COMMISSIONE
EUROPEA

Strasburgo, 15.2.2022
COM(2022) 61 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI

Tabella di marcia relativa alle tecnologie critiche per la sicurezza e la difesa

1. Introduzione

Rimanere all'avanguardia nello sviluppo tecnologico è fondamentale per garantire la prosperità, la sicurezza e lo stile di vita europei. Le nuove tecnologie stanno trasformando i settori della sicurezza e della difesa a un ritmo più rapido che mai e stanno rendendo meno netto il confine tra la sfera civile e quella militare. Le tecnologie digitali, in particolare, incidono sugli equilibri di potere consolidati nel panorama mondiale della sicurezza. È pertanto essenziale fare in modo che i settori europei della sicurezza e della difesa rimangano tecnologicamente idonei alla loro finalità.

Accade sempre più spesso che molte tecnologie critiche per la sicurezza e la difesa nascano nel settore civile e si avvalgano di componenti critici a duplice uso. Per accelerare l'innovazione in tutti i campi e promuovere la sovranità tecnologica nei settori della sicurezza e della difesa occorre migliorare gli scambi tra gli ambienti di ricerca e innovazione delle sfere civile e della difesa. Alla luce della sua lunga esperienza in materia di sviluppo tecnologico civile e dei suoi nuovi strumenti di cooperazione nel settore della difesa[1], l'UE si trova nella posizione ideale per assumere un ruolo guida. Perché questo sia possibile occorrerà tuttavia un uso più efficiente delle risorse e la disponibilità a studiare le opportunità offerte dal duplice uso, nel rispetto dei valori fondamentali dell'UE. Sarà necessario anche ridurre le dipendenze strategiche e le vulnerabilità delle catene del valore e dell'approvvigionamento associate a queste tecnologie.

La frammentazione delle capacità di sicurezza e difesa europee ha provocato inefficienze economiche, ridotto la capacità operativa e aumentato le dipendenze strategiche. La rivoluzione in atto nelle tecnologie della sicurezza e della difesa e i nuovi strumenti UE di cooperazione in materia di difesa offrono all'UE l'occasione di evitare gli errori del passato, sviluppare le capacità attuali e preservare la sua prosperità economica e la sua sicurezza. **Il futuro panorama europeo delle tecnologie e dell'innovazione in materia di sicurezza e difesa dovrebbe essere sviluppato sin dall'inizio nell'ambito dei quadri di cooperazione dell'UE.**

Nel suo discorso sullo stato dell'Unione 2021[2] la Presidente von der Leyen ha riconosciuto che, sebbene l'UE abbia iniziato a sviluppare un ecosistema europeo della difesa, c'è bisogno di un'Unione europea della difesa. La bussola strategica dell'UE per la sicurezza e la difesa ("bussola strategica"), che gli Stati membri adotteranno a marzo 2022, definirà una visione strategica comune per il prossimo decennio e delineerà in che modo l'UE rafforzerà la sua capacità di: agire e rispondere a varie crisi e sfide; tutelare i propri interessi e proteggere i propri cittadini; investire e innovare per sviluppare in maniera congiunta le capacità e le tecnologie necessarie; rafforzare i partenariati che si fondano sui valori e gli interessi dell'UE.

La presente tabella di marcia relativa alle tecnologie critiche per la sicurezza e la difesa risponde alla richiesta formulata dal Consiglio europeo del 25 e 26 febbraio 2021[3] di tracciare un percorso per promuovere la ricerca, lo sviluppo tecnologico e l'innovazione e ridurre le dipendenze

---

1 Il Fondo europeo per la difesa (FED), la revisione coordinata annuale sulla difesa (CARD) e la cooperazione strutturata permanente in materia di difesa (PESCO).

2 Discorso sullo stato dell'Unione 2021 della Presidente von der Leyen.

3 Dichiarazione dei membri del Consiglio europeo del 26 febbraio 2021.

strategiche dell'UE nelle tecnologie critiche e nelle catene del valore per la sicurezza e la difesa. Il documento sarà presentato al vertice informale che si terrà a Parigi il 10 e 11 marzo 2022 e contribuirà alla bussola strategica. La tabella di marcia propone azioni da intraprendere affinché l'UE e gli Stati membri raggiungano insieme l'obiettivo di cui sopra, in particolare:

- individuando le tecnologie critiche per la sicurezza e la difesa dell'UE e incentivandole tramite i programmi europei di ricerca, sviluppo tecnologico e innovazione;
- garantendo che i programmi europei civili di ricerca, sviluppo tecnologico e innovazione e, se del caso, le politiche industriali e commerciali tengano maggiormente conto delle considerazioni in materia di difesa e, d'altro canto, che i possibili usi civili delle tecnologie siano maggiormente presi in considerazione nei programmi di ricerca, sviluppo tecnologico e innovazione nel settore della difesa;
- promuovendo fin dall'inizio un approccio strategico e coordinato a livello dell'UE per le tecnologie critiche per la sicurezza e la difesa, al fine di utilizzare al meglio i programmi di ricerca, sviluppo tecnologico e innovazione dell'UE e degli Stati membri, realizzare sinergie tra gli ambienti di ricerca, sviluppo tecnologico e innovazione civile e di difesa e attenuare le dipendenze strategiche da fonti esterne; e
- coordinandosi il più possibile con altri partner che condividono gli stessi principi, come gli Stati Uniti e l'Organizzazione del Trattato del Nord Atlantico (NATO), a condizioni reciprocamente vantaggiose.

2. Tecnologie critiche e dipendenze strategiche nei settori della sicurezza e della difesa

La comunicazione "Aggiornamento della nuova strategia industriale 2020: costruire un mercato unico più forte per la ripresa dell'Europa" ("strategia industriale aggiornata")[4] del maggio 2021 conferma che la leadership tecnologica è motore essenziale della competitività e dell'innovazione dell'UE, in particolare per le "tecnologie critiche"[5]. Sottolinea poi l'importanza di individuare e ridurre le dipendenze strategiche negli "ecosistemi sensibili", tra cui "prossimità, economia sociale e sicurezza civile" e "industria aerospaziale e della difesa", per garantire la resilienza dell'UE.

Il piano d'azione della Commissione sulle sinergie tra l'industria civile, della difesa e dello spazio ("piano d'azione sulle sinergie")[6] del febbraio 2021 riconosce la crescente importanza delle tecnologie abilitanti e di rottura provenienti dal settore civile per il futuro della sicurezza e della difesa europee, e la necessità di promuovere il reciproco arricchimento e le sinergie tra le tecnologie del settore civile e quelle della difesa. Definisce inoltre diverse azioni chiave volte a favorire lo scambio di informazioni e la cooperazione tra gli ambienti civili e della difesa partendo dai programmi e dagli strumenti UE di ricerca, sviluppo tecnologico e innovazione.

---

4 COM(2021) 350 final.

5 Nell'ambito del lavoro sull'osservatorio dell'UE sulle tecnologie critiche, la Commissione sta elaborando una definizione di "tecnologie critiche" per i settori spaziale e della difesa e i settori civili correlati (compresa la sicurezza).

