COMMISSIONE
EUROPEA

Bruxelles, 22.2.2021
COM(2021) 70 final

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

Piano d'azione sulle sinergie tra l'industria civile, della difesa e dello spazio

1. Introduzione

Una delle innovazioni più importanti e durature del settore automobilistico in Europa proviene dall'industria della difesa. Dopo essersi dedicato alla realizzazione di seggiolini eiettabili per aerei da caccia per conto di una società aeronautica europea, Nils Ivar Bohlin, un ingegnere meccanico svedese, progettò una nuova cintura di sicurezza per una società automobilistica europea. Ispirata alle imbracature utilizzate dai piloti di caccia, la cintura di sicurezza a tre punti di ancoraggio è diventata uno standard mondiale nell'industria automobilistica e dalla sua introduzione ha salvato più di un milione di vite.

Questo esempio illustra l'intento con cui la presidente von der Leyen ha incaricato[1] la Commissione di "garantire il reciproco arricchimento tra l'industria civile, della difesa e dello spazio" e di "concentrarsi sul miglioramento del legame fondamentale tra spazio, difesa e sicurezza". A tale scopo, nel marzo 2020 è stato annunciato, nell'ambito della strategia industriale per l'Europa[2], un "piano di azione sulle sinergie tra l'industria civile, della difesa e dello spazio, anche a livello di programmi, tecnologie, innovazione e start-up", che è stato accolto con favore dal Consiglio[3].

Il presente piano d'azione (il **"piano in tre punti"**) getta le basi per la realizzazione di iniziative politiche concrete incentrate su tre obiettivi principali:

- rafforzare la complementarità tra i programmi e gli strumenti pertinenti dell'UE per incrementare l'efficienza degli investimenti e l'efficacia dei risultati (le "*sinergie*");
- promuovere i vantaggi economici e tecnologici per i cittadini dell'UE derivanti dai finanziamenti dell'UE a favore di ricerca e sviluppo, anche nei settori della difesa e dello spazio (gli "*spin-off*")[4];
- favorire l'utilizzo dei risultati della ricerca e dell'innovazione nell'industria civile nell'ambito dei progetti di cooperazione europea in materia di difesa (gli "*spin-in*").

Sinergie: in un contesto internazionale difficile, nel quale l'UE deve mantenere il proprio vantaggio tecnologico e sostenere la propria base industriale, il quadro finanziario pluriennale (QFP) dell'UE per il periodo 2021-2027 prevede un incremento significativo degli investimenti nelle tecnologie per la difesa o gli usi civili connessi, quali sicurezza, mobilità, salute, gestione delle informazioni, informatica e spazio. I programmi pertinenti del QFP riguardano in modo complementare la ricerca, lo sviluppo, la dimostrazione, la realizzazione di prototipi e la diffusione (appalti di prodotti e servizi innovativi).

La pervasività delle tecnologie emergenti e di rottura nelle industrie civile, della difesa e dello spazio crea nuove opportunità di sinergie tra i programmi e gli strumenti dell'UE[5]. Un approccio strutturato, che stabilisca processi e meccanismi adeguati tra questi strumenti tenendo conto delle loro finalità e limitazioni specifiche, comporterà finanziamenti più mirati, ridurrà i rischi di duplicazione e massimizzerà il valore aggiunto per i contribuenti dell'UE.

Spin-off: l'aumento degli investimenti nella difesa deve anche rappresentare un vantaggio per l'economia nel suo insieme, nel pieno rispetto dei vincoli inerenti al settore della difesa

[1] Cfr. lettere di incarico alla vicepresidente esecutiva Vestager e al commissario Breton.

[2] Comunicazione COM(2020) 102 del 10.3.2020.

[3] Conclusioni del Consiglio sulla sicurezza e la difesa, 8910/20 del 17 giugno 2020: "Il Consiglio [...] accoglie con favore la richiesta di maggiori sinergie tra le industrie civili e quelle della difesa, anche per quanto riguarda lo spazio, nei programmi dell'UE, nel rispetto della natura e delle basi giuridiche diverse dei rispettivi programmi e iniziative dell'UE, compresa la natura civile dei programmi spaziali europei, al fine di rendere più efficace l'uso delle risorse e delle tecnologie e creare economie di scala."

[4] A medio e lungo termine, quando non sarà più necessario proteggere i principali mezzi di superiorità operativa.

[5] L'allegato IV del "Regolamento che istituisce Orizzonte Europa - il programma quadro di ricerca e innovazione - e ne stabilisce le norme di partecipazione e diffusione" contiene disposizioni specifiche per le sinergie con altri programmi.

(ad esempio il ruolo delle autorità nazionali nell'orientare la domanda, la gestione delle informazioni o le norme specifiche in materia di diritti di proprietà intellettuale). Anche una maggiore sensibilizzazione dell'opinione pubblica in merito al notevole effetto moltiplicatore della spesa dell'UE in ricerca e sviluppo (R&S) nei settori della sicurezza, della difesa e dello spazio contribuisce a consolidare il sostegno pubblico a queste iniziative.

Tali spese rispondono all'esigenza pubblica di una maggiore sicurezza e costituiscono un investimento a lungo termine nello sviluppo tecnologico sostenibile, nella resilienza economica e nella crescita. Diverse imprese europee che operano a livello mondiale devono la loro posizione agli spin-off della ricerca europea in materia di difesa, dalla tecnologia delle fibre ottiche agli aeromobili civili o persino al cibo in scatola. Analogamente, molte innovazioni utilizzate per la prima volta nello spazio hanno avuto successo in ambito civile, come ad esempio i sensori di imaging digitale, i microinfusori di insulina o le cuffie wireless. I dati e i servizi spaziali generati da Galileo, EGNOS e Copernicus sono utilizzati per applicazioni in numerosi settori all'interno e all'esterno dell'UE, con notevoli vantaggi in termini di benessere economico e qualità generale della vita.

Spin-in: in molti casi è sempre più difficile tracciare una chiara linea di demarcazione tra ricerca civile e ricerca relativa alla difesa, in particolare per le tecnologie di base (bassi livelli di maturità tecnologica, *Technology Readiness Levels* - TRL). Le applicazioni civili della tecnologia stanno diventando sempre più economiche grazie alla globalizzazione delle conoscenze, all'accesso a un pubblico più ampio e all'accesso generalizzato ai dati. Al tempo stesso, molte tecnologie emergenti e digitali offrono un notevole potenziale per la difesa, tra cui intelligenza artificiale (IA), microelettronica, infrastrutture cloud di dati e robotica.

L'innovazione in questi settori proviene spesso dalle start-up, dalle piccole e medie imprese (PMI) e dalle organizzazioni di ricerca e tecnologia (ORT). Ove possibile, l'industria europea della difesa dovrebbe poter attingere ai risultati della ricerca dell'industria civile dell'UE per evitare costose duplicazioni delle attività di ricerca[6].

La promozione di sinergie tra gli strumenti pertinenti finanziati dall'UE e l'agevolazione del reciproco arricchimento tra le industrie civile, della difesa e dello spazio (spin-in e spin-off) possono rafforzare la crescita economica europea, sviluppare ulteriormente il mercato unico e migliorare la sicurezza per i cittadini europei.

Attingere alle competenze di tutta l'Unione, oltre che dei leader consolidati delle industrie civile, della difesa e dello spazio, comprese le PMI e le start-up, contribuirà a rafforzare la cooperazione, la competitività e la resilienza a livello europeo.

In tale contesto, il presente piano d'azione presenta **11 azioni**[7] volte a: a) rafforzare l'approccio basato sulle capacità nel settore della sicurezza; b) migliorare le sinergie tra i programmi e gli strumenti dell'UE; c) sostenere start-up, PMI e ORT; d) monitorare le tecnologie critiche per ridurre le dipendenze; e) promuovere la standardizzazione delle norme ibride in ambito civile/di difesa; f) stimolare l'innovazione e il reciproco arricchimento tra le industrie civile, della difesa e dello spazio; e g) avviare tre progetti faro che potrebbero rappresentare una svolta.

[6] Cfr., ad esempio, la relazione *Horizon 2020-funded security research projects with dual-use potential: An overview (2014-2018)*, EUR 30210 EN, del Centro comune di ricerca.

