The European House Ambrosetti | LEONARDO

Peace through security:
the strategic role of digital technologies

Peace through security: the strategic role of digital technologies

Settembre 2024

Indice

Colophon 4
Prefazioni 8
Impostazione metodologica dello Studio strategico 18

1 Un mondo in stato di “no-peace” 20

1.1 Il mondo in uno stato di “no-peace” 23
1.1.1 I cambiamenti climatici 25
1.1.2 Le aree di instabilità 27
1.1.3 L’accesso a energia, tecnologie e materie prime 31
1.1.4 Il nuovo ordine globale 33
1.1.5 Il posizionamento dell’Unione Europea nel nuovo ordine globale 37

2 Le nuove minacce ibride e gli strumenti per contrastarle 40

2.1 Minacce Militari, Economiche, Cognitive e di Global Health 43
2.1.1 Le minacce militari 45
2.1.2 Le minacce economiche 51
2.1.3 Le minacce cognitive 55
2.1.4 Le minacce di Global Health 57
2.2 La necessità di un approccio alla difesa di Total Security 59

3 La centralità delle tecnologie digitali per la competitività internazionale e la difesa 62

3.1 L'importanza della leadership nelle tecnologie digitali 65
3.2 Il nuovo paradigma della difesa 75

4 Le criticità dell'Europa nella gestione della difesa e nello sviluppo di tecnologie digitali 82

4.1 Le 5 aree di debolezza legate alla difesa europea 85
4.2 Debolezza nel settore digitale 87
4.3.1 Frammentazione politica 93
4.3.2 Frammentazione militare 97
4.3.3 Frammentazione industriale e della ricerca 99
4.4.1 Limitati investimenti pubblici e difficoltà per gli investimenti privati 103
4.4.2 Limitati investimenti pubblici 105
4.4.3 Difficoltà degli investimenti privati nel settore della difesa 106
4.5 Dipendenza strategica 109
4.6 Social Acceptance 113

5 Proposte per rafforzare lo sviluppo delle tecnologie digitali per la difesa 116

1. Riorganizzare e ottimizzare il quadro istituzionale e finanziario della difesa europea 119
2. Dotare l'Europa di uno strumento di «total security» 120
3. Rafforzare lo strumento militare comune europeo 122
4. Promuovere l'adozione di requisiti comuni e programmi industriali cooperativi tra gli Stati membri 124
5. Favorire la creazione di sinergie tra aziende della difesa europee 126
6. Limitare l'utilizzo di misure protezionistiche nel mercato interno europeo 128
7. Reinterpretare i parametri di sostenibilità degli investimenti in difesa per incentivare la partecipazione di investitori privati e istituzionali 130
8. Dotare l'Europa di una strategia a lungo termine per garantire autonomia strategica e sovranità tecnologica digitale per la difesa 132
9. Rafforzare l'integrazione e la cooperazione in ambito spaziale 134
10. Creare dialogo tra mondo dell'innovazione e della difesa 136

Bibliografia 138

Colophon

Lo Studio Strategico ***Peace through security: the strategic role of digital technologies*** è stato realizzato da TEHA Group in collaborazione con Leonardo.

L'iniziativa ha la missione di approfondire il ruolo delle tecnologie digitali nell'assicurare la competitività internazionale e un posizionamento geopolitico di primo piano per l'Europa. Gli obiettivi di questo Studio possono essere così riassunti:

- Approfondire l'**attuale contesto geopolitico internazionale**, analizzandone i fattori di cambiamento e le forze in gioco, e leggendone le ricadute soprattutto per il contesto europeo;
- Fornire una vista d'insieme delle **minacce emergenti** sul piano internazionale, approfondendone le caratteristiche e le **implicazioni in termini di sicurezza fisica, economica e sociale per l'Europa**, mettendo in luce quali sono i punti di debolezza di quest'ultima;
- Approfondire il **ruolo delle tecnologie digitali** funzionali al mantenimento della pace, come strumento trasversale a tutti i domini militari, e come l'Europa si posiziona relativamente a queste, in un'ottica di sovranità e presidio;
- Fornire una **prospettiva indipendente e autorevole rispetto al ruolo dell'industria europea della Difesa** relativamente allo sviluppo di capacità tecnologica autonoma;
- Elaborare **indirizzi e proposte di policy per posizionare l'Europa come leader** nella creazione di innovazione in tecnologie digitali, anche per la difesa, affinché mantenga un ruolo di primo piano nella geopolitica internazionale.

Il team del progetto è composto da un Comitato Scientifico, responsabile della guida strategica della ricerca, i cui membri hanno indirizzato le analisi e fornito consulenza scientifica, garantendo la terzietà, l'indipendenza e l'autorevolezza dello studio, e da un Gruppo di Lavoro, incaricato dello sviluppo dello Studio Strategico.

