, è indispensabile salvaguardare la sicurezza economica dell'UE. Affrontare i rischi che derivano da tale apertura è fondamentale per preservare quest'ultima, nonché per la nostra sicurezza in senso più ampio e per la competitività della nostra industria.

L'UE dispone già di numerosi strumenti per perseguire questo obiettivo. Tali strumenti devono ora essere utilizzati in modo strategico e, ove necessario, ulteriormente migliorati, al fine tanto di scoraggiare in modo credibile le minacce alla sicurezza economica dell'UE prima che queste si manifestino, quanto di rispondere efficacemente quando tali minacce si concretizzano. Il conseguimento di tale obiettivo richiede che la Commissione, il Parlamento

europeo e gli Stati membri lavorino in modo coordinato e cooperino strettamente con l'industria, ai fini di un processo decisionale efficiente e informato.

L'UE è determinata a fare un uso più proattivo, strategico e coordinato di tutti gli strumenti disponibili al fine di costruire un'economia forte, sicura e resiliente a lungo termine e di operare efficacemente nelle nuove condizioni geopolitiche e geoeconomiche che plasmano il commercio mondiale.