[7] Tutte le azioni devono essere pienamente conformi al diritto nazionale, dell'UE e internazionale applicabile, comprese le norme in materia di concorrenza.

Sebbene il mandato del presente piano d'azione sia limitato ai programmi e agli strumenti dell'UE[8], la promozione di sinergie a livello dell'UE può innescare azioni analoghe a livello nazionale e regionale, anche attraverso il cofinanziamento nazionale di progetti dell'UE, moltiplicando così l'effetto positivo previsto.

Benché non rientrino nell'ambito di applicazione del presente piano d'azione, saranno prese in considerazione anche le pertinenti iniziative in materia di sicurezza e difesa sotto la guida degli Stati membri[9], in particolare la bussola strategica, la revisione coordinata annuale sulla difesa (CARD), la cooperazione strutturata permanente (PESCO) e il patto sulla dimensione civile della PSDC[10]. Ove opportuno, si terrà conto inoltre della cooperazione UE-NATO, anche per quanto riguarda l'interoperabilità. I servizi della Commissione continueranno a lavorare in stretta collaborazione con il servizio europeo per l'azione esterna (SEAE) e con l'Agenzia europea per la difesa (AED), le cui attività pertinenti saranno prese in considerazione nella ricerca di sinergie e scambi di conoscenze[11].

In un contesto geopolitico più ampio, l'UE si è impegnata a sviluppare un approccio transatlantico comune in materia di protezione delle tecnologie critiche alla luce delle preoccupazioni economiche e di sicurezza globali e a collaborare nell'ambito della tecnologia, del commercio e delle norme. Il partenariato transatlantico e la cooperazione con altri paesi che condividono gli stessi principi possono sostenere gli sforzi dell'UE in questo ambito.

2. L'approccio basato sulle capacità

Le industrie dello spazio, della difesa e della sicurezza sono strategiche per l'Europa. La strategia digitale dell'UE[12], adottata nel febbraio 2020, ha sottolineato l'importanza della leadership dell'UE nelle tecnologie digitali e nella cibersicurezza e ha previsto un livello di investimenti senza precedenti nella transizione digitale dell'UE nei prossimi sette anni. Nell'ottobre 2020[13] il Consiglio europeo ha sottolineato che raggiungere l'autonomia strategica mantenendo nel contempo un'economia aperta è un obiettivo fondamentale dell'Unione e ha invitato a sviluppare l'autonomia dell'UE nel settore spaziale e una base industriale della difesa più integrata. Nel luglio 2020 la strategia dell'UE per l'Unione della sicurezza[14] ha sottolineato la necessità di rafforzare ulteriormente la ricerca e l'innovazione in materia di sicurezza; il piano d'azione potrebbe rispondere anche a questa esigenza e sostenere le industrie della sicurezza dell'UE con soluzioni innovative e all'avanguardia derivanti dal reciproco arricchimento e da sinergie efficienti tra l'industria civile, della difesa e dello spazio. Il Green Deal dell'UE ha posto l'accento su una transizione ambiziosa verso una società trasformativa, che richiederà una ricerca e un'innovazione sostanziali nel campo delle tecnologie e delle transizioni sociali e stimolerà notevoli progressi in molti settori.

L'ecosistema industriale aerospaziale e della difesa comprende i settori aeronautico, dello spazio e della difesa. Rappresenta 376 miliardi di EUR di fatturato annuo, 44 000 imprese

[8] I finanziamenti dell'UE devono essere pienamente conformi al diritto applicabile, compresi i trattati, il regolamento finanziario e le norme specifiche definite nel pertinente atto di base per un programma o uno strumento di finanziamento.

[9] Sviluppate nel quadro della politica estera e di sicurezza comune (PESC)/della politica di sicurezza e di difesa comune (PSDC).

[10] Il "cluster dei PNA (piani nazionali di attuazione)" di recente introduzione in materia di sicurezza, tecnologia e RSI (ricerca, sviluppo e innovazione) per lo sviluppo delle capacità nazionali nella PSDC civile mira a individuare e utilizzare i programmi pertinenti dell'UE.

[11] In linea con l'obbligo della Commissione e del Consiglio, assistiti dall'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, di garantire la coerenza tra l'azione esterna e le politiche interne (articolo 21, paragrafo 3, TUE).

[12] Comunicazione COM(2020) 67 del 19.2.2020, "Plasmare il futuro digitale dell'Europa".

[13] Conclusioni del Consiglio europeo, EUCO 13/20 del 2 ottobre 2020.

[14] COM(2020) 605 del 24.7.2020.

e 1,5 milioni di dipendenti[15]. Secondo i dati del 2015[16], l'industria della sicurezza in Europa impiega 4,7 milioni di persone e realizza un fatturato annuo di 200 miliardi di EUR in oltre 20 sottosettori dell'economia europea. La maggior parte delle imprese aveva registrato una crescita che secondo le previsioni era destinata a proseguire, ma la COVID-19 ha invertito questa tendenza.

Il presente piano d'azione riguarda i settori dello spazio e della difesa di questo ecosistema, nonché le loro interazioni con i settori civili (come la sicurezza). Queste industrie stanno cercando di riprendersi dalla crisi, ma anche di rispondere alla duplice transizione verde e digitale e di plasmarne l'accelerazione. Si tratta di industrie ad alta tecnologia che impiegano lavoratori altamente qualificati e tendono ad esportare gran parte dei loro prodotti. Gli stessi grandi attori industriali sono spesso coinvolti nei settori dello spazio, della difesa e in numerosi settori civili (quali sicurezza, aeronautica o digitale). Si basano sulla collaborazione internazionale, stanno cercando di diventare più resilienti e presentano catene del valore dinamiche. I recenti sviluppi tecnologici mostrano una tendenza mutevole in cui l'innovazione civile, in particolare quella delle start-up e delle PMI, stimola sempre più l'innovazione nel settore della difesa.

I settori dello spazio, della difesa e della sicurezza offrono possibilità di sinergie e scambi di conoscenze reciproci e con altri settori civili. Tali settori devono far fronte a numerose sfide e vincoli, tra cui ostacoli normativi, mancanza di parità di condizioni sui mercati internazionali, accesso a costose infrastrutture di ricerca e sperimentazione, necessità di competenze specializzate, scarsa attrattiva per le donne e i giovani in particolare, accesso a materiali o componenti critici e necessità di norme e certificazioni europee. Sono inoltre conformi ai controlli specifici sulle esportazioni per i prodotti della difesa e i prodotti a duplice uso[17]. Poiché sviluppano tecnologie o infrastrutture con possibili implicazioni per la sicurezza, possono essere sottoposti al controllo degli investimenti esteri diretti[18].

Per comprendere meglio le interconnessioni tra questi e altri settori civili, la Commissione continuerà a consultare tutti i portatori di interessi. In particolare, cercherà di affrontare le sfide cui devono far fronte PMI, start-up, ORT e il mondo accademico europei e che impediscono loro di svolgere un ruolo più attivo: tra queste sfide figurano gli elevati requisiti in materia di sicurezza, l'espansione per rispondere alle esigenze del mercato, l'accesso al credito (finanziamenti, investimenti privati), l'accesso ai mercati dei paesi terzi, l'accesso alle infrastrutture di sperimentazione e l'insufficiente riduzione dei rischi degli investimenti nella ricerca.

Un modo per affrontare queste sfide è promuovere l'approccio basato sulle capacità (*capability driven approach*, CDA). Un approccio di tipo CDA presenta due caratteristiche fondamentali: da un lato, gli utenti definiscono le capacità di cui hanno bisogno e, dall'altro, esprimono la loro intenzione di acquistare prodotti che, una volta sviluppati, offriranno la capacità desiderata. Tale approccio si è rivelato utile nei settori dello spazio e della difesa in quanto consente un orientamento strategico chiaro, una mentalità lungimirante, una pianificazione a lungo termine, un approccio interdisciplinare che coinvolge tutti i portatori di interessi e prevede la sincronizzazione dei vari processi.