Il Comitato Scientifico è composto da:

- **Roberto Cingolani**, CEO, Leonardo
- **Lorenzo Mariani**, Condirettore generale, Leonardo
- **Valerio De Molli**, Managing Partner and Chief Executive Officer, The European House Ambrosetti & TEHA Group
- **Vincenzo Camporini**, già Capo di Stato Maggiore, Aeronautica Militare e Difesa
- **Barbara Mazzolai**, Direttore, Laboratorio di Robotica Morbida Bioispirata, Istituto Italiano di Tecnologia
- **Federico Rampini**, Giornalista, editorialista da New York, Corriere della Sera

Il Gruppo di Lavoro di **Leonardo** è composto da:

- **Simone Ungaro**, Chief Strategy & Innovation Officer
- **Angelo Pansini**, Chief of Staff - General Management Business Operations
- **Fabio Gastaldi**, Senior Vice President Strategy & Technology
- **Salvatore Scervo**, Senior Vice President Innovation Labs & IP

Il Gruppo di Lavoro di **TEHA Group** è composto da:

- **Corrado Panzeri**, Partner & Head of Innovation and Technology Hub
- **Alessandro Viviani**, Associate Partner, Project Leader
- **Andrea Alejandro Merli**, Consultant, Project Coordinator
- **Carlotta Molteni**, Consultant
- **Sofia Odolini**, Analyst
- **Fabiola Gnocchi**, Communication Manager
- **Roberta Braccio**, Project Assistant

Un ringraziamento particolare al management di Leonardo, che ha contribuito allo sviluppo dello Studio Strategico attraverso interviste riservate:

- **Barbara Borasca**, Strategy & Technology
- **Andrea Campora**, Managing Director Divisione Cyber & Security Solution
- **Carlo Cavazzoni**, Head of Computational R&D
- **Massimo Claudio Comparini**, CEO, Thales Alenia Space Italia
- **Manlio Cuccaro**, Chief Procurement, Services & Operations
- **Gian Piero Cutillo**, Managing Director Divisione Elicotteri
- **Marco De Fazio**, Managing Director Divisione Elettronica
- **Carlo Gualdaroni**, Chief Commercial & Business Development
- **Simon Harwood**, Managing Director UK Capability & Innovation
- **Deborah Iglesias**, Strategy & Technology
- **Raffaella Luglini**, Chief Sustainability Officer
- **Guglielmo Maviglia**, Director GCAP
- **Carlo Musso**, Strategy & Technology
- **Franco Ongaro**, Managing Director Space Business
- **Stefano Pontecorvo**, Chairman
- **Francesco Sabatini**, Strategy & Technology
- **Giovanni Soccodato**, Managing Director Italia, MBDA
- **Marco Zoff**, Managing Director Aircraft division

Al fine di potenziare la profondità delle analisi e individuare rapidamente i principali temi da affrontare all'interno dello Studio Strategico, sono stati realizzati diversi colloqui riservati. Nello specifico, questi incontri avevano l'obiettivo di:

- rilevare direttamente la **percezione delle sfide e opportunità** derivanti dalla ricerca e sviluppo di tecnologie digitali nell'attuale scenario economico-industriale italiano, in relazione alla competitività internazionale;
- **coinvolgere attivamente i diversi importanti stakeholder**, anche a livello istituzionale, nel processo di progettazione e condivisione dei contenuti;
- **stimolare il dibattito sulle proposte emerse**, soprattutto sul tema di una maggior integrazione della difesa europea e dello sviluppo di capacità di innovazione nelle tecnologie digitali di matrice europea, coinvolgendo alcuni attori significativi nel processo;
- **mantenere alta l'attenzione sull'iniziativa**, anche attraverso alcune azioni di comunicazione mirate;
- **sviluppare un'intelligence qualificata** utile a supportare le riflessioni/scelte strategiche di Leonardo.

A questo proposito, vogliamo ringraziare tutti gli esperti che hanno contribuito attraverso i propri preziosi spunti e punti di vista:

- **Giuseppe Caire**, Full Professor for Electrical Engineering | School IV EECS, Technische Universität Berlin
- **Alessandro Ercolani**, Amministratore Delegato, Rheinmetall Italy
- **Bruno Frattasi**, Direttore Generale, Agenzia per la Cybersicurezza Nazionale
- **Nicolas Kerleroux**, Responsible for Security e Crisis Management, RELEX.5 Directorate, Council of the European Union
- **Soenke Marahrens**, Colonel and Director of COI Strategy and Defense, Hybrid Center for Excellence
- **Carmine Masiello**, Capo di Stato Maggiore, Esercito Italiano
- **Matteo Perego di Cremnago**, Sottosegretario, Ministero della Difesa
- **Luisa Riccardi**, Vicesegretario Generale, Ministero della Difesa
- **Alec Ross**, Board Partner, Amplo, USA
- **Simone Severini**, General Manager, Quantum Technologies, AWS
- **Carlo Vaiti**, Distinguished Chief Technologist, HPE

I contenuti di questo Studio Strategico si riferiscono esclusivamente all'analisi e alla ricerca effettuata da TEHA Group e rappresentano la sua opinione che può non coincidere con le opinioni e il punto di vista dei soggetti intervistati e coinvolti nell'iniziativa.