6 COM(2021) 70 final.

2.1. Caratteristiche specifiche dei settori della sicurezza e della difesa

L'industria della difesa dell'UE ha una struttura diversificata, che comprende grandi multinazionali e operatori di piccole e medie dimensioni. La domanda proviene quasi esclusivamente dai governi nazionali, che controllano anche ogni acquisizione di prodotti e tecnologie per la difesa, nonché le relative esportazioni. Le differenze nazionali in termini di requisiti, spesa pubblica e investimenti continuano a frammentare il mercato UE della difesa, rischiando talvolta di ostacolare l'interoperabilità tra le forze armate nazionali dei vari Stati membri. Il settore della difesa non segue dunque le norme convenzionali e i modelli commerciali che disciplinano i mercati più tradizionali, e per questo ha un margine di manovra limitato per influenzare gli investimenti e le scelte di mercato correlati. Pertanto è difficile per l'industria intraprendere importanti progetti autofinanziati di ricerca, sviluppo tecnologico e innovazione nel settore della difesa.

L'industria della sicurezza dell'UE si trova ad affrontare sfide analoghe, poiché anche in questo settore i mercati sono prevalentemente nazionali e persino più frammentati. La clientela è diversificata (per esempio forze di polizia, agenzie responsabili della sicurezza interna, agenzie delle Dogane, autorità di frontiera, servizi di sicurezza privati), le attività si svolgono a vari livelli (locale, regionale, nazionale) e l'organizzazione varia da uno Stato membro all'altro. **Nel 2022 la Commissione presenterà uno studio sul mercato della sicurezza dell'UE, in cui riporterà ulteriori dati su questo complesso settore.** Inoltre nella prima metà del 2022 i servizi della Commissione riassumeranno le proposte per promuovere l'adozione di approcci basati sulle capacità da applicare in tutti i settori della sicurezza. Queste proposte rafforzeranno l'individuazione tempestiva e orientata al futuro delle esigenze e delle soluzioni nel campo della sicurezza interna e delle attività di contrasto.

Lo spazio e l'informatica sono "fattori abilitanti" strategici per i settori della sicurezza e della difesa. Il settore spaziale condivide molte delle loro caratteristiche specifiche, come i volumi di mercato ridotti e la leva limitata che possono esercitare sul mercato privato dei componenti. La resilienza dei programmi spaziali e delle catene del valore nel settore spaziale è di vitale importanza per gli obiettivi dell'UE in materia di sicurezza e difesa. Anche l'informatica ha un ruolo sempre più importante nell'ambito delle capacità di difesa, e richiede attenzione e investimenti. Il rapido aumento degli attacchi informatici contro le risorse e le reti civili e della difesa e il ruolo sempre maggiore del settore civile nelle innovazioni e nella normazione in ambito informatico rendono necessaria una relazione più stretta tra la cibersicurezza e la ciberdifesa. Il contributo della Commissione alla difesa europea nell'ambito della bussola strategica ("comunicazione sulla difesa"), che fa parte del presente pacchetto sulla difesa, illustra altre misure relative a questi due settori.

2.2. Mappatura delle tecnologie critiche e delle dipendenze strategiche nei settori della sicurezza e della difesa

La strategia industriale aggiornata fornisce una mappatura e un'analisi di ampia portata delle dipendenze e delle capacità strategiche dell'UE, basata su una prima tornata di indagini

approfondite sugli ecosistemi sensibili[7]. Benché tale lavoro abbia fornito una base per un'azione politica volta a rafforzare la resilienza dell'UE, riconosce anche che è necessario continuare a lavorare per comprendere meglio le dipendenze strategiche dell'UE e il modo in cui possono svilupparsi e determinare ulteriori vulnerabilità. Il lavoro comprende una seconda tornata di indagini approfondite sugli ecosistemi sensibili e un sistema di monitoraggio attraverso l'osservatorio sulle tecnologie critiche ("osservatorio"), cfr. sezione 2.3.

I servizi della Commissione hanno iniziato a svolgere indagini approfondite sui settori tecnologici della difesa e della sicurezza, tra cui quello della cibersicurezza, per sostenere la strategia industriale aggiornata e lo sviluppo dell'osservatorio. Finora sono stati condotti due studi preliminari di casi sui settori tecnologici della difesa relativi ai sistemi autonomi e ai semiconduttori, considerati campioni rappresentativi in virtù della loro rilevanza trasversale per le capacità militari in diversi ambiti, cfr. riquadro 1. L'obiettivo era quello di individuare tendenze comuni in questi settori tecnologici della difesa, in particolare per quanto riguarda le cause delle dipendenze e i relativi rischi, nonché le soluzioni iniziali per attenuarli.

Gli studi di casi confermano che in linea di massima il settore della difesa presenta le stesse dipendenze strategiche e vulnerabilità di altri ecosistemi sensibili, in particolare in relazione alle lacune tecnologiche, alle materie prime (critiche), alle competenze, al basso livello di investimenti in ricerca, sviluppo tecnologico e innovazione e alle norme extraterritoriali dei paesi terzi. Dagli studi emerge anche che generalmente le vulnerabilità del settore sono acuite dalla natura strategica e sensibile delle sue attività (per esempio standard più elevati di sicurezza delle informazioni e sicurezza dell'approvvigionamento) e dalle dimensioni relativamente ridotte del mercato.

Gli studi di casi evidenziano poi che alcuni dei concorrenti mondiali dell'UE adottano più azioni offensive e difensive per promuovere le tecnologie critiche e affrontare le dipendenze strategiche di quanto abbia fatto finora l'UE. Per esempio integrano in modo più sistematico le considerazioni sul tema della difesa nazionale nello sviluppo tecnologico civile, realizzano ingenti investimenti nella ricerca, nello sviluppo tecnologico e nell'innovazione e nella capacità industriale a livello nazionale, attirano investitori esterni e a volte mettono in campo strategie di acquisizione aggressive nei paesi terzi. Proteggono inoltre le proprie competenze industriali e la propria influenza facendo leva sulle interdipendenze o applicando rigide norme extraterritoriali per limitare l'accesso dei paesi terzi alle tecnologie.

Sebbene l'UE disponga di strumenti propri per rafforzare la capacità industriale nel rispetto delle norme UE, è ostacolata dalla domanda ancora ampiamente frammentata del mercato europeo della difesa, dalla storica separazione netta a livello dell'UE tra ricerca, sviluppo tecnologico e innovazione del settore civile e del settore della difesa e dagli investimenti comparativamente insufficienti degli Stati membri nella base industriale e tecnologica di difesa europea (EDTIB). La spesa collettiva degli Stati membri per l'innovazione nel settore della difesa (2,5 miliardi di EUR, pari all'1,2 % della spesa per la difesa), infatti, continua a non raggiungere l'obiettivo del 2 % fissato dall'Agenzia europea per la difesa 15 anni fa.

[7] SWD(2021) 352 final.