---

[15] I calcoli si basano sulle statistiche strutturali delle imprese e sullo studio *National accounts aggregates by industry* di Eurostat. La maggior parte dei valori si riferisce all'UE-27, 2017. I valori mancanti sono sostituiti dai dati disponibili più recenti.

[16] Cfr. la relazione del 2015 qui. Questi dati potrebbero non essere del tutto esatti perché la maggior parte delle organizzazioni industriali è attiva sia nel settore della difesa che in quello della sicurezza. Di recente la Commissione ha avviato un nuovo studio.

[17] In linea con il regolamento del Consiglio sul commercio di prodotti a duplice uso, nel presente piano d'azione i prodotti a duplice uso sono definiti come i prodotti, i software e le tecnologie che possono avere un utilizzo per applicazioni sia civili che di difesa.

[18] Regolamento (UE) 2019/452 del 19 marzo 2019. L'attuazione e l'applicazione del regolamento possono contribuire a salvaguardare le tecnologie e le infrastrutture critiche in modo da apportare benefici anche agli operatori dell'UE che vi fanno affidamento.

Il Fondo europeo per la difesa (FED) e i suoi programmi precursori[19] si basano su un approccio di tipo CDA, tenendo conto in particolare degli strumenti e dei processi di definizione delle priorità dell'UE in materia di difesa[20] che sostengono il processo decisionale a livello nazionale e dell'UE. Ciò contribuisce ad aumentare la convergenza della pianificazione della difesa negli Stati membri e fornisce riferimenti per uno sviluppo più coerente delle capacità di difesa dell'Europa.

Il quadro di governance spaziale consolidato e il finanziamento stabile da parte degli Stati membri attraverso l'Agenzia spaziale europea e a titolo del bilancio dell'Unione hanno altresì consentito l'attuazione di un approccio di tipo CDA per il settore dello spazio. Il CDA garantisce che i futuri sistemi spaziali siano in grado di offrire capacità che rispondano in modo ottimale alle esigenze dell'UE in materia di monitoraggio dell'ambiente o della sicurezza, sicurezza delle comunicazioni, posizionamento, navigazione e misurazione del tempo, ecc.

Con la significativa eccezione della gestione integrata delle frontiere[21], **non esiste un analogo processo onnicomprensivo di tipo CDA per il settore della sicurezza dell'UE**. L'elevata diversità geografica, tematica e degli utenti dà origine a diversi "sottosettori della sicurezza" con vari approcci adattati alle loro esigenze specifiche. La mancanza di una pianificazione coordinata può portare a un'eccessiva dipendenza dalle tecnologie importate già disponibili sul mercato. Pur mantenendo la flessibilità necessaria per ciascun sottosettore della sicurezza, un approccio di tipo CDA può apportare un contributo positivo a un settore della sicurezza moderno e orientato al futuro. Può favorire l'uso di tecnologie innovative al fine di rispondere all'evoluzione dei problemi di sicurezza delle autorità di contrasto (ad esempio polizia, autorità doganali e altre autorità di ispezione) e andare incontro agli interessi delle autorità degli Stati membri, agevolando anche il rispetto delle norme europee in materia di etica e protezione dei dati.

L'UE si trova in una posizione ideale per promuovere un CDA in tutto il settore della sicurezza. Il rafforzamento del CDA nelle agenzie dell'UE, ad esempio, può contribuire a strutturare le esigenze degli utenti, individuare le vulnerabilità, colmare le lacune in termini di capacità, definire tabelle di marcia tecnologiche e opportunità di ricerca, garantire la corretta transizione dalla fase di R&S alle operazioni e creare opportunità di aggiudicazione congiunta. Si terrà conto anche delle possibili sinergie con la gestione civile delle crisi.

Azione 1: entro la fine del 2021 la Commissione presenterà una proposta per rafforzare l'individuazione tempestiva e orientata al futuro delle esigenze e delle soluzioni nel campo della sicurezza interna e delle attività di contrasto, promuovendo **approcci basati sulle capacità in tutti i settori della sicurezza**, sulla base delle migliori pratiche dei settori della difesa e dello spazio.

3. Sinergie tra i programmi e gli strumenti dell'UE

Nell'ambito del QFP 2021-2027, l'UE incrementerà gli investimenti nelle tecnologie per applicazioni civili, di difesa e spaziali mediante: a) programmi di ricerca, sviluppo e

[19] L'azione preparatoria sulla ricerca in materia di difesa e il programma europeo di sviluppo del settore industriale della difesa.

[20] In particolare, il piano di sviluppo delle capacità (e la relativa casistica di contesti strategici) e la revisione annuale coordinata sulla difesa.

[21] A norma dell'articolo 9 del regolamento (UE) 2019/1896 relativo alla guardia di frontiera e costiera europea, è stata stabilita una procedura specifica di pianificazione dello sviluppo delle capacità per la gestione integrata delle frontiere dell'UE. Ciò favorirà il coordinamento dei piani nazionali di sviluppo delle capacità degli Stati membri relativi alla gestione delle frontiere e dei piani di capacità della stessa FRONTEX. Tale procedura di pianificazione dello sviluppo delle capacità sosterrà l'impiego del corpo permanente della guardia di frontiera e costiera europea e orienterà la programmazione degli strumenti pertinenti dell'UE.

diffusione quali Orizzonte Europa, il programma Europa digitale (DEP), il meccanismo per collegare l'Europa (MCE), il Fondo sicurezza interna, il FED e il programma spaziale; b) appalti[22] per soluzioni tecnologiche intersettoriali innovative.

Le attività di R&S nel settore della difesa sono previste dal FED. Anche i programmi della politica di coesione possono contribuire alle attività di R&S nel settore della difesa, a condizione che siano in linea con le norme pertinenti in materia di gestione concorrente. Altri strumenti di finanziamento si concentrano sulle applicazioni civili, mentre i rispettivi regolamenti contengono spesso disposizioni sul duplice uso[23]. Ad esempio, nel settore della protezione civile, rescEU[24] erogherà finanziamenti agli Stati membri e agli Stati partecipanti per sviluppare le capacità dell'UE di rispondere alle catastrofi chimiche, biologiche, radiologiche e nucleari (CBRN) qualora le capacità nazionali si rivelino insufficienti.

Il QFP comprende anche strumenti orizzontali a sostegno delle politiche marittime e dei trasporti. Particolarmente importanti sono i programmi (ad esempio il Fondo per la gestione integrata delle frontiere) o le agenzie dell'UE (ad esempio FRONTEX, l'Agenzia europea della guardia di frontiera e costiera) che mirano a migliorare la sicurezza interna ed esterna e la protezione dell'UE. Inoltre il dispositivo per la ripresa e la resilienza dell'UE e lo strumento di sostegno tecnico sosterranno le riforme e gli investimenti degli Stati membri, a condizione che siano in linea con le priorità stabilite dall'UE, in particolare quelle relative alle transizioni verde e digitale.

L'aumento della portata di questi investimenti, realizzato attraverso una serie di programmi e strumenti dell'UE, favorisce la creazione di sinergie che possono evitare il rischio di duplicazioni e assicurare opportunità di finanziamento più facilmente fruibili (ad esempio sovvenzioni, appalti pubblici, garanzie). Esse sosterranno i progetti lungo il percorso dalle attività di R&S alla diffusione tramite l'immissione sul mercato o gli appalti pubblici per l'innovazione.

Il QFP comprende anche strumenti volti a sostenere: investimenti (ad esempio InvestEU); progetti regionali per la ricerca, l'innovazione, le tecnologie e le PMI (ad esempio a titolo del FESR o del Fondo sociale europeo - FSE); innovazione tecnologica, start-up e PMI (ad esempio la ricerca collaborativa di Orizzonte Europa comprendente partenariati e missioni, in particolare gli strumenti Pathfinder e Accelerator del Consiglio europeo per l'innovazione - CEI) o i poli europei dell'innovazione digitale.

Qualora i programmi dell'UE prevedano esenzioni in materia di sicurezza, la Commissione e le agenzie dell'UE limiteranno, per motivi debitamente giustificati, la partecipazione agli appalti ai soggetti giuridici costituiti negli Stati membri o che non siano controllati da paesi terzi.