Prefazioni

Roberto Cingolani
CEO, Leonardo

Viviamo in un contesto sempre meno sicuro e sempre più imprevedibile.

I conflitti che si stanno accendendo in diverse parti del mondo e la debolezza mostrata dai sistemi democratici occidentali delineano degli scenari complessi da interpretare e difficili da prevedere nella loro evoluzione.

Tuttavia, queste difficoltà e queste incertezze paradossalmente ci danno un'indicazione semplice e univoca: l'Europa deve fare OGGI delle scelte chiare e coraggiose per poter affrontare in modo consapevole ed efficace, e con le proprie forze se necessario, situazioni future difficili e imprevedibili, che richiederanno capacità di difesa e di sicurezza migliori di quelle attualmente disponibili.

Per fare queste scelte, occorre però tenere presente che il settore della difesa e della sicurezza negli ultimi anni è cambiato, e continuerà a farlo.

Da un punto di vista industriale, le aziende del settore si trovano ad operare in un contesto di competizione sempre più acceso, complicato anche dalle contrapposizioni politiche che hanno impatti non trascurabili sulle catene di approvvigionamento, obbligando i Paesi Occidentali a riorganizzare le proprie reti di fornitura. A questo bisogna aggiungere l'evoluzione sempre più rapida e diffusa della tecnologia, che oggi è disponibile per un sempre maggior numero di attori statali e non statali.

Il conflitto in Ucraina sta dimostrando che occorre essere pronti a combattere con mezzi tradizionali, ma che, al tempo stesso, la superiorità tecnologica dà vantaggi determinanti sul campo di battaglia. Più in generale, bisogna riconoscere che la difesa sarà sempre più basata sui *byte* rispetto ai *bullets*: gli scenari dei conflitti stanno cambiando, e vanno verso un mix di sistemi tradizionali e sistemi avanzati, tecnologie digitali e applicazioni satellitari che devono poter operare all'unisono secondo una logica multi-dominio che sia le forze armate, sia l'industria devono fare propria e saper porre in atto.

Data la complessità dello scenario internazionale, occorre un vero e proprio cambio di paradigma, passando dall'idea di difesa convenzionale a quella di più ampio respiro di 'sicurezza globale', ove 'globale' non ha un'accezione unicamente geografica, ma anche, e soprattutto, concettuale. La sicurezza non è infatti solo sicurezza fisica o dei confini, ma è anche sicurezza energetica, alimentare, informatica e delle infrastrutture. Per difendere tutte queste dimensioni contemporaneamente è necessaria una consapevolezza globale che si deve basare sulla disponibilità in tempo reale e sulla fruibilità di dati sempre più numerosi, che devono anche essere sicuri, attendibili e facilmente condivisibili.

Per poter realizzare efficacemente e in tempi rapidi tutti i cambiamenti richiesti da un sistema di sicurezza che non può più essere la semplice somma di sistemi di sicurezza nazionali – ancorché coordinati fra loro – ma deve diventare un vero sistema di sicurezza europeo, in grado di stare al passo con l'accelerazione del progresso tecnologico e con il rapido susseguirsi degli eventi nel contesto geopolitico internazionale, è necessario un incremento e un migliore utilizzo degli investimenti. Il problema più grande della difesa europea, infatti, sta proprio nella frammentazione: occorrono processi decisionali più semplici e lineari, una reale sinergia a livello tecnologico e industriale e una maggiore standardizzazione dei requisiti, che consenta la riduzione del numero di piattaforme e sistemi, con benefici sia operativi, sia produttivi.

Il sostegno di Leonardo al presente studio vuole essere un contributo concreto e propositivo, per favorire l'evoluzione della visione strategica europea di fronte ai cambiamenti globali in atto, con l'obiettivo di poter contribuire a un futuro più sicuro per tutti cittadini italiani, europei e di tutto il mondo.

Valerio De Molli
Managing Partner & CEO, The European House - Ambrosetti & TEHA Group

"La più grande minaccia al nostro pianeta è la convinzione che lo salverà qualcun altro" Robert Swan

In un mondo in stato di "no-peace" in cui gli assetti geopolitici si evolvono con una rapidità senza precedenti, l'Europa si trova in una posizione di minore influenza e di fronte alla necessità di rafforzare le proprie capacità difensive per navigare il delicato equilibrio tra pace e sicurezza.

La crescente sfida posta da minacce ibride di natura imprevedibile e non convenzionale richiede un approccio alla difesa in chiave di **total security**, ovvero che sia in grado di coordinare gli strumenti di potere sia militare che politico-economico. In tal senso, le tecnologie digitali rappresentano una svolta fondamentale, offrendo soluzioni innovative per rispondere a minacce sempre più sofisticate e imprevedibili. Il loro impiego permette di migliorare l'efficacia delle operazioni, garantendo una maggiore precisione e rapidità di intervento, oltre a favorire una migliore condivisione delle informazioni e una più stretta collaborazione tra le forze di sicurezza a livello internazionale.