Se da un lato le forze di mercato hanno portato a una situazione in cui nessun paese può raggiungere da solo la piena sovranità tecnologica in un determinato settore tecnologico, dall'altro c'è una corsa mondiale alla leadership tecnologica e ai vantaggi economici e militari che ne derivano. In assenza di un intervento a livello europeo, questa situazione potrebbe acuire le attuali dipendenze strategiche dell'UE e crearne di nuove. L'UE ha bisogno di un approccio strutturato per rimanere all'avanguardia nelle tecnologie critiche e individuare e attenuare le dipendenze strategiche nel campo della sicurezza e della difesa. La presente tabella di marcia intende delineare tale approccio, che andrà incorporato nella bussola strategica dell'UE.

Riquadro 1: Studi di casi – Sistemi autonomi e semiconduttori per la difesa

Le analisi della Commissione sui sistemi autonomi per la difesa, con particolare attenzione all'intelligenza artificiale (IA) e all'apprendimento automatico, hanno individuato le tecnologie critiche pertinenti e quattro settori principali in cui l'UE è in ritardo: competenze, dati, hardware e prove. Le eventuali misure per affrontare la situazione dovrebbero basarsi sull'attuale strategia dell'UE sull'intelligenza artificiale[8], sulle iniziative politiche correlate e sulle strategie nazionali degli Stati membri in materia di IA. Comprendono attività di ricerca, sviluppo tecnologico e innovazione (per esempio una maggiore disponibilità di dati e formazione sull'IA, un collegamento con l'iniziativa europea in materia di processori), infrastrutture (per esempio capacità di cloud computing a fini di difesa, impianti di prova nazionali) e la protezione delle attuali risorse critiche (per esempio il meccanismo di controllo degli investimenti esteri diretti).

Le analisi sui semiconduttori per la difesa hanno evidenziato la presenza costante dei semiconduttori nei materiali di difesa, e le attuali e future dipendenze causate in particolare dalla carenza di capacità interne dell'UE (fonderie) per realizzare i nodi più avanzati. La Commissione ha inserito misure di attenuazione nella proposta di legge europea sui semiconduttori adottata l'8 febbraio 2022[9], che mira a creare un ecosistema europeo dei semiconduttori all'avanguardia per migliorare le capacità dell'UE in questo settore, rispondendo così anche alle esigenze di difesa.

2.3. Osservatorio sulle tecnologie critiche

Alcune delle attuali dipendenze strategiche dell'UE dai paesi terzi (per esempio per quanto riguarda i sistemi a pilotaggio remoto e i semiconduttori) derivano in parte dalla scarsa lungimiranza sull'importanza futura delle tecnologie. L'UE ha bisogno di previsioni e riflessioni strategiche più strutturate sulle tecnologie critiche per la sicurezza e la difesa al fine di individuare i settori prioritari per stimolare la ricerca e l'innovazione, ridurre le dipendenze strategiche attuali ed evitare che ne emergano di nuove.

L'osservatorio sulle tecnologie critiche, che la Commissione sta istituendo in linea con il piano d'azione sulle sinergie (azione 4), contribuirà a queste riflessioni. I suoi metodi di lavoro terranno

[8] COM(2018) 237 final.
[9] COM(2022) 45 final.

conto di altre iniziative analoghe[10] per evitare duplicazioni, il che consentirà di perfezionare l'elenco delle tecnologie critiche del piano d'azione sulle sinergie affinché rispecchi l'evoluzione del panorama tecnologico e delle esigenze in termini di capacità.

L'osservatorio individuerà, monitorerà e valuterà le tecnologie critiche per i settori dello spazio, della difesa e i settori civili connessi, la loro potenziale applicazione e le relative catene del valore e di approvvigionamento. Individuerà, monitorerà e analizzerà anche i divari tecnologici attuali e quelli prevedibili, le cause profonde delle dipendenze e delle vulnerabilità strategiche.

Sarà fondamentale trovare un accordo con gli Stati membri su quale possa essere il livello di dettaglio adeguato per dibattere tali questioni a livello dell'UE e sulla necessità di condividere i dati pertinenti tra Stati membri e con la Commissione. Nell'ambito dell'osservatorio sarà istituito un meccanismo, sotto forma di gruppo di esperti ad hoc, per lo scambio e la discussione con gli Stati membri in un contesto classificato. Ciò comprenderà discussioni su come far emergere tecnologie nuove e di rottura per evitare nuove dipendenze nei settori della sicurezza, della difesa e dello spazio. L'Alto rappresentante e i suoi servizi saranno coinvolti in questo processo.

Sulla scorta dei dati dell'osservatorio, la Commissione presenterà agli Stati membri entro la fine del 2022 e successivamente ogni due anni una relazione classificata concernente le tecnologie critiche e i rischi correlati alle dipendenze strategiche che incidono su sicurezza, spazio e difesa. Sulla base di queste relazioni la Commissione preparerà tabelle di marcia tecnologiche comprendenti misure di attenuazione per stimolare la ricerca, lo sviluppo tecnologico e l'innovazione e ridurre le dipendenze strategiche che incidono sulla sicurezza e la difesa.

Non appena l'osservatorio avrà consolidato le sue attività potrà estendere l'ambito di intervento ad altri settori, come indicato nella strategia industriale aggiornata.

Azioni previste

- Nel 2022 la Commissione istituirà un gruppo di esperti per facilitare gli scambi con gli Stati membri sulle tecnologie critiche e le catene del valore e dell'approvvigionamento. Il gruppo farà parte dell'osservatorio sulle tecnologie critiche per la difesa, lo spazio e i settori civili correlati e sarà incaricato di:
  - consultare regolarmente le autorità degli Stati membri per preparare la relazione classificata;
  - garantire un trattamento adeguato delle informazioni sensibili e classificate eventualmente scambiate nell'ambito dell'osservatorio sulle tecnologie critiche e delle relative relazioni e tabelle di marcia.
- Entro la metà del 2022 la Commissione presenterà uno studio sul mercato della sicurezza dell'UE, che servirà a comprendere meglio le caratteristiche specifiche del mercato della sicurezza civile, a favorire l'individuazione delle tecnologie critiche e delle dipendenze strategiche e a sostenere il nuovo approccio basato sulle capacità per la sicurezza e altre

[10] Per esempio l'assistenza e gli strumenti disponibili nell'ambito del progetto Advanced technologies for industry (ATI, tecnologie avanzate per l'industria), il monitoraggio delle tecnologie critiche per lo spazio, l'agenda strategica di ricerca onnicomprensiva (OSRA), gli elementi tecnologici (Technology Building Blocks, TBB) e le attività strategiche chiave (KSA) dell'Agenzia europea per la difesa (AED).

attività di ricerca, sviluppo tecnologico e innovazione.

- Entro la metà del 2022 i servizi della Commissione redigeranno un documento di sintesi delle proposte per promuovere l'adozione di approcci basati sulle capacità da applicare in tutti i settori della sicurezza.