Le misure volte a migliorare l'accesso ai finanziamenti e le sinergie nell'ambito dei programmi del QFP possono includere:

- meccanismi di **finanziamento misto** a livello dell'UE, che combinano diverse forme di sostegno agli investimenti a titolo del bilancio dell'UE (ad esempio sovvenzioni e risorse rimborsabili) e altre fonti di finanziamento per una maggiore efficacia;
- gli **strumenti Pathfinder e Accelerator del CEI**, il cui obiettivo sarà sfruttare al meglio la solida base di ricerca dell'Europa e sostenere le innovazioni rivoluzionarie;

[22] Appalti diretti dell'UE o sostegno agli appalti da parte degli Stati membri.

[23] Il programma Orizzonte Europa prevede che le sinergie con il FED andranno a beneficio della ricerca in ambito civile e di difesa, anche se le attività del programma quadro si concentreranno esclusivamente sulle applicazioni civili.

[24] rescEU fa parte del meccanismo di protezione civile dell'UE.

- **sinergie tra Orizzonte Europa e altri programmi del QFP a gestione diretta** (se le rispettive basi giuridiche lo consentono), che costituiscono una leva strategica significativa grazie alla possibilità di combinare i finanziamenti. Anche i programmi in regime di gestione concorrente (ad esempio il FESR) possono essere presi in considerazione per il trasferimento di fondi (trasferimenti volontari tra fondi o verso strumenti a gestione diretta o indiretta e il meccanismo del marchio di eccellenza).

Oltre a queste misure, la Commissione ribadisce il proprio sostegno, già affermato nel piano d'azione europeo in materia di difesa del 2016[25] e nelle conclusioni del Consiglio europeo di dicembre 2016[26], a favore di un adeguamento dei criteri di prestito della Banca europea per gli investimenti (BEI) al settore della difesa entro i limiti stabiliti dai trattati.

Azione 2: entro la fine del 2021 e in vista dei programmi di lavoro del 2022 la Commissione rafforzerà ulteriormente il proprio processo interno **per promuovere sinergie** tra le industrie dello spazio, della difesa e le industrie civili connesse, migliorando il coordinamento dei programmi e degli strumenti dell'UE e avviando azioni volte ad agevolare l'accesso ai finanziamenti.

4. Sostegno alle start-up, alle PMI e alle ORT

Salvo poche eccezioni, il livello di partecipazione delle start-up, delle PMI e delle ORT ai mercati della difesa e della sicurezza è ancora basso. Dato il potenziale di questi tipi di organizzazioni, è necessario agevolare la creazione di opportunità di "spin-in" dalle industrie civili alla difesa. A tal fine, le PMI e le start-up di tutta l'Unione:

- dovrebbero essere maggiormente consapevoli delle potenziali opportunità commerciali, in particolare nel mercato della difesa;
- dovrebbero avere un quadro d'insieme completo delle opportunità offerte dagli inviti a presentare proposte nell'ambito dei programmi dell'UE nel settore dello spazio, della difesa e dell'industria civile connessa;
- devono adeguare i propri prodotti/modelli imprenditoriali alle specificità di tali mercati.

Le ORT potrebbero svolgere un ruolo importante a sostegno delle PMI, in quanto sono in grado di apportare idee e approcci innovativi. Tale innovazione ha il potenziale per plasmare le reti esistenti e creare nuove interazioni tra istituzioni di difesa, industria e ORT. La capacità di coinvolgere le PMI e le ORT in tutta l'Unione sarà fondamentale per garantire la diversità necessaria in termini di innovazione e specializzazione.

Dai fornitori di dati spaziali quali Galileo o Copernicus alle nuove forme di rappresentazione e analisi dei dati, tra cui Destination Earth[27], i poli europei dell'innovazione digitale possono riunire PMI innovative lungo la catena del valore dei dati. Per sostenere ulteriormente le PMI, le start-up e le ORT dell'UE e garantire il reciproco arricchimento tra le industrie civile, della difesa e dello spazio, la Commissione intende:

- intensificare le sue attività di sensibilizzazione, coinvolgendo anche la rete europea di regioni connesse con il settore della difesa, la rete europea di ricerca e innovazione

[25] COM(2016) 950 del 30.11.2016.

[26] Nelle conclusioni del Consiglio europeo del 15 dicembre 2016, si invitava la BEI "a valutare iniziative per sostenere gli investimenti in attività di ricerca e sviluppo nel settore della difesa".

[27] "Destination Earth" è un'iniziativa dell'UE volta a sviluppare un modello digitale ad altissima precisione della Terra per monitorare e simulare le attività naturali e umane, nonché a elaborare e sperimentare scenari che consentano uno sviluppo più sostenibile e sostengano le politiche ambientali europee.

in materia di difesa, la rete Enterprise Europe e i cluster industriali, come quelli sulla piattaforma europea di collaborazione tra cluster[28];

- ricorrere ai comunicatori dell'UE sul campo, quali le rappresentanze della Commissione e le reti di sensibilizzazione dell'UE presenti negli Stati membri, per contribuire alla diffusione di messaggi chiave e alla creazione di partenariati;
- basarsi sulle reti esistenti e sugli organismi dell'UE per sviluppare partenariati industriali e scientifici nel campo delle tecnologie critiche;
- facilitare l'accesso al sostegno dell'UE attraverso uno strumento interattivo multilingue che orienti le imprese verso i finanziamenti dell'UE più adatti al loro progetto;
- valutare le opportunità di creazione di punti focali nazionali per tutti gli aspetti della partecipazione al FED, cercando sinergie con altre entità che promuovano le opportunità di finanziamento dell'UE;
- promuovere ulteriormente le opportunità offerte dall'iniziativa per l'imprenditoria spaziale CASSINI per l'accelerazione e l'incubazione di imprese, i finanziamenti di avviamento e gli appalti pre-commerciali, nonché il partenariato e gli appalti per l'innovazione;
- collaborare con il CEI per fornire servizi di accelerazione per le start-up/PMI civili ad alta tecnologia al fine di raggiungere i mercati della difesa e della sicurezza;
- sostenere la creazione di poli europei dell'innovazione digitale, come previsto dalla strategia industriale dell'UE, che fungano da sportelli unici per l'accesso delle imprese alla sperimentazione tecnologica e presentare soluzioni innovative per i mercati civile, della difesa e dello spazio;
- fornire supporto tecnico e formazione pratica alle start-up, PMI e ORT interessate ad aderire ai programmi e agli strumenti pertinenti dell'UE;
- organizzare attività di sensibilizzazione quali competizioni, hackathon, laboratori di start-up, giornate della tecnologia, forum sull'innovazione, *serious gaming*, seminari sulle previsioni e sullo sviluppo di competenze.

Azione 3: a partire dalla seconda metà del 2021 la Commissione annuncerà azioni mirate per **start-up, PMI e ORT** al fine di sensibilizzarle ai programmi e agli strumenti dell'UE che offrono opportunità di finanziamento, forniscono supporto tecnico e formazione pratica, offrono servizi di accelerazione delle imprese, presentano soluzioni innovative e agevolano l'accesso al mercato della difesa, della sicurezza, dello spazio o di altri mercati civili pertinenti.

5. Tecnologie critiche e tabelle di marcia tecnologiche

Nei suoi orientamenti politici del 2019, la presidente von der Leyen ha sottolineato che "non è troppo tardi perché l'Europa consegua una **sovranità tecnologica** in alcuni settori tecnologici fondamentali". Nella strategia industriale dell'UE per il 2020 si affermava: "L'autonomia strategica dell'Europa consiste nel ridurre la dipendenza dalle fonti esterne per ciò di cui abbiamo più bisogno: materiali e tecnologie critici, prodotti alimentari, infrastrutture, sicurezza e altri settori strategici. Ciò offre inoltre all'industria europea l'opportunità di sviluppare mercati, prodotti e servizi che stimolano la competitività." L'UE sosterrà pertanto lo sviluppo di tecnologie critiche che rivestono un'importanza strategica per l'Europa.

[28] https://www.endr.eu/, https://www.edrin.org/, https://een.ec.europa.eu/, https://www.clustercollaboration.eu.