A fronte della centralità delle tecnologie digitali, TEHA Group ha elaborato il **TEHA - Digital Technologies Security Index** (TEHA-DTSI), uno strumento informativo e di orientamento decisionale per valutare il posizionamento dell'Europa rispetto ad altre geografie mondiali in cinque tecnologie digitali: Artificial Intelligence, Big Data e Digital Twin, Cloud Computing e High Performance Computing, Connectivity, Cybersecurity, Quantum Technologies. Il TEHA-DTSI è composto da 38 Key Performance Indicator monitorati in 13 Paesi e regioni per gli anni 2019 e 2024. Ne emerge una chiara leadership degli Stati Uniti in tutte le dimensioni e tecnologie analizzate, mentre l'Unione Europea, sebbene competitiva in alcune aree (per esempio nella capacità di diffusione di AI, Big Data e Digital Twin, Connectivity e Cybersecurity), presenta una performance complessiva significativamente inferiore, suggerendo la necessità di maggiori investimenti in Ricerca e Sviluppo e strategie di implementazione più efficaci.

A questa debolezza tecnologica si somma la frammentazione politica e della capacità industriale in ambito difesa, gli esigui investimenti pubblici e privati, l'eccessiva dipendenza strategica dell'Europa dalle forniture militari extra-UE (in particolare statunitensi) e le difficoltà in termini di accettazione sociale.

L'Europa, se intende puntare ad avere una strategicità geopolitica a livello internazionale, deve risolvere queste criticità attraverso una visione unica di interesse europeo e non di singoli Paesi membri, implementando un paradigma di nuovo modello di collaborazione con il settore privato nel settore della difesa.

A tal fine, lo Studio Strategico di TEHA delinea **10 proposte** per potenziare il posizionamento dell'Europa nella leadership internazionale relativamente allo sviluppo di innovazione di frontiera e di tecnologie digitali per la difesa e, più in generale, per dotarla di autonomia strategica nella difesa attraverso tre linee di indirizzo strategiche fondamentali: I) **definire una chiara governance europea** che uniformi gli interessi dell'Europa come voce unica sul piano internazionale; II) **evitare di cedere sovranità industriale**, dove un forte sviluppo digitale è cruciale; III) **fare leva sugli investimenti** per costruire filiere europee delle tecnologie digitali, promuovendo la crescita economica e il perseguimento di un'autonomia strategica.

Prima di invitarvi alla lettura, ringrazio sentitamente il Comitato Scientifico alla guida dell'iniziativa per i preziosi contributi: Vincenzo Camporini (già Capo di Stato Maggiore dell'Aeronautica e della Difesa), Barbara Mazzolai (Direttore, Laboratorio di Robotica Morbida Bioispirata, Istituto Italiano di Tecnologia) e Federico Rampini (Giornalista, editorialista da New York, Corriere della Sera).

Desidero inoltre esprimere la mia più sentita gratitudine a tutti i vertici di Leonardo, a partire da Stefano Pontecorvo (Chairman), Roberto Cingolani (CEO) e Lorenzo Mariani (Condirettore generale) e dal suo leadership team composto da Simone Ungaro (Chief Strategy & Innovation Officer), Angelo Pansini (Chief of Staff - General Management Business Operations), Fabio Gastaldi (Senior Vice President Strategy & Technology) e Salvatore Scervo (Senior Vice President Innovation Labs & IP), per aver approfondito un tema di tale importanza strategica per il nostro Paese e per l'Europa.

Infine, un ringraziamento va al gruppo di lavoro di TEHA Group formato, oltre che dal sottoscritto, da Corrado Panzeri, Alessandro Viviani, Andrea Alejandro Merli, Carlotta Molteni, Sofia Odolini, Fabiola Gnocchi e Roberta Braccio.

Vincenzo Camporini
già Capo di Stato Maggiore, Aeronautica Militare e Difesa

In una prospettiva storica, le illusioni di una pace perpetua, con la fine della guerra fredda, sono durate pochi istanti. Il mondo è ripiombato presto in un clima di incertezze e di conflittualità latenti, via via accentuate e alimentate da crisi di varia natura, economiche, sanitarie, politiche in senso lato. Il tutto in un quadro di complessità crescente e di crescenti vulnerabilità delle nostre società che si affidano, spesso ciecamente, al tumultuoso sviluppo di tecnologie, la cui straordinaria utilità e le cui ancora inesplorate potenzialità si accompagnano ad una progressiva deresponsabilizzazione del fattore umano.

In questo quadro chi ha responsabilità politiche e manageriali in senso lato ha il preciso e irrinunciabile dovere di predisporre tutti gli strumenti cognitivi e operativi per affrontare le sfide di varia natura, in qualche caso anche imprevedibili, che rischiano di investire le nostre società.

È per questi motivi che questo studio approfondito, condotto da TEHA in collaborazione con Leonardo, sul rivoluzionario impatto delle tecnologie digitali sulla sicurezza in senso lato va bene al di là di un ambito accademico: il lavoro, infatti, costituisce uno strumento concettuale e pragmatico di straordinaria importanza per coloro che saranno chiamati a prendere decisioni cruciali per gli indirizzi futuri e merita una diffusione che vada bene al di là degli 'addetti ai lavori', per diffondere una consapevolezza più ampia, idonea a garantire il necessario consenso ai provvedimenti, anche a quelli impopolari, che sarà necessario assumere.