3. Stimolare le attività di ricerca, sviluppo tecnologico e innovazione sulle tecnologie critiche per la sicurezza e la difesa

Le tabelle di marcia tecnologiche che la Commissione preparerà basandosi sulle valutazioni dell'osservatorio sosterranno interventi che vanno dalla programmazione di attività di ricerca, sviluppo tecnologico e innovazione sulle tecnologie critiche allo sviluppo di iniziative faro più ampie, che contribuiranno a rafforzare la competitività e la resilienza dell'UE nei settori della sicurezza e della difesa. Per realizzare questi obiettivi sarà necessario utilizzare in modo più efficiente le risorse finanziarie disponibili, attraverso un migliore coordinamento degli strumenti e dei programmi di ricerca, sviluppo tecnologico e innovazione esistenti a livello nazionale e dell'UE.

3.1. Superare la separazione esistente tra le attività di ricerca, sviluppo tecnologico e innovazione UE in ambito civile e quelle del settore della difesa

Nell'ambito del piano d'azione sulle sinergie (azione 2), la Commissione si è impegnata a rafforzare entro la fine del 2022 il coordinamento interno dei programmi e degli strumenti dell'UE (cfr. riquadro 2) per poter usufruire dei notevoli vantaggi che le sinergie tra le attività di ricerca, sviluppo tecnologico e innovazione in ambito civile e quelle del settore della difesa possono determinare per la crescita economica, il mercato unico e la sicurezza dei cittadini europei.

Anche se l'attuazione di questo obiettivo potrà essere portata avanti anche nel 2023 (per esempio tramite una migliore pianificazione e sincronizzazione, orientamenti alle autorità di gestione degli Stati membri ecc.), alcuni ostacoli saranno più difficili da superare nel breve e medio periodo e potrebbero richiedere il coinvolgimento di altri portatori di interessi. Ciò vale in particolare quando le disposizioni giuridiche contenute negli atti di base dei programmi e degli strumenti dell'UE pongono vincoli pratici. Per esempio, mentre le attività a duplice uso possono essere finanziate nell'ambito del meccanismo per collegare l'Europa (MCE) e dei fondi strutturali e d'investimento europei (fondi SIE), le attività svolte nell'ambito di Orizzonte Europa[11] sono incentrate sulle applicazioni civili; i programmi e gli strumenti di ricerca, sviluppo tecnologico e innovazione non prevedono un quadro di sostegno diretto a tali attività. Analogamente, la politica di prestiti della Banca europea per gli investimenti prevede ancora restrizioni per il settore della difesa.

[11] Nel presente documento "Orizzonte Europa" indica il programma specifico di attuazione di Orizzonte Europa e l'Istituto europeo di innovazione e tecnologia; le attività svolte in questi ambiti sono incentrate esclusivamente sulle applicazioni civili.

Per facilitare gli scambi tra gli ambienti civile e della difesa, specialmente nel settore delle tecnologie critiche, nel 2023 la Commissione elaborerà un approccio per promuovere la piena attuazione a medio-lungo termine in tutti i programmi e gli strumenti dell'UE di attività di ricerca, sviluppo tecnologico e innovazione a duplice uso. Il lavoro contribuirà anche alla valutazione intermedia dei programmi settoriali pertinenti, come i fondi nell'ambito del regolamento sulle disposizioni comuni, compresi i fondi per la preparazione alle emergenze sanitarie.

Riquadro 2: Programmi e strumenti UE che sostengono la ricerca, lo sviluppo tecnologico e l'innovazione sulle tecnologie critiche pertinenti per la sicurezza e la difesa e la realizzazione delle relative infrastrutture nell'ambito del quadro finanziario pluriennale (2021-2027)

- Il Fondo europeo per la difesa destina 8 miliardi di EUR alla ricerca e allo sviluppo nel settore della difesa. Tra il 4 e l'8 % del bilancio del FED per la ricerca e allo sviluppo, ossia fino a 100 milioni di EUR l'anno, sarà destinato alle tecnologie di rottura.
- Nell'ambito del pilastro II, "Sfide globali e competitività industriale europea", Orizzonte Europa assegna 1,6 miliardi di EUR alla ricerca e all'innovazione in materia di sicurezza civile nel quadro del polo tematico "Sicurezza civile per la società", mentre il sostegno alle tecnologie critiche rientra nei poli tematici "Digitale, industria e spazio", "Clima, energia e mobilità" e "Prodotti alimentari, bioeconomia, risorse naturali, agricoltura e ambiente". Le attività complementari sono finanziate nell'ambito del pilastro I, "Scienza di eccellenza", dal Consiglio europeo per l'innovazione (CEI) e dall'Istituto europeo di innovazione e tecnologia (EIT) nell'ambito del pilastro III "Europa innovativa", nonché dai partenariati europei, che mettono in comune e mobilitano risorse per garantire la leadership tecnologica e l'autonomia strategica aperta dell'UE nei settori critici.
- Il programma Europa digitale promuoverà le attività di diffusione pertinenti per le tecnologie critiche nei settori prioritari della cibersicurezza, dell'IA e del supercalcolo.
- Nel 2022 il centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza e rete di centri di coordinamento adotterà un'agenda strategica sugli investimenti nella componente cibernetica, che confluirà in Orizzonte Europa e nel programma Europa digitale. Sarà possibile studiare le sinergie tra le tecnologie dei settori civile e della difesa e le applicazioni a duplice uso attraverso collegamenti al Fondo europeo per la difesa, in linea con le norme applicabili.
- I fondi SIE (in particolare il Fondo europeo di sviluppo regionale e il Fondo sociale europeo Plus) potranno essere utilizzati a sostegno della base industriale e tecnologica di difesa europea (EDTIB).
- Tra gli altri programmi, fondi e strumenti pertinenti dell'UE figurano il programma spaziale, il meccanismo per collegare l'Europa (MCE), il programma InvestEU, il dispositivo per la ripresa e la resilienza, il programma LIFE, i partenariati pubblico-privato e i meccanismi di finanziamento misto.

3.2. Collegare programmi e strumenti nazionali e dell'UE che sostengono la ricerca, lo sviluppo tecnologico e l'innovazione in materia di tecnologie critiche per la sicurezza e la difesa

Benché i programmi e gli strumenti dell'UE eroghino cospicui finanziamenti alle attività di ricerca, sviluppo tecnologico e innovazione per la sicurezza e la difesa nell'UE, la maggior parte dei finanziamenti per queste attività proviene ancora dagli Stati membri, e la frammentazione dei mercati della sicurezza e della difesa rimane un problema serio. Di conseguenza, per raggiungere la sovranità tecnologica in alcuni settori tecnologici critici e attenuare le dipendenze strategiche in altri settori occorrerà un coordinamento a livello dell'UE.

Gli Stati membri sono invitati a impegnarsi, nell'ambito della bussola strategica, a sviluppare fin dall'inizio insieme alla Commissione un approccio coordinato a livello dell'UE per le tecnologie critiche pertinenti per la sicurezza e la difesa, nel pieno rispetto della varietà e complessità della governance dei programmi e degli strumenti nazionali ed europei. Questo approccio dovrebbe tenere conto anche di altre strutture di coordinamento, quali il nuovo polo UE dell'innovazione per la sicurezza interna, presieduto dal comitato permanente per la cooperazione operativa in materia di sicurezza interna (COSI), e il nuovo polo UE dell'innovazione nel settore della difesa che sarà istituito dall'Agenzia europea per la difesa.