Per alcune di queste tecnologie, la Commissione si è avvalsa della sua capacità di mobilitazione per avviare alleanze industriali[29]. Tali alleanze esistono già per le tecnologie energetiche (batterie, idrogeno pulito) e per le materie prime, mentre altre sono in esame.

Individuare quali tecnologie critiche apportino un contributo decisivo alle capacità fondamentali può contribuire a decidere: i) quali tecnologie siano importanti per la sovranità tecnologica (cioè quando sia necessario ridurre il rischio di dipendenza); ii) se un sostegno combinato/coordinato proveniente da diversi programmi e strumenti dell'UE possa far fronte a tali sfide. Per rafforzare la propria sovranità tecnologica, l'UE deve mantenere una forte competenza industriale e, ove possibile, puntare alla leadership nelle suddette tecnologie critiche. Oltre a queste ultime, l'UE deve considerare anche:

- le catene del valore, compresa la sicurezza dell'approvvigionamento di materiali (materie prime) essenziali che sono elementi fondamentali delle tecnologie critiche civili, di difesa e spaziali[30,31,32];
- le relative infrastrutture di ricerca e di sperimentazione, fondamentali per la normazione e la certificazione.

Nel contesto del presente piano d'azione, le tecnologie critiche sono tecnologie[33] che rivestono un'importanza trasversale nelle industrie della difesa, dello spazio e nelle industrie civili connesse e che contribuiscono alla sovranità tecnologica dell'Europa riducendo i rischi di eccessiva dipendenza da terzi per ciò di cui abbiamo più bisogno. La tabella seguente presenta un **elenco[34,35] di esempi di tecnologie critiche che rivestono un'importanza trasversale nelle pertinenti industrie civili (compresa la sicurezza), della difesa e dello spazio** (non sono incluse le tecnologie la cui rilevanza è limitata a una sola di tali industrie).

Settore	***Tecnologie***
Elettronica e digitale	• *Intelligenza artificiale, analisi avanzata e big data* • *Cibersicurezza e tecnologie di ciberdifesa* • *Tecnologie digitali forensi* • *Calcolo ad alte prestazioni, cloud e spazi di dati* • *Fotonica* • *Microprocessori a bassissima potenza, elettronica leggera stampata o flessibile* • *Tecnologie quantistiche* • *Comunicazioni e reti sicure* • *Sensori (elettroottici, radar, chimici, biologici, di radiazione, ecc.)*

[29] Le alleanze industriali servono a riunire e mettere insieme un'ampia gamma di portatori di interessi in un dato ecosistema o una determinata catena del valore in cui vi siano: i) una motivazione urgente per cambiare il modello imprenditoriale; ii) il rischio di essere esclusi dai mercati fondamentali per il futuro dell'industria/dell'economia dell'UE; o iii) l'opportunità di conquistare un mercato promettente e adeguato alle esigenze future, con conseguenti effetti di ricaduta.

[30] CE, Resilienza delle materie prime critiche: tracciare un percorso verso una maggiore sicurezza e sostenibilità, COM(2020) 474 final.

[31] JRC, 2019, *Materials dependencies for dual-use technologies relevant to Europe's defence sector*, JRC117729.

[32] CE, 2020, *Critical raw materials for strategic technologies and sectors in the EU – a Foresight study*.

[33] Comprese, se del caso, le relative tecnologie abilitanti fondamentali individuate, che costituiscono una categoria complementare distinta.

[34] L'elenco si basa sulle tecnologie critiche presentate nella comunicazione del 2020 sulla strategia industriale e nel regolamento sul controllo delle esportazioni di prodotti a duplice uso. Tiene conto dell'elenco UE delle tecnologie abilitanti fondamentali e il suo approccio è coerente con la recente analisi dell'industria dell'UE.

[35] Alcune tecnologie possono riguardare più di un settore.

Produzione	• *Produzione avanzata e additiva* • *Tecnologie dei materiali avanzati e materiali sostenibili per progettazione* • *Nanotecnologie* • *Robotica* • *Semiconduttori e microelettronica*
Spazio e aeronautica	• *Tecnologie spaziali (compresa la progettazione e la produzione di lanciatori e satelliti)* • *Tecnologie sicure e di precisione per la misurazione del tempo, il posizionamento e la navigazione* • *Tecnologie di osservazione della Terra ad alta definizione* • *Comunicazione e connettività sicure via satellite*
Salute	• *Biotecnologie* • *Tecnologie chimiche, biologiche, radiologiche e nucleari*[36]
Energia	• *Tecnologie energetiche (compreso lo stoccaggio di energia, la resilienza energetica, le energie rinnovabili, l'idrogeno e il nucleare)*
Mobilità	• *Sistemi autonomi*

Le tecnologie critiche sono destinate a cambiare con l'emergere di nuove tecnologie. La Commissione istituirà, nell'ambito dei suoi servizi, un osservatorio dell'UE sulle tecnologie critiche[37]. Esso monitorerà e analizzerà periodicamente le tecnologie critiche, le loro potenziali applicazioni, le catene del valore, le infrastrutture di ricerca e di sperimentazione necessarie, il livello auspicato di controllo dell'UE su tali tecnologie e le lacune e dipendenze esistenti[38]. Ogni due anni l'osservatorio, in consultazione con i principali portatori di interessi, elaborerà una relazione classificata concernente le tecnologie critiche, le dipendenze, le catene del valore e le infrastrutture di sperimentazione per le industrie della difesa, dello spazio e le industrie civili connesse[39].

Sulla base di tali relazioni, la Commissione elaborerà **tabelle di marcia tecnologiche** per stimolare il reciproco arricchimento tra le industrie civile, della difesa e dello spazio in materia di tecnologie critiche. Le tabelle di marcia tecnologiche sono sempre più utilizzate dalla Commissione[40] come tecnica flessibile per sostenere la pianificazione strategica, conciliando gli obiettivi a breve e a lungo termine con soluzioni tecnologiche specifiche.

Servendosi delle tabelle di marcia tecnologiche, la Commissione si baserà sulle tecnologie critiche individuate e: a) si dedicherà a tutti i pertinenti strumenti di finanziamento, alle esigenze politiche e all'accesso alle opportunità di finanziamento al fine di creare sinergie tra

[36] Ad esempio per l'uso in soluzioni sanitarie preventive o terapeutiche, in ambito forense, ecc.

[37] L'osservatorio collaborerà, se del caso, con gli strumenti di monitoraggio delle tecnologie dell'UE esistenti, come quelli della Commissione (https://ati.ec.europa.eu/) o dell'AED.

[38] Le dipendenze critiche nell'interazione tra le tecnologie civili, di difesa e spaziali sono un sottoinsieme specifico (e quindi pienamente allineato) dell'intera serie di dipendenze critiche industriali trattate dalla strategia industriale dell'UE, che ha un ambito di applicazione molto più ampio.

[39] Si terrà conto, se del caso, dell'operato dell'AED sulle tecnologie critiche, anche tramite l'agenda strategica di ricerca onnicomprensiva (OSRA) e i relativi elementi tecnologici (*Technology Building Blocks*, TBB).

[40] Cfr. anche la comunicazione COM(2020) 628 del 30.9.2020, "Un nuovo SER per la ricerca e l'innovazione".

le azioni dell'UE; b) mirerà a soddisfare esigenze tecnologiche e socioeconomiche più ampie al fine di promuovere il reciproco arricchimento tra industrie; c) riunirà tutti i portatori di interessi, compresi i governi, l'industria, il mondo accademico e la società civile.

Le tabelle di marcia tecnologiche utilizzeranno la previsione tecnologica per individuare le tecnologie emergenti idonee, evitare la duplicazione dei costi, contribuire alla stabilità del mercato in Europa, promuovere la cooperazione transfrontaliera e stimolare l'innovazione da parte delle start-up e delle PMI. Ogni tabella di marcia avrà un orizzonte specifico, tappe fondamentali e un obiettivo finale concreto.

Sulla base dei risultati dei lavori svolti nell'ambito delle tabelle di marcia tecnologiche, la Commissione potrà decidere di avviare progetti faro, tenendo conto dei loro probabili effetti sulla sovranità tecnologica e sulla leadership dell'UE, sulle loro fonti di finanziamento e sulla loro governance (cfr. sezione 8).