Barbara Mazzolai
Direttore del Laboratorio di Robotica Soffice Bioispirata, Istituto Italiano di Tecnologia

Il contesto geopolitico odierno, segnato da rapide trasformazioni e crescenti tensioni internazionali, richiede una riflessione profonda sulle dinamiche che guidano questi cambiamenti e sulle conseguenze che tali forze possono esercitare sulla sicurezza e la stabilità dell'Europa. Lo Studio Strategico "Peace through Security: the Strategic Role of Digital Technologies," elaborato da TEHA Group in collaborazione con Leonardo, offre una visione critica e approfondita su queste tematiche fondamentali, delineando le sfide e le opportunità che l'Europa dovrà affrontare nel prossimo futuro.

In un mondo sempre più instabile, le minacce ibride—che combinano attacchi fisici, cibernetici, economici e psicologici—pongono un rischio crescente per la sicurezza europea. Questi pericoli non minacciano solo la difesa militare, ma hanno anche implicazioni profonde per la stabilità economica e sociale del continente. Lo studio mette in luce vulnerabilità strategiche per l'Europa, quali la frammentazione delle politiche di difesa, la fragilità delle infrastrutture digitali e la dipendenza da tecnologie esogene. Superare queste criticità richiede una comprensione chiara del contesto, dei rischi e l'adozione di strategie moderne, integrate ed efficaci per la loro risoluzione.

In questo quadro, le tecnologie digitali assumono un ruolo di primaria importanza. Queste tecnologie, ormai fondamentali in ogni ambito della nostra società, possono diventare strumenti potenti per garantire la pace e la sicurezza a livello internazionale. L'Europa, però, deve affrontare l'urgenza di affermarsi come leader in questo settore, assicurando la propria sovranità tecnologica e riducendo la dipendenza da attori esterni. Investire nello sviluppo di soluzioni innovative è essenziale per rafforzare la struttura economica e industriale dell'intero continente.

L'Italia, in questo scenario, si distingue come un leader mondiale nella robotica, sia nel campo della ricerca sia in quello industriale. **L'integrazione di soluzioni digitali con hardware avanzato rappresenta un asset strategico per il Paese**, offrendo nuove prospettive di crescita e consolidando la competitività sia a livello nazionale che europeo. Tuttavia, permane un divario significativo tra il settore industriale della difesa e il mondo della ricerca, che limita lo sfruttamento pieno del potenziale innovativo a disposizione. È necessario attrezzarsi con una buona dose di coraggio. Impegno. Creatività. Finanza. L'innovazione dirompente non nasce dall'ovvio, non è figlia della consuetudine, ma si origina dalla sfida, dalla capacità di ideare e affrontare progetti pionieristici e visionari, capaci di attrarre e affascinare giovani menti, avvicinandole a un contesto applicativo così cruciale per la nostra società.

L’Europa, per mantenere il proprio ruolo sulla scena geopolitica globale, dovrebbe promuovere una maggiore sinergia tra ricerca, salute, difesa e sicurezza, esplorando nuovi territori. Con coraggio. Attraverso lo sviluppo di piattaforme innovative che intreccino soluzioni fisiche, digitali ed economiche, in grado di rispondere a un contesto globale sempre più complesso, anticipando le risposte a minacce multidimensionali. Questo non solo colmerebbe le lacune esistenti, ma aprirebbe anche nuove opportunità per l’industria europea, favorendo lo sviluppo di capacità tecnologiche autonome. Solo così l’Europa potrà affermarsi non solo come consumatore di tecnologia, ma come creatore e innovatore di soluzioni avanzate, cruciali per la sicurezza, la competitività e la sostenibilità del futuro.

Una pace e prosperità durature nascono dall’equilibrio tra sicurezza, benessere condiviso e crescita sostenibile. L’innovazione e la cooperazione globale, arricchite dalle diverse prospettive culturali, rappresentano la ‘nuova via’ per costruire una stabilità futura.

Federico Rampini
Writer and Columnist, Corriere della Sera

La difesa comune europea è una delle sfide più complesse che l'Unione Europea deve affrontare oggi. È una priorità vitale per garantire sicurezza e benessere dei propri cittadini, e rafforzare il proprio posizionamento internazionale nel confronto con le altre grandi potenze.

La democrazia e la prosperità dell'Europa sono esposte a minacce ibride, sempre più imprevedibili e non convenzionali, di diversa natura: militare, economica, cognitiva e sanitaria. Ciò rende vulnerabili tutti gli ambiti della nostra società, dalle infrastrutture critiche alla pubblica amministrazione, dai servizi finanziari al sistema sanitario. Anche il sistema delle imprese è il target di guerre asimmetriche, che già oggi non fanno distinzione tra ambito civile e militare, tra forze armate e industria. Tuttavia finora il sistema produttivo pare non avere ancora consapevolezza di questi rischi e non ha ancora messo in campo strumenti per difendersi adeguatamente.