L'approccio dovrebbe utilizzare le relazioni classificate sulle tecnologie critiche e le tabelle di marcia tecnologiche elaborate dalla Commissione come punto di partenza per le discussioni tra le autorità degli Stati membri e la Commissione, con l'obiettivo di individuare, sulla base delle tabelle di marcia tecnologiche, i settori che richiedono le azioni più urgenti e mobilitare i programmi, gli strumenti e le politiche dell'UE e degli Stati membri per procedere in modo coordinato, nel rispetto delle norme dell'UE in materia di aiuti di Stato. In questo modo si garantirebbe la concentrazione degli investimenti nei settori più importanti per la sicurezza dei cittadini dell'UE. Le priorità sarebbero aggiornate periodicamente per far sì che restino pertinenti e che la spesa sia efficiente.

La Commissione collaborerà con gli Stati membri per individuare il meccanismo più idoneo a facilitare il lavoro di coordinamento (per esempio il gruppo di esperti dell'osservatorio).

3.3. Sostenere l'innovazione e l'imprenditorialità nel settore della sicurezza e della difesa – Creare un sistema UE di innovazione nel settore della difesa

L'UE deve sfruttare meglio il pieno potenziale della propria comunità dell'innovazione per sostenere i settori della sicurezza e della difesa. A tal fine sarà necessario aiutare gli operatori non tradizionali e le start-up e piccole e medie imprese (PMI) innovative esistenti nei due settori a superare i complessi ostacoli tecnologici, amministrativi, normativi e di accesso al mercato, a rispettare gli elevati standard di sicurezza e ad accedere ai finanziamenti. Il mercato della difesa ruota spesso intorno a pochi grandi operatori sostenuti da una serie di PMI specializzate che hanno limitato accesso diretto a tale mercato. Di conseguenza le PMI innovative del settore della difesa possono avere difficoltà ad accedere ai finanziamenti, e questo aumenta le probabilità che si rivolgano a investitori stranieri o che suscitino l'interesse di questi ultimi. La situazione è

simile per le PMI innovative del settore della sicurezza, che affrontano sfide analoghe nell'avvicinare potenziali clienti o nell'accedere a finanziamenti su misura[12].

Finora la Commissione ha sostenuto le start-up e le PMI innovative del settore della sicurezza tramite Orizzonte 2020, e i finanziamenti assegnati e i tassi di successo complessivi nell'ambito della sfida per la società 7 "Sicurezza civile per la società" sono stati superiori alla media per quanto riguarda le piccole imprese innovatrici. Questo sostegno proseguirà nell'ambito di Orizzonte Europa, ma le start-up e le PMI del settore della sicurezza avranno comunque bisogno di un ulteriore sostegno su misura per accedere più rapidamente al mercato. Lo studio di nuovi strumenti per l'innovazione a duplice uso potrebbe stimolare la capacità produttiva, la competitività e la sostenibilità di tali imprese.

La Commissione ha iniziato ad avviare attività analoghe nell'ambito del Fondo europeo per la difesa per sviluppare un pacchetto di strumenti sulla difesa e l'innovazione a duplice uso che riguardi i livelli di maturità tecnologica (TRL)[13] da 1 a 9. Sono in corso lavori sui seguenti strumenti riguardanti la difesa, le nuove tecnologie e il duplice uso:

a) *Innovazione nel settore della difesa tramite il FED* – Sono allo studio azioni specifiche per sostenere meglio i progetti sulle tecnologie di rottura e le soluzioni innovative e orientate al futuro nel settore della difesa, incoraggiando in particolare la partecipazione di PMI innovative, laboratori innovativi e organizzazioni di ricerca e tecnologia (ORT). Tali azioni potranno assumere forme diverse, ad esempio coaching aziendale (programma di lavoro per il 2021); concorsi sulle tecnologie (programma di lavoro per il 2022), hackathon o premi (programma di lavoro per il 2023 o per gli anni successivi). Attingeranno inoltre all'esperienza pertinente del CEI e potrebbero collegarsi alla nuova iniziativa CASSINI per la difesa.

b) *Un meccanismo di finanziamento misto degli investimenti nel settore della difesa nell'ambito di InvestEU* – La creazione di un meccanismo di questo tipo consentirebbe alla Commissione di garantire investimenti nelle PMI innovative o strategiche del settore della difesa da parte di intermediari finanziari in tutta l'UE. In questo modo si attenuerebbero i problemi legati all'accesso limitato ai finanziamenti per le PMI che sviluppano tecnologie promettenti per la difesa europea, e nel contempo si fornirebbero capitali affidabili e si eviterebbero acquisizioni ostili da parte di soggetti di paesi terzi. Facilitare l'accesso al finanziamento azionario per le PMI e le imprese a media capitalizzazione innovative del settore della difesa ne favorirebbe la crescita e gioverebbe quindi alla capacità di innovazione della base industriale e tecnologica di difesa europea (EDTIB). La Commissione valuterà anche la

[12] Challenges and opportunities for SMEs and start-ups in EU security R&I, evento online sul tema del potenziamento della ricerca e dell'innovazione nel settore della sicurezza della Comunità per la ricerca e l'innovazione in materia di sicurezza, 30 aprile 2021.

[13] Dal 2014 l'UE utilizza in modo diffuso una scala di livelli di maturità tecnologica (TRL) nei suoi strumenti e programmi di ricerca, sviluppo tecnologico e innovazione. La scala distingue nove livelli di maturità tecnologica, che vanno dalla ricerca di base (TRL 1) al prodotto finale pronto per l'ingresso sul mercato (TRL 9). Dato che l'applicazione e quindi il potenziale di duplice uso di una tecnologia si rivelano di solito ai livelli di maturità tecnologica 5 e 6, una tecnologia può essere considerata "neutra" ai livelli da 1 a 4.

necessità di ulteriori strumenti a sostegno dei principali partecipanti al mercato nella catena del valore.

c) *Iniziativa CASSINI per la difesa* – Questa iniziativa si ispirerebbe all'attuale iniziativa CASSINI per sostenere le PMI e le start-up nel settore spaziale, e fornirebbe loro servizi quali: sviluppo imprenditoriale e reti di imprese (per esempio abbinamenti tra imprese, acceleratore d'impresa) e premi e concorsi (compresi hackathon, tutoraggio ecc.) a integrazione del summenzionato meccanismo di finanziamento misto degli investimenti nel settore della difesa.

d) *Incubatore di innovazione* – Nel 2022 la Commissione, in linea con il piano d'azione sulle sinergie (azione 6), istituirà un incubatore di innovazione per sostenere lo sviluppo di nuove tecnologie e plasmare l'innovazione a duplice uso, che potrebbe svolgere un ruolo importante nel colmare il divario tra i programmi di ricerca, sviluppo tecnologico e innovazione incentrati sul settore civile e quelli incentrati sul settore della difesa. Dopo un'analisi sistematica dei risultati delle prime fasi di sviluppo tecnologico, l'incubatore segnalerebbe ai servizi competenti della Commissione e degli Stati membri i progetti e/o le tecnologie con potenziali applicazioni nei settori della sicurezza, dello spazio e della difesa. La Commissione valuterebbe in che modo questi progetti segnalati potrebbero essere indirizzati, se necessario, verso ulteriori opportunità di finanziamento, come ad esempio il regime di finanziamento della transizione del CEI o il FED.