Azione 4: la Commissione elaborerà **tabelle di marcia tecnologiche** per stimolare l'innovazione nell'ambito delle tecnologie critiche per i settori della difesa, dello spazio e civili connessi e promuovere la cooperazione transfrontaliera utilizzando in modo sinergico tutti gli strumenti pertinenti dell'UE. Tali tabelle di marcia si baseranno su una valutazione effettuata ogni due anni da un nuovo **osservatorio per le tecnologie critiche** all'interno della Commissione. Le tabelle di marcia potranno portare all'avvio di nuovi progetti faro.

6. Normazione

La promozione e l'applicazione di norme comuni in tutti i settori possono contribuire a rendere meno dispendiosi i cicli di produzione e la gestione dei costi, ma anche migliorare l'efficacia operativa rafforzando l'interoperabilità, in particolare in un contesto multinazionale.

Un migliore collegamento tra le norme e i programmi di appalti pubblici in materia di sicurezza può aiutare l'industria dell'UE a mantenere il suo ruolo guida nelle tecnologie critiche importanti per la sovranità tecnologica dell'UE. Nel complesso, norme comuni possono contribuire all'innovazione e alla creazione di sinergie.

In stretta collaborazione con i principali portatori di interessi, la Commissione individuerà le norme e le migliori pratiche esistenti, commissionerà l'elaborazione di nuove norme che possano essere utilizzate nelle industrie civile, della difesa e dello spazio e ne promuoverà l'uso nei programmi e negli strumenti pertinenti dell'UE in settori in cui la normazione è ancora carente. Alcuni esempi comprendono:

- il lavoro pianificato nell'ambito di rescEU, che potrebbe rivelarsi un catalizzatore per migliorare la collaborazione transfrontaliera ai fini dello sviluppo di norme CBRN unificate a livello di utenti (agenzie di protezione civile) e a livello industriale, oppure
- l'iniziativa prevista nell'ambito del programma Europa digitale su uno spazio europeo dei dati in materia di sicurezza, che contribuirà alla definizione di norme di qualità a livello dell'UE.

Può essere necessaria un'azione volta a elaborare norme[41] tecnologiche ibride e migliori pratiche applicabili in tutti i settori civili (ad esempio le attività di contrasto) e della difesa. Ciò può includere la definizione e l'armonizzazione di norme, protocolli di sperimentazione concordati, migliori pratiche e codici di condotta dell'UE per ridurre i costi, aumentare

[41] L'intenzione di emanare norme ibride (ad esempio per i sistemi radio definiti da software) è stata annunciata per la prima volta nei documenti COM(2012) 417 e SWD(2012) 233 del 26.7.2012, "Piano d'azione per un'industria della sicurezza innovativa e competitiva".

l'interoperabilità, accrescere il potenziale di sinergie e migliorare la comprensibilità. L'UE può servire al meglio i suoi interessi assumendo un ruolo guida nello sviluppo di norme a livello internazionale (ad esempio in materia di cibersicurezza), tenendo conto dei valori e delle priorità dell'UE (ad esempio la legislazione dell'UE in materia di protezione dei dati).

Azione 5: entro la fine del 2022 la Commissione, in stretta collaborazione con altri portatori di interessi principali, presenterà un piano per promuovere l'uso delle **norme** ibride esistenti in materia civile/di difesa e lo sviluppo di nuove norme.

7. Innovazione e reciproco arricchimento tra le industrie civile, della difesa e dello spazio

L'innovazione[42] è al centro degli sforzi dell'Europa volti a guidare la transizione digitale e rafforzare la competitività. Idee e tecnologie possono emergere da grandi imprese, start-up, ORT e PMI in qualsiasi ecosistema e avere ripercussioni di carattere generale sulle capacità. Favorendo il reciproco arricchimento (spin-in e spin-off) tra le industrie civile, dello spazio e della difesa sarà possibile far fronte all'attuale frammentazione del panorama innovativo civile e della difesa. Ciò può rafforzare ulteriormente l'innovazione e favorire la crescita economica europea, sviluppare maggiormente il mercato unico e migliorare la sicurezza dei cittadini europei.

Un **incubatore di innovazione** in grado di sviluppare e accelerare le tecnologie nel campo dell'**innovazione a duplice uso** potrebbe diventare una risorsa fondamentale per stimolare l'innovazione e creare tecnologie innovative per i tre settori industriali, nonché per migliorare il reciproco arricchimento con altri ecosistemi. Tale incubatore di innovazione può assumere la forma di una rete virtuale, basata sulla stretta collaborazione della Commissione con il CEI e l'AED. Può, ad esempio: i) esaminare i risultati positivi della ricerca pertinente finanziata dall'UE e proporli per erogare finanziamenti supplementari o favorire l'accettazione da parte degli utenti; ii) sostenere le nuove tecnologie, con particolare attenzione all'innovazione a duplice uso proveniente da start-up, PMI e ORT; e iii) collegare e integrare le iniziative settoriali come il polo europeo per la sicurezza ospitato da Europol.

La Commissione istituirà inoltre **reti di innovazione nel settore della difesa**, con l'obiettivo di fornire servizi di dimostrazione tecnologica (ospitati da ORT, università o altre infrastrutture di ricerca) per testare la pertinenza delle tecnologie derivanti dal settore civile nelle potenziali applicazioni nel settore della difesa. Fungendo da intermediarie dell'innovazione tra attori di diverse dimensioni e provenienti da settori diversi, tali reti tematiche sosterranno l'innovazione in specifiche catene del valore della difesa promuovendo l'adozione di tecnologie civili da parte degli operatori della difesa, consentendo nel contempo alle imprese civili di valorizzare le loro tecnologie nei confronti di nuovi partner nel settore della difesa.

Inoltre i seguenti due settori tecnologici critici offrono opportunità promettenti di arricchimento reciproco.

Cibersicurezza e ciberdifesa. Nel 2021 la Commissione istituirà il centro di competenza sulla cibersicurezza[43] (CCC) e la rete di centri nazionali di coordinamento. Il CCC contribuirà

[42] Anche il polo dell'innovazione dell'UE nei settori della sicurezza interna e della giustizia, annunciato di recente dal Consiglio (6158/20 del 19.2.2020) mira a individuare opportunità di sinergie.

[43] https://ec.europa.eu/commission/presscorner/detail/it/ip_20_2384.

a proteggere l'economia e la società europee dagli attacchi informatici, promuovere e mantenere alta l'eccellenza nel settore della ricerca e rafforzare la competitività dell'industria dell'UE in materia di cibersicurezza. Il centro si avvarrà delle risorse provenienti da Europa digitale e da Orizzonte Europa, nonché dagli Stati membri. Parallelamente il Fondo europeo per la difesa (FED) sosterrà la ricerca e lo sviluppo europei di soluzioni di ciberdifesa, ad esempio nei settori della conoscenza situazionale informatica e delle capacità operative, della formazione e delle esercitazioni in ambito informatico. Il programma spaziale dell'UE continuerà a sviluppare soluzioni volte ad affrontare le sfide in materia di cibersicurezza (ad esempio Galileo).

La Commissione cercherà di migliorare il reciproco arricchimento e le sinergie tra le attività informatiche nelle sfere civili, della difesa e dello spazio al fine di ridurre le vulnerabilità e creare efficienze[44].

Tecnologie di rottura, compresa l'intelligenza artificiale[45]. Con il termine "tecnologia di rottura" si intende una tecnologia che provoca una perturbazione o un cambiamento di paradigma, ossia un cambiamento radicale anziché incrementale. Lo sviluppo di tale tecnologia è "ad alto rischio e ad alto impatto potenziale" e il concetto si applica anche ai settori civile, della difesa e dello spazio. Le tecnologie di rottura[46] per la difesa possono basarsi su concetti o idee provenienti da attori non tradizionali della difesa e nascere da spin-in del settore civile.