Occorre un cambio di paradigma. Dobbiamo adottare un approccio di "total security", inteso non solo come sicurezza fisica o dei confini, ma anche energetica, alimentare, informatica e delle infrastrutture. Per difendere tutte queste dimensioni è necessaria una nuova consapevolezza globale in cui la sicurezza deve essere integrata in una strategia di difesa più ampia e coordinata.

Per raggiungere questo obiettivo, l'Europa deve ripensare l'attuale sistema della difesa e il processo industriale, rendendoli in grado di stare al passo con l'accelerazione del progresso tecnologico e con il contesto geopolitico internazionale.

Il presente Studio strategico approfondisce ciascuno di questi aspetti e suggerisce alcune proposte affinché l'Europa agisca in modo coordinato per potenziare il proprio posizionamento geopolitico con un orizzonte di lungo termine.

Così come nel dopoguerra si era creata, a livello europeo, una forte integrazione economico-industriale, funzionale a garantire la pace nel continente, ora è necessario rafforzare il posizionamento internazionale dell'Europa, costruendo una consapevolezza comune verso l'approccio di "total security", che includa le istituzioni, l'industria e la società civile.

Impostazione metodologica dello Studio strategico

5 consapevolezze dello scenario geopolitico e geoeconomico globale

1. Il mondo è in uno stato di no-peace, in cui l'Unione Europea è sempre meno influente
2. I Paesi sono esposti a minacce ibride di natura imprevedibile e non convenzionale, che sfruttano vulnerabilità specifiche per infliggere danni a infrastrutture critiche, a settori governativi, economici e sociali
3. Emerge la necessità di un approccio alla difesa di total security che coordini gli strumenti di influenza sia militare che politico-economica
4. La leadership nelle tecnologie digitali avanzate è un elemento sempre più centrale per il posizionamento geopolitico. In questo, l'Europa risulta più debole rispetto alle altre grandi potenze mondiali
5. Lo sviluppo delle tecnologie digitali per la difesa richiede un nuovo modello di collaborazione con il settore privato

5 debolezze dell'Europa

1. Debolezza nel settore digitale
2. Frammentazione politica, militare, industriale e della ricerca
3. Limitati investimenti pubblici e difficoltà per gli investimenti privati
4. Dipendenza strategica
5. Social Acceptance

10 proposte dello Studio strategico

Un mondo in stato di “no-peace”

CAPITOLO 1

Il primo capitolo dello Studio Strategico si pone l'obiettivo di offrire una panoramica sullo scenario geopolitico, economico e tecnologico che qualifica il **mondo attuale in uno stato di "no-peace"**, con le relative implicazioni per l'Unione Europea.

Nel corso del capitolo verranno analizzati i fattori di instabilità altamente complessi e interconnessi, di portata globale che hanno, e avranno nel medio termine, un impatto sulle dinamiche interne dell'Unione Europea e dei 27 Paesi Membri. Nello specifico, verranno presentati il cambiamento climatico, i conflitti sia vicini sia lontani dai confini europei e l'accesso a risorse energetiche, tecnologie e materie prime.

Da questa analisi emergerà la necessità di un riposizionamento dell'Europa in questo mutato ordine globale, caratterizzato da una fitta e fluida rete di alleanze regionali, e del posizionamento dell'Unione Europea in questo contesto.

Infine, il capitolo approfondisce l'importanza del settore della difesa per la sicurezza, la stabilità e la resilienza dell'Unione Europea, analizzando le spese destinate alla difesa nei principali Paesi del mondo.

CONSAPEVOLEZZA 1

Il mondo è in uno **stato di no-peace**, in cui l'**Unione Europea è sempre meno influente**

1.1 Il mondo in uno stato di “no-peace”

Il punto di partenza del presente Studio strategico identifica una prima consapevolezza, cruciale per le considerazioni e le analisi successive sullo stato della difesa europea e sul ruolo delle tecnologie digitali: **la prosperità e la democrazia europea sono minacciate da quattro fattori di instabilità a livello mondiale** che impongono una seria riflessione rispetto alla **preparazione dell’Europa nell’affrontare un futuro in stato di «no-peace»**.

In particolare, i sempre più frequenti fenomeni di cambiamento climatico influenzano profondamente la resilienza di alcune regioni, con un conseguente impatto sui flussi migratori. La diffusione di aree di tensione sia nei territori vicini sia in quelli lontani dai confini europei ha riacceso il dibattito pubblico e politico sullo stato di prontezza e sicurezza dell’Europa in materia di difesa. Parallelamente, l’accesso a risorse energetiche, tecnologie avanzate e materie prime è diventato sempre più determinante per l’autonomia strategica di un Paese.

Queste tre dinamiche, altamente complesse e interconnesse tra loro, mettono in luce un mutato ordine globale e la necessità di un ripensamento del posizionamento geopolitico dell’Europa in questo quadro.

Figura 1. I fattori di instabilità a livello mondiale.
Fonte: elaborazione TEHA Group su fonti varie, 2024.