e) *Sostegno alle reti di innovazione* – Le reti di innovazione transfrontaliere nel settore della difesa potrebbero svolgere il ruolo di intermediari dell'innovazione e promuovere l'integrazione di soluzioni innovative nei progetti collaborativi. La prospezione tecnologica consentirebbe di individuare nuove soluzioni e tecnologie innovative potenzialmente vantaggiose per le applicazioni nel settore della difesa. I centri di ricerca e le strutture dedicate alle prove tecniche testerebbero poi la pertinenza di tali tecnologie provenienti dal settore civile e condividerebbero le migliori pratiche. L'Agenzia europea per la difesa sarebbe un partner fondamentale della Commissione per l'attuazione di un altro elemento dell'azione 6 del piano d'azione sulle sinergie.

La Commissione studierà come collegare il pacchetto di strumenti ad altri strumenti a sostegno dell'innovazione nei settori della sicurezza (per esempio Orizzonte Europa) o della cibersicurezza (per esempio la rete di centri nazionali di coordinamento per la cibersicurezza in collaborazione con i poli europei dell'innovazione digitale).

I punti di forza complementari della Commissione e dell'AED dovrebbero essere riuniti in un **"sistema UE di innovazione nel settore della difesa"**, nell'ambito del quale la Commissione, forte della sua esperienza nell'esecuzione del bilancio dell'UE a sostegno delle attività di ricerca, sviluppo tecnologico e innovazione nell'ambito della difesa, civile e del duplice uso, avrà un ruolo centrale nello stimolare l'innovazione per la base industriale e tecnologica di difesa europea (EDTIB). Date le sue competenze in materia di difesa, anche in relazione al raggruppamento delle tecnologie emergenti e di rottura e del fabbisogno di capacità militari, l'AED continuerà a mettere in collegamento e sostenere gli sforzi degli Stati membri tramite il suo polo di innovazione nel settore della difesa. Grazie alla stretta collaborazione, la Commissione e l'AED

accelereranno sinergicamente l'innovazione nei settori della sicurezza e della difesa per l'UE e gli Stati membri.

3.4. Competenze

La carenza di competenze e di manodopera, specialmente di personale qualificato con formazione nel campo delle scienze, della tecnologia, dell'ingegneria e della matematica, costituisce una grande sfida per i settori della difesa e della sicurezza, che, come molte altre industrie ad alta tecnologia, vi fanno grande affidamento. Poiché le tecnologie e il panorama delle minacce sono in rapida evoluzione, è importante che l'industria si apra maggiormente a nuovi e giovani ricercatori e imprenditori, ricercatrici e imprenditrici, adottando un approccio di inclusività e accessibilità nei confronti di tutti i talenti, le competenze e la manodopera disponibili.

A novembre 2020 la Commissione ha varato il patto per le competenze avviando un primo ciclo di partenariati per le competenze in tre ecosistemi industriali chiave: il settore della microelettronica, l'industria automobilistica e quella aerospaziale e della difesa. I membri del patto (industria, università e organizzazioni di formazione, parti sociali) si sono impegnati a garantire un'offerta continua e sostenibile di competenze negli ambiti più richiesti migliorando il livello di competenze di 200 000 dipendenti e provvedendo alla riqualificazione di 300 000 persone, con investimenti pubblici e privati di 1 miliardo di EUR entro il 2030.

Azioni previste

- La Commissione invita gli Stati membri a impegnarsi, nell'ambito della bussola strategica, a sviluppare fin dall'inizio un approccio strategico coordinato a livello dell'UE per le tecnologie critiche pertinenti per la sicurezza e la difesa.
- Nel 2023 la Commissione riesaminerà gli strumenti dell'UE esistenti e proporrà ulteriori modalità per incoraggiare la ricerca, lo sviluppo tecnologico e l'innovazione a duplice uso a livello dell'UE.
- La Commissione sosterrà l'innovazione e l'imprenditorialità in materia di tecnologie critiche per la sicurezza e la difesa sulla base dei seguenti strumenti: a) azioni specifiche del Fondo europeo per la difesa; b) un nuovo meccanismo di finanziamento misto per gli investimenti nel settore della difesa nell'ambito di InvestEU; c) una nuova iniziativa CASSINI per la difesa; d) un nuovo incubatore di innovazione per le nuove tecnologie e l'innovazione a duplice uso nel 2022; e) un maggiore sostegno alle reti di innovazione.
- La Commissione, insieme all'Agenzia europea per la difesa e al suo polo di innovazione nel settore della difesa, creerà un sistema UE di innovazione nel settore della difesa al fine di accelerare l'innovazione nei settori della sicurezza e della difesa per l'UE e gli Stati membri.

4. Ridurre le dipendenze strategiche nelle tecnologie critiche e nelle catene del valore per la sicurezza e la difesa

Oltre ai suoi strumenti e programmi di ricerca, sviluppo tecnologico e innovazione, l'UE dispone di diversi strumenti politici che possono contribuire a ridurre la sua dipendenza strategica per quanto riguarda le tecnologie critiche e le catene del valore nei settori della sicurezza e della

difesa. Tali strumenti contribuiscono a rafforzare la capacità industriale, la competitività, la sovranità tecnologica e la resilienza dell'UE, ma anche a proteggere le capacità e gli sviluppi tecnologici attuali e futuri.

Sulla base del lavoro dell'osservatorio sulle tecnologie critiche e nell'ambito della strategia industriale aggiornata, se del caso la Commissione valuterà sistematicamente le considerazioni in materia di sicurezza e difesa in sede di attuazione e revisione degli strumenti industriali e commerciali dell'UE esistenti, o di progettazione di nuovi strumenti di questo tipo, per garantirne l'idoneità allo scopo.

– *Alleanze industriali* – Le alleanze industriali coinvolgono un'ampia gamma di partner (per esempio soggetti pubblici e privati, società civile) in azioni congiunte sugli obiettivi strategici chiave dell'UE in settori o catene del valore specifici. Si basano sui principi di apertura, trasparenza, diversità e inclusività, operano nel pieno rispetto delle norme in materia di concorrenza e possono comprendere, se del caso, filoni di lavoro specifici volti a ridurre le dipendenze strategiche nei settori della sicurezza e della difesa. L'alleanza europea per i dati industriali, l'edge e il cloud e l'alleanza industriale per i processori e le tecnologie dei semiconduttori stanno prendendo in considerazione questa possibilità.
– *Importanti progetti di comune interesse europeo (IPCEI)* – Gli IPCEI sono avviati dagli Stati membri e sono soggetti alle norme dell'UE in materia di aiuti di Stato. Sono pensati per riunire conoscenze, competenze, risorse finanziarie e operatori economici di tutta l'UE al fine di superare fallimenti sistemici o del mercato e sfide sociali che i soggetti privati non potrebbero affrontare da soli, in particolare nel settore delle innovazioni pionieristiche e delle infrastrutture chiave. Gli IPCEI possono considerare aspetti relativi alla sicurezza e alla difesa, come potrebbe accadere con il secondo IPCEI sulla microelettronica, di prossima realizzazione, annunciato nella legge europea sui semiconduttori.
– *Programmi di finanziamento dell'UE* – L'UE ha sempre praticato una politica aperta in materia di ricerca e innovazione, guidata dal principio dell'autonomia strategica aperta e mirante a garantire condizioni di parità e reciprocità. L'approccio globale dell'UE in materia di ricerca e innovazione promuove i partenariati strategici con partner che condividono gli stessi principi, in linea con gli obblighi internazionali dell'UE (per esempio la NATO, gli Stati Uniti, il Canada, il Giappone, la Corea del Sud ecc.)[14].