Il regolamento del FED prevede di impiegare fino all'8 % del suo bilancio per sostenere le tecnologie di rottura, promuovere la partecipazione di attori non tradizionali nel settore della difesa e attrarre start-up in progetti di difesa mediante inviti aperti o premi per applicazioni innovative in tale ambito. Questi meccanismi di finanziamento innovativi costituiranno una misura concreta per mettere in luce idee innovative e facilitare il reciproco arricchimento in materia di innovazione tra il settore civile e quello della difesa. Una parte molto significativa del programma Europa digitale sosterrà le tecnologie di rottura per applicazioni civili. Altri strumenti di finanziamento dell'UE, compresi quelli del programma spaziale e del CEI, prevedono investimenti analoghi.

Per promuovere l'innovazione e garantire la competitività dell'industria dell'UE sarà inoltre necessaria una politica ambiziosa in materia di **competenze**. La Commissione adotterà misure mirate per individuare eventuali carenze, competenze più pertinenti e potenziali sinergie nell'interazione tra i settori civile, della difesa e dello spazio.

La partecipazione delle donne e di altri gruppi sottorappresentati nei settori della difesa e della sicurezza resta bassa. Poiché la diversità è un fattore importante per stimolare l'innovazione, sarà promosso un maggiore coinvolgimento di tali profili. La Commissione

[44] Cfr. COM(2020) 18 del 16.12.2020 "La strategia dell'UE in materia di cibersicurezza per il decennio digitale", pagg. 14-21: Sviluppare capacità operative di prevenzione, dissuasione e risposta.

[45] Gli sviluppi in materia di IA devono essere realizzati apertamente in tutta l'UE, garantire la sicurezza e il rispetto della società e dell'ambiente delle applicazioni basate sull'IA, prendere in considerazione gli aspetti etici fin dall'inizio, valutare i rischi e mitigarne il potenziale di utilizzo dannoso e discriminazione involontaria, ad esempio i pregiudizi basati sul genere, sulla razza o sulla disabilità. L'IA sarà sviluppata in un quadro ben coordinato che rispetti i valori e i principi etici dell'UE e la Carta dei diritti fondamentali dell'Unione europea. Il contributo finanziario dell'Unione garantirà un approccio antropocentrico e inclusivo che rispetti i valori dell'Unione e sia in linea con il "Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia", COM(2020) 65 del 19.2. 2020, per il quale la Commissione presenterà una proposta supplementare nel 2021.

[46] In linea con il regolamento del FED, la Commissione può fornire sostegno finanziario alle azioni che favoriscano lo sviluppo di tecnologie di rottura per la difesa. Tuttavia, per garantire il rispetto degli obblighi internazionali dell'Unione e dei suoi Stati membri, le azioni relative a prodotti o tecnologie il cui utilizzo, il cui sviluppo e la cui fabbricazione sono vietati dal diritto internazionale non devono ricevere alcun sostegno finanziario. Pertanto, nel proporre nuovi prodotti o tecnologie per la difesa o l'aggiornamento di quelli esistenti, i richiedenti dovrebbero impegnarsi a rispettare i principi etici, come quelli relativi al benessere degli esseri umani e alla protezione del genoma umano, rispecchiati anche nel pertinente diritto nazionale, dell'Unione e internazionale, comprese la Carta dei diritti fondamentali dell'Unione europea e la Convenzione europea dei diritti dell'uomo e, ove pertinente, i relativi protocolli.

perseguirà inoltre una maggiore partecipazione delle donne innovatrici e si impegnerà per raggiungere obiettivi in materia di uguaglianza e inclusione (ad esempio l'accessibilità digitale)[47].

Azione 6: nel primo semestre del 2022 la Commissione avvierà, in collaborazione con il Consiglio europeo per l'innovazione e altri portatori di interessi, un **"incubatore di innovazione"** per sostenere le nuove tecnologie e plasmare l'**innovazione a duplice uso**. La Commissione sosterrà inoltre le **reti transfrontaliere di innovazione nel settore della difesa** che sperimenteranno la pertinenza delle tecnologie del settore civile e fungeranno da supporto all'innovazione responsabile nelle catene del valore della difesa. Tali azioni faranno anche fronte all'attuale frammentazione del panorama innovativo in ambito civile e di difesa, alla carenza di competenze nonché agli obiettivi in materia di uguaglianza e inclusione.

Azione 7: a partire dal giugno 2021 la Commissione istituirà insieme agli Stati membri il centro di competenza sulla cibersicurezza, assegnando le necessarie risorse dei programmi e degli strumenti pertinenti dell'UE. La Commissione cercherà di rafforzare le sinergie, gli spin-in e gli spin-off tra le attività del centro, del FED e del programma spaziale dell'UE in materia di **cibersicurezza e ciberdifesa**, al fine di ridurre le vulnerabilità e creare efficienze.

Azione 8: a partire dal primo semestre del 2022, per sostenere le **tecnologie di rottura** la Commissione presenterà forme innovative di finanziamento per promuovere la partecipazione di attori non tradizionali, attrarre start-up e favorire lo scambio reciproco di soluzioni, sulla base delle opportunità offerte dai programmi e dagli strumenti dell'UE, compresi il programma Europa digitale e il FED.

8. Promuovere le sinergie e il reciproco arricchimento attraverso progetti faro

Un modo per dare impulso alle sinergie tra l'industria civile, della difesa e dello spazio consiste nell'avvio di progetti faro che sosterranno le tecnologie critiche e forniranno soluzioni a importanti problematiche sociali o strategiche. I progetti faro offrono un notevole potenziale di sinergie e arricchimento reciproco tra settori: a livello di programma (ad esempio inviti complementari rivolti a settori simili, collegamento delle esigenze in materia di appalti con la ricerca, sinergie nei finanziamenti); mediante la tecnologia (ad esempio tecnologie a duplice uso, soprattutto a basso livello di maturità tecnologica); e tramite l'innovazione e le PMI (ad esempio agevolando nuove interazioni con l'industria della difesa e della sicurezza).

Varie iniziative finanziate dall'UE gettano le basi per la creazione di sinergie intersettoriali, tra cui:

- il meccanismo per collegare l'Europa, che cofinanzierà progetti per infrastrutture di trasporto a duplice uso allo scopo di migliorare la mobilità sia civile che militare;
- Galileo, che offre un servizio pubblico regolamentato che potrebbe essere utilizzato per scopi di difesa;
- Copernicus, che offre servizi ambientali e di sicurezza regolarmente utilizzati da varie comunità di utenti per scopi civili e di difesa, soprattutto in applicazioni quali la verifica della conformità e l'applicazione delle norme ai sensi del diritto dell'UE (ad esempio in materia di garanzia della conformità ambientale e criminalità);

[47] Comunicazione "Un'Unione dell'uguaglianza: la strategia per la parità di genere 2020-2025", COM(2020) 152 final.

- SESAR (ricerca sulla gestione del traffico aereo nel cielo unico europeo), che esamina soluzioni tecniche per una cooperazione civile-militare flessibile al fine di massimizzare l'uso dello spazio aereo;
- i servizi di sorveglianza dello spazio e tracciamento (SST) dell'UE per gli operatori satellitari nazionali e commerciali che utilizzano risorse nazionali;
- ricerca orientata alla difesa per modelli energetici sicuri e sostenibili (a livello di generazione, stoccaggio, efficienza e gestione dell'energia), che favorisca una maggiore resilienza ed efficienza operativa nel contesto dei cambiamenti climatici;
- il forum consultivo per l'energia sostenibile nel settore della difesa e della sicurezza[48] e l'azione comune prevista con l'AED per individuare gli ostacoli allo sviluppo delle energie rinnovabili offshore nei settori riservati alla difesa e per migliorarne la coesistenza[49];
- risposta medica e attività CBRN che sono i) supportate da rescEU (ad esempio il trasporto di pazienti contaminati e infettivi), ii) pianificate dal FED o iii) sostenute dal programma dell'UE per la salute (ad esempio l'azione comune per rafforzare la preparazione sanitaria e la risposta agli attacchi terroristici biologici e chimici).