I cambiamenti climatici cui stiamo assistendo negli ultimi anni hanno conseguenze dirette sullo stress idrico e sulla scarsità di cibo, provocando un incremento delle migrazioni e creando un'ulteriore pressione sui confini europei

Fenomeni climatici estremi	In uno scenario di aumento di temperatura di 2.0 C°: • **Eventi di temperatura estrema:** **x5,6** volte in frequenza e **x2,6** in intensità* • **Eventi pluviometrici estremi:** **x1,7** volte in frequenza e **+14%** in intensità*	I fenomeni climatici estremi continueranno ad aumentare nei prossimi decenni con **impatti diretti sull'economia e la tenuta democratica di molti paesi**
Stress idrico	L'**83%** della **popolazione** esposta a stress idrico estremo è in **Medio Oriente e in Nord Africa** (meno di 2.000 km dalle coste italiane)	Entro il 2050, si prevede che la **domanda di acqua** nell'Africa Sub-Sahariana aumenterà del **163%**
Sicurezza alimentare	1,1 miliardi di persone vive in **condizioni di povertà multidimensionale** (misura le privazioni interconnesse in materia di salute, istruzione e tenore di vita che incidono direttamente sulla vita e sul benessere di un individuo)	Il **53%** della popolazione in condizioni di povertà, pari a circa **600 milioni di persone**, si trova in **Africa Sub-Sahariana** e in **Medio Oriente**
Incremento delle migrazioni in Europa	**In Europa il numero** di rifugiati, richiedenti asilo e altri bisognosi di protezione internazionale è **più che triplicato tra il 2021 e il 2022**, superando i **10 milioni**	Le crisi internazionali in corso ai confini dell'Europa influiranno ancora di più, gravando la **pressione sulle risorse e il dibattito pubblico** in Unione Europea

Figura 2. Principali fenomeni con impatto sui flussi migratori. (*) Rispetto allo scenario di riferimento 1850 – 1900.

Fonte: elaborazione TEHA Group su fonti varie, 2024.

1.1.1 I CAMBIAMENTI CLIMATICI

Nell'attuale epoca di riscaldamento globale, **i fenomeni climatici estremi sono in aumento e continueranno ad aumentare**, sia in termini di frequenza che di intensità. In uno scenario di incremento di temperatura pari a 2.0 C°, si prevede per gli eventi di temperatura estrema un aumento di frequenza fino a 5,6 volte e un'intensificazione fino a 2,6 volte[1] rispetto allo scenario di riferimento 1850 – 1900. In parallelo, gli eventi pluviometrici estremi saranno 1,7 volte più frequenti e più intensi del 14%.

Allo stesso tempo, siccità prolungate alternate a piogge intense e irregolari possono ridurre la disponibilità di risorse idriche e il livello di fiumi, laghi e falde acquifere, amplificando il **rischio di stress idrico**, soprattutto in regioni già aride o semiaride come il **Medio Oriente e il Nord Africa, dove risiede l'83% della popolazione mondiale esposta a stress idrico estremo**[2], e che si trova a soli 2.000 km di distanza dalle coste italiane. La situazione è destinata ad aggravarsi: entro il 2050, si prevede che la domanda di acqua nell'Africa subsahariana aumenterà del 163%, quasi 4 volte il tasso di crescita della domanda di acqua in America Latina (43%), la seconda regione con la crescita più alta.

Questi fenomeni hanno impatti diretti sulla stabilità socioeconomica di regioni già in difficoltà: secondo il Global Multidimensional Poverty Index, l'Africa Sub-Sahariana e il Medio Oriente ospitano il **53% della popolazione mondiale in condizioni di povertà, pari a quasi 600 milioni di persone**[3].

Condizioni economiche difficili, insicurezza alimentare, cambiamenti climatici e conflitti spesso costringono le persone a migrare in cerca di migliori opportunità di vita: nel 2023, si stimano oltre 117,3 milioni di sfollati nel mondo. **Le migrazioni verso l'Europa sono un fenomeno in crescita, con il numero di rifugiati, richiedenti asilo e altri bisognosi di protezione internazionale che è più che triplicato tra il 2021 e il 2022, superando i 10 milioni di persone**[4]. Le crisi internazionali in corso ai confini dell'Europa influiranno ancora di più, gravando la pressione sulle risorse e il dibattito pubblico in Unione Europea.

1 Fonte: elaborazione TEHA Group su dati IPCC, 2024.
2 Fonte: elaborazione TEHA Group su dati World Resources Institute, 2024.
3 Fonte: elaborazione TEHA Group su dati UN Human Development Report Office (HDRO) e Oxford Poverty and Human Development Initiative (OPHI), 2024.
4 Fonte: elaborazione TEHA Group su dati United Nations High Commissioner for Refugees (UNHCR), 2024.