  Allo stesso tempo l'Europa deve assicurare la tutela dei suoi interessi strategici. Per il periodo 2021-2027 la Commissione ha chiarito e armonizzato le norme di partecipazione dei paesi terzi e di ammissibilità dei soggetti ai vari programmi e strumenti dell'UE. Per determinati programmi (Orizzonte Europa, programma Europa digitale, Fondo europeo per la difesa, programma spaziale, meccanismo per collegare l'Europa) sono state stabilite specifiche condizioni di ammissibilità per le attività sensibili dal punto di vista della sicurezza, poi perfezionate nei pertinenti programmi di lavoro per tutelare gli interessi essenziali di sicurezza dell'UE. La revisione in corso del regolamento finanziario della Commissione farà

[14] Occorre tuttavia segnalare che i programmi di ricerca e sviluppo relativi al settore della difesa della maggior parte dei nostri partner non sono aperti alle imprese dell'UE.

ulteriore chiarezza su come mantenere l'approccio di autonomia strategica aperta dell'UE, cioè su come tutelare gli interessi essenziali dell'UE in materia di sicurezza nel rispetto dei suoi obblighi internazionali.

– *Norme* – Nell'ambito del piano d'azione sulle sinergie, la Commissione promuove l'uso delle norme ibride esistenti in materia civile/di difesa e lo sviluppo di nuove norme entro la fine del 2022 (azione 5) e invita a prendere in considerazione la difesa nelle politiche e nelle azioni di normazione della Commissione. La strategia dell'UE in materia di normazione[15] mira a garantire la leadership dell'UE nell'elaborazione delle norme nella sfera civile, ma sarà molto pertinente anche per il settore della difesa, in quanto quasi l'80 % delle norme utilizzate in questo settore proviene dal settore civile. La Commissione, insieme ai portatori di interessi (per esempio l'Agenzia europea per la difesa) studierà la possibilità di includere requisiti in materia di difesa nei futuri sforzi di normazione che sosterrà, per aumentarne la compatibilità con le esigenze in materia di difesa.

– *Controllo degli investimenti esteri diretti* – L'UE è uno degli ambienti più favorevoli al mondo per gli investimenti esteri ed è una delle principali destinazioni mondiali degli investimenti esteri diretti (IED). Ciononostante, determinati investimenti possono anche compromettere gli interessi essenziali di sicurezza dell'UE. Per prevenire tali rischi, l'UE ha istituito un quadro per il controllo degli investimenti esteri diretti, operativo dall'ottobre 2020. La prima relazione annuale sul controllo degli investimenti esteri diretti ribadisce l'importanza di un controllo efficace degli IED a livello degli Stati membri e di una stretta collaborazione a livello dell'UE, concentrandosi sui rischi potenziali per la sicurezza e l'ordine pubblico. Gli Stati membri sono esortati a istituire meccanismi nazionali di controllo degli IED; 18 Stati membri hanno già provveduto e altri sei vi stanno provvedendo. La Commissione valuterà il regolamento e presenterà una relazione al Parlamento europeo e al Consiglio entro ottobre 2023.

– *Infrastrutture critiche* – La comparsa sempre più rapida di tecnologie nuove e di rottura ha avuto un impatto significativo sulla sicurezza di materiali, infrastrutture, servizi, catene del valore e di approvvigionamento dei settori strategici, compresi quelli della sicurezza e della difesa. L'UE e gli Stati membri devono tenere conto di queste vulnerabilità in modo più organico nelle valutazioni e nel monitoraggio pertinenti dei rischi e nell'attuazione di misure volte ad aumentare la resilienza contro le minacce alla sicurezza, per esempio di natura ibrida o informatica. Sarà necessario un coordinamento a livello dell'UE per fare in modo che gli Stati membri mantengano un livello di resilienza adeguato alle esigenze future e norme di sicurezza coerenti a livello dell'UE per evitare vulnerabilità.

– *Uso intelligente e circolare dei materiali* – Il nuovo piano d'azione per l'economia circolare di marzo 2020 è uno dei principali elementi costitutivi del Green Deal europeo, la nuova agenda europea per la crescita sostenibile. Le innovazioni e i nuovi modelli commerciali basati su una maggiore efficienza in termini di risorse, lo sviluppo di nuovi materiali, la promozione di materie prime secondarie e appalti pubblici più sostenibili non serviranno

[15] COM(2022) 31 final.

soltanto a tutelare l'ambiente, ma anche a garantire garantire all'industria l'accesso ai materiali. Anche le tecniche di produzione additiva, gli appalti verdi e il riciclaggio dei materiali, se attuati correttamente, potrebbero contribuire a rafforzare la competitività dei settori della sicurezza e della difesa dell'UE e la resilienza dell'Unione.

- *Sicurezza dei dati* – La strategia europea per i dati prevede misure volte a garantire che le persone e le imprese possano mantenere il controllo dei loro dati. La questione sarà affrontata nella legge sui dati che la Commissione adotterà nei primi mesi del 2022.

  Nell'ambito del progetto multinazionale sulle infrastrutture e i servizi di dati comuni (che riunisce la federazione europea del cloud e gli spazi comuni europei dei dati), la Commissione favorisce gli investimenti (per esempio il programma Europa digitale, il meccanismo per collegare l'Europa e il fondo Next Generation EU) in capacità cloud-to-edge sicure, resilienti, efficienti sotto il profilo energetico, accessibili in tempo reale e in grado di fornire servizi di qualità in tutta Europa. Garantire il trasferimento di tecnologie cloud ed edge tra i settori civile (in particolare quello della sicurezza), della difesa e dello spazio rafforzerebbe la sovranità tecnologica. L'alleanza europea per i dati industriali, l'edge e il cloud offre una possibile piattaforma per promuovere queste sinergie.
- *Politica commerciale* – La complessità e vulnerabilità delle catene di approvvigionamento mondiali non rappresentano un problema soltanto per l'UE. Altri paesi dipendono dall'UE ("dipendenze inverse") e il commercio ("interdipendenza") può contribuire alla stabilità delle catene del valore mondiali. L'UE è inoltre pronta ad agire con risolutezza e a difendersi dalle pratiche commerciali sleali, quali l'uso di sovvenzioni estere distorsive, sempre nel rispetto degli impegni internazionali assunti. L'UE continuerà a sfruttare al meglio il suo pacchetto di strumenti in materia di commercio e concorrenza, assicurandosi nel contempo che tali strumenti siano efficienti e aggiornati. La Commissione ha perciò proposto nuovi strumenti, come ad esempio il regolamento relativo alle sovvenzioni estere[16], che affronta le distorsioni sul mercato interno causate dalle sovvenzioni estere.