Per garantire che queste iniziative realizzino appieno il loro potenziale, la Commissione ne monitorerà l'attuazione e individuerà le possibilità di migliorare il rendimento degli investimenti. Ad esempio:

- la Commissione garantirà sinergie con gli organismi, i programmi e gli strumenti esistenti dell'UE nell'ambito delle azioni preparatorie, che saranno avviate nel 2021 per l'istituzione dell'autorità dell'UE per la preparazione e la risposta alle emergenze sanitarie (HERA)[50], incentrate fra l'altro sulle minacce biologiche emergenti per la salute umana e sulle attività relative a una risposta europea in materia di biosicurezza;
- la Commissione garantirà sinergie tra gli investimenti in ambito di difesa e civile nelle tecnologie informatiche, del cloud, dei processori e quantistiche;
- per rispondere meglio alle sfide odierne in materia di sicurezza[51], la Commissione cercherà di promuovere la diffusione degli ingenti investimenti nell'infrastruttura transeuropea di comunicazione sicura (TESTA). TESTA consente una connettività sicura a livello dell'UE (anche per la videoconferenza) tra le istituzioni dell'UE, gli organi e le agenzie dell'UE e le autorità nazionali nel settore della difesa e della sicurezza;
- nel contesto della strategia per la sicurezza marittima dell'UE (EUMSS)[52], la Commissione promuoverà ulteriormente la cooperazione tra le agenzie che si occupano di attività civili e di difesa (ad esempio FRONTEX, EMSA - Agenzia europea per la sicurezza marittima, EFCA - Agenzia europea di controllo della pesca) e sosterrà l'attuazione dell'agenda di ricerca sulla **sicurezza marittima** civile e militare coordinata. La cooperazione in materia civile e di difesa fa parte dei principi fondamentali del piano d'azione dell'EUMSS[53], che comprende: azioni volte a migliorare l'interconnessione e

[48] https://cordis.europa.eu/project/id/882171/it.

[49] COM(2020) 741 final, Strategia dell'UE per sfruttare il potenziale delle energie rinnovabili offshore per un futuro climaticamente neutro.

[50] Cfr. anche COM(2020) 724 dell'11.11.2020 "Costruire un'Unione europea della salute: rafforzare la resilienza dell'UE alle minacce per la salute a carattere transfrontaliero".

[51] In linea con l'obiettivo espresso nella "Prima relazione sui progressi compiuti nella strategia dell'UE per l'Unione della sicurezza" (COM(2020) 797) di promuovere la resilienza delle infrastrutture digitali e accrescere la preparazione a livello nazionale e dell'UE, sviluppando solide capacità per prevenire, individuare, affrontare e attenuare le minacce.

[52] https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52014JC0009&from=EN.

[53] https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/2018-06-26-eumss-revised-action-plan_en.pdf.

lo scambio di informazioni tra le autorità civili e militari tramite il sistema comune per la condivisione delle informazioni sul settore marittimo (CISE)[54]; la promozione di un quadro per il settore della cantieristica navale civile e militare; e il rafforzamento della cooperazione civile-militare in materia di ricerca e soccorso in mare (SAR).

Inoltre, sulla base di un'analisi preliminare e di iniziative da finanziare con gli strumenti dell'UE, la Commissione sta avviando tre progetti faro:

- **tecnologie UE dei droni.** Questo progetto faro mirerà a rafforzare la competitività dell'industria dell'UE in questo settore tecnologico critico. Individuerà le aree di reciproco arricchimento, in modo tale che i progetti nel settore della difesa traggano vantaggio dagli sviluppi innovativi realizzati dalle PMI attive nel campo dei droni civili e che, a sua volta, l'aeronautica civile tragga vantaggio dagli sviluppi nel settore della difesa. In particolare, si concentrerà sugli aeromobili senza equipaggio ed esaminerà lo sviluppo degli elementi tecnologici necessari per un'ulteriore automazione del traffico di droni. Il progetto faro sarà parte integrante di un'ambizione generale da definire ulteriormente nella "Strategia 2.0 dell'UE per i droni" prevista per il 2022[55], al fine di favorire e accelerare l'ulteriore sviluppo e utilizzo di questa tecnologia in Europa, rafforzando in tal modo la sovranità tecnologica;
- **sistema di comunicazione sicuro globale dell'UE basato sulla tecnologia spaziale.** Questo progetto faro mira a fornire accesso alla connettività ad alta velocità attraverso un'infrastruttura spaziale multi-orbita, compresi i satelliti in bassa orbita terrestre, e a integrare Galileo/EGNOS e Copernicus come terzo sistema satellitare dell'UE. L'integrazione delle tecnologie di crittografia quantistica garantirà una connettività e una comunicazione altamente sicure per i servizi governativi e commerciali (ad esempio collegando meglio le infrastrutture chiave, coadiuvando la gestione delle crisi, la sorveglianza e le potenziali applicazioni a banda larga di massa). Consentirà a tutti i cittadini europei di usufruire di connessioni ad alta velocità e fornirà un sistema di connettività resiliente che permetterà all'Europa di rimanere connessa in ogni circostanza, anche in caso di attacchi informatici su larga scala in Internet. Si tratterà infine di un'infrastruttura geostrategica al centro di partenariati specifici, ad esempio con l'Africa;
- **strategia dell'UE per la gestione del traffico spaziale (STM).** Questo progetto faro svilupperà norme e regole di STM al fine di evitare eventi di collisione che potrebbero derivare dalla proliferazione di satelliti e detriti spaziali e causare eventi catastrofici per le risorse dell'UE nello spazio. La strategia di STM eviterà inoltre il rischio che le regole non UE diventino la norma, in quanto tale dipendenza avrebbe un effetto negativo sugli sforzi europei volti a conseguire la sovranità tecnologica. Questa iniziativa faro dovrebbe inoltre contribuire alla definizione di un approccio internazionale in materia di STM.

Ciascuno dei progetti faro potrebbe diventare un fattore di svolta grazie alla sua portata o al suo impatto e ai benefici che apporterebbe alla sovranità tecnologica dell'Europa e alla società in generale. Per sviluppare ulteriormente ciascun progetto, la Commissione continuerà ad analizzare i casi d'uso, le caratteristiche tecniche, le tecnologie critiche da utilizzare, i costi e gli eventuali strumenti di finanziamento, le strutture di governance e le idee innovative (legate alla tecnologia o al mercato) delle PMI, delle start-up e delle ORT. Su tale base, la Commissione deciderà le possibili misure supplementari per ciascun progetto, comprese, se del caso, eventuali proposte legislative.

[54] http://emsa.europa.eu/cise.html.

[55] Cfr. pag. 18 del documento COM(2020) 789 del 9.12.2020, "Strategia per una mobilità sostenibile e intelligente: mettere i trasporti europei sulla buona strada per il futuro".

Le tabelle di marcia tecnologiche relative ad alcune delle tecnologie critiche individuate nella sezione 5 potrebbero anche portare alla nascita di futuri progetti faro.

La Commissione intende intensificare il dialogo e le attività di sviluppo su tre progetti faro potenzialmente in grado di determinare un cambiamento di rotta. Dopo un'adeguata analisi e consultazione dei portatori di interessi, la Commissione deciderà in merito alle possibili misure supplementari, comprese, se del caso, eventuali proposte legislative.

Azione 9: "Tecnologie UE dei droni".

Azione 10: "Sistema di comunicazione sicuro globale dell'UE basato sulla tecnologia spaziale".

Azione 11: "Gestione del traffico spaziale".

9. Le nostre iniziative per realizzare l'obiettivo

La Commissione vigilerà sull'attuazione del presente piano d'azione in stretta collaborazione con il Parlamento europeo e il Consiglio. Presterà particolare attenzione alla realizzazione più efficace ed efficiente delle priorità programmatiche (politiche tematiche e politiche volte a promuovere la competitività generale, la ricerca e l'innovazione), salvaguardando al contempo la massima coerenza e le migliori sinergie tra i programmi e gli strumenti dell'UE.

Per promuovere il reciproco arricchimento tra le industrie civile, della difesa e dello spazio nel lungo periodo, la Commissione monitorerà i progressi specifici di ciascuna delle 11 azioni elencate e presenterà ogni due anni una relazione sui progressi compiuti. Il calendario di attuazione di ciascuna azione sarà allineato alla pianificazione degli strumenti pertinenti dell'UE.