Ulteriori misure politiche pertinenti (per esempio l'introduzione di una potenziale esenzione dall'imposta sul valore aggiunto (IVA) o l'agevolazione del trasferimento di prodotti per la difesa finanziati dall'UE) sono elencate nella comunicazione sulla difesa.

Azioni previste

- La Commissione sta studiando la possibilità di aggiungere filoni di lavoro nel settore della difesa in iniziative come l'alleanza europea per i dati industriali, l'edge e il cloud e l'alleanza industriale per i processori e le tecnologie dei semiconduttori.
- La Commissione valuterà insieme agli Stati membri la necessità di effettuare una valutazione dei rischi per le catene di approvvigionamento delle infrastrutture critiche, in particolare nel settore digitale, per tutelare meglio gli interessi dell'UE in materia di sicurezza e difesa e presenterà una relazione in merito nel 2023.
- La Commissione esorta tutti gli Stati membri che non vi hanno ancora provveduto a

[16] COM(2021) 223 final.

istituire un meccanismo nazionale di controllo degli investimenti esteri diretti.

5. Dimensione esterna

La collaborazione con partner di tutto il mondo che condividono gli stessi principi è fondamentale per potenziare la resilienza e la sicurezza dell'approvvigionamento dell'UE, riducendo nel contempo le dipendenze strategiche e aumentando i vantaggi reciproci. Il principio di reciprocità svolge un ruolo importante in questo contesto. Tra i partner tradizionali dell'UE nei settori della tecnologia, della sicurezza e della difesa figurano i membri dello Spazio economico europeo (in particolare la Norvegia), i paesi candidati, i paesi del vicinato e altri paesi terzi (per esempio Stati Uniti, Canada, Giappone, Corea del Sud) e le organizzazioni internazionali (per esempio la NATO). Tra gli scambi recenti figurano in particolare:

5.1. Consiglio UE-USA per il commercio e la tecnologia

Il Consiglio UE-USA per il commercio e la tecnologia (TTC) si è riunito per la prima volta il 29 settembre 2021. Nella dichiarazione congiunta l'UE e gli Stati Uniti hanno ribadito il loro impegno a concentrarsi per migliorare la resilienza delle rispettive catene di approvvigionamento e la sicurezza dell'approvvigionamento nei settori chiave per la transizione verde e digitale nonché a garantire la protezione dei propri cittadini e realizzare l'obiettivo di: aumentare la trasparenza dell'offerta e della domanda; mappare le rispettive capacità settoriali esistenti; scambiarsi informazioni sulle misure politiche e sulle priorità di ricerca e sviluppo; cooperare su strategie di promozione della resilienza e diversificazione della catena di approvvigionamento. I lavori in corso nei gruppi di lavoro sulle catene di approvvigionamento sicure (compreso un canale specializzato sui semiconduttori), sulla sicurezza delle tecnologie dell'informazione e della comunicazione e sul controllo delle esportazioni e degli investimenti hanno la massima pertinenza per la presente tabella di marcia. Anche il dialogo UE-Stati Uniti in materia di sicurezza e difesa, avviato di recente, potrebbe costituire la sede di discussione di tali questioni.

5.2. Partenariato con la NATO

In occasione del vertice di Bruxelles del 2021, i leader della NATO hanno definito un'agenda ambiziosa sulle tecnologie, in particolare le tecnologie emergenti e di rottura[17], che ha fornito ulteriori orientamenti per il lavoro svolto conformemente alla strategia di attuazione della NATO in materia di tecnologie emergenti e di rottura, approvata dai ministri della difesa della NATO nel febbraio 2021.

La Commissione e l'Alto rappresentante monitoreranno i progressi delle pertinenti iniziative della NATO in questo settore tramite contatti regolari con la NATO a livello operativo in vista di un'eventuale interazione reciprocamente accettabile e vantaggiosa con le pertinenti iniziative dell'UE, nella massima trasparenza nei confronti degli Stati membri, ed evitando allo stesso tempo di creare nuove dipendenze tecnologiche o di capacità ovvero di aumentare quelle esistenti.

[17] Ivi compresa la decisione di varare l'acceleratore per l'innovazione nel settore della difesa per il Nord Atlantico (DIANA) e un fondo NATO per l'innovazione.

Azioni previste

- Nell'ambito del Consiglio UE-USA per il commercio e la tecnologia e del dialogo UE-USA sulla sicurezza e la difesa avviato di recente, la Commissione e l'Alto rappresentante valuteranno come migliorare la resilienza della catena di approvvigionamento e garantire la protezione dei cittadini.
- Nel quadro delle dichiarazioni congiunte sulla cooperazione tra l'UE e la NATO e nella massima trasparenza nei confronti degli Stati membri, la Commissione e l'Alto rappresentante valuteranno insieme alla NATO come promuovere interazioni reciprocamente accettabili e vantaggiose tra le rispettive iniziative pertinenti.

6. Conclusioni

Poiché la situazione geopolitica mondiale rimane complessa e la corsa alle nuove tecnologie pertinenti per la sicurezza e la difesa continua, l'UE e gli Stati membri devono rafforzare la collaborazione in materia di tecnologie critiche per la sicurezza e la difesa a lungo termine dell'Europa, nonché aumentare gli sforzi per ridurre le dipendenze strategiche correlate.

La presente tabella di marcia propone una stretta collaborazione con gli Stati membri per individuare le tecnologie e le catene del valore critiche per la sicurezza e la difesa (nonché le cause profonde delle dipendenze strategiche correlate nell'ambito dell'osservatorio sulle tecnologie critiche) al fine di sostenere un approccio strategico coordinato a livello dell'UE in materia di tecnologie critiche pertinenti per la sicurezza e la difesa che sfrutti al meglio gli strumenti e i programmi di ricerca, sviluppo tecnologico e innovazione nazionali e dell'UE.

Al fine di potenziare la competitività e la resilienza dei settori della sicurezza e della difesa, le risultanze dell'osservatorio e i lavori correlati nell'ambito della strategia industriale aggiornata contribuiranno anche a garantire che le politiche industriali e commerciali dell'UE tengano maggiormente conto delle considerazioni in materia di sicurezza e difesa, se necessario e nel rispetto delle norme UE in materia di concorrenza e degli obblighi internazionali dell'Unione.

Le proposte avanzate nella presente tabella di marcia intendono contribuire alla dimensione relativa alla ricerca, allo sviluppo tecnologico e all'innovazione della prossima bussola strategica dell'UE, attraverso la quale gli Stati membri fisseranno obiettivi ambiziosi a lungo termine per rafforzare in misura sostanziale la sicurezza e la difesa dell'Europa.