Le aree di instabilità a livello globale sono aumentate rispetto a qualche anno fa, con le principali aree di crisi (Ucraina, Medio Oriente e Africa) sempre più vicine all'Europa e con crescenti tensioni nell'area del Pacifico occidentale (Taiwan)

Conflitti vicini all'Europa 	• Dal 2022, il conflitto in **Ucraina** ha causato **oltre 500 mila morti e feriti** tra i due schieramenti • Dopo l'attacco di Hamas del 7 ottobre, **Israele** ha avviato un'**offensiva aerea e terrestre a Gaza**, con il rischio di escalation e allargamento del conflitto dopo gli attacchi Houthi nel Mar Rosso	I conflitti vicini ai confini dell'Europa hanno **impatti economici in termini di interscambio commerciale** (Ucraina e Russia producevano **¼** del grano mondiale) e **aiuti militari** (l'UE e i Paesi Membri hanno fornito **€ 63,3 mld** in 2 anni), oltre a un **incremento dei flussi migratori**
Conflitti lontani dall'Europa 	Oltre ai motivi ideologici dietro alla **tensione tra Cina e Taiwan**, ci sono **fattori strategici, militari ed economici**. Il controllo su Taiwan offrirebbe alla Cina la possibilità di espandere l'**influenza militare nell'Oceano Pacifico**. Taiwan è anche il **2°** produttore mondiale di **semiconduttori**	Un'escalation a Taiwan porterebbe a uno spostamento del **focus e delle forze militari USA verso il Pacifico**, oltre alla **contrazione del PIL mondiale** (con stime fino a **-10%**) e **interruzioni nelle catene del valore** (**¼** dell'import UE da Taiwan è di componenti elettroniche)
Relazioni geopolitiche in Africa 	**In Africa** si susseguono conflitti e tensioni politiche, con **8 colpi di stato riusciti tra il 2020 e il 2023** (e 3 tentati)	**Russia** e **Cina** sono motivate da **forti interessi** in Africa: nell'ultimo quinquennio hanno aumentato la **presenza militare** (**~5.000** soldati del Gruppo Wagner) ed **economica** (i creditori cinesi rappresentano il **12%** del debito estero privato e pubblico dell'Africa)

Figura 3. Le aree di instabilità a livello globale.

Fonte: elaborazione TEHA Group su fonti varie, 2024.

1.1.2 LE AREE DI INSTABILITÀ

Il mondo è lontano dall'essere in una condizione di pace duratura: negli ultimi anni, **le aree di tensione sono aumentate** significativamente e, tra queste, alcune sono di più **diretto interesse per l'Europa**: la guerra russa in Ucraina, il conflitto a Gaza, le guerre civili in alcuni paesi in Africa, l'aumento di tensione nel Pacifico Occidentale tra la Repubblica Popolare Cinese e la Repubblica di Cina (Taiwan).

L'invasione russa dell'Ucraina ha segnato la fine del più lungo periodo di pace nella storia recente dell'Europa, interrompendo decenni di stabilità e cooperazione internazionale. A due anni dall'avvio, si stima che il conflitto abbia causato mezzo milione di morti e feriti tra i due schieramenti. Inoltre, si sono registrati danni diretti alle infrastrutture e agli edifici ucraini per un valore complessivo di 152 miliardi di dollari[5] e una riduzione del PIL ucraino (a prezzi correnti) pari al 22% tra il 2021 e il 2022. Il volume delle esportazioni dell'Ucraina si è ridotto del 37% nel primo anno di guerra, con un saldo negativo della bilancia commerciale pari a 12,4 miliardi di euro nel 2022 (-144% vs. 2021), aggravatosi nel 2023 a 24,8 miliardi di euro. **Si stima che saranno necessari 486 miliardi di dollari per la ripresa e la ricostruzione del territorio ucraino.**

In termini assoluti, l'**Europa**[6] **è il primo fornitore di supporto per l'Ucraina, con un contributo pari a 102 miliardi di euro** (a cui aggiungere 75,8 miliardi di euro ancora da consegnare), seguita dagli Stati Uniti con 73,9 miliardi di euro (a cui aggiungere 24,7 miliardi di euro). Vi è una differenza nella tipologia di aiuti distribuiti, distinti tra militari, finanziari e umanitari: **se il contributo delle istituzioni comunitarie è quasi esclusivamente in forma finanziaria (per un valore pari a 33,7 miliardi di euro), per gli aiuti militari** – intesi come fornitura di assistenza, attrezzature militari e sovvenzioni e prestiti per attrezzature militari – gli Stati Uniti sono il singolo maggior fornitore, per 50,4 miliardi di euro (33,8% del totale di **148,8 miliardi di euro**), mentre i singoli Stati Membri hanno complessivamente contribuito per un valore pari a 47,9 miliardi di euro (32,2%). **Nell'ipotesi in cui, in seguito all'elezione presidenziale negli Stati Uniti, il flusso di aiuti militari americani dovesse interrompersi, l'Europa dovrebbe raddoppiare l'attuale ritmo di fornitura di armamenti** per garantire lo stesso flusso di armamenti all'Ucraina e, di conseguenza, la sicurezza dei confini europei. Se la Russia dovesse vincere il conflitto e rovesciare il governo di Kiev, le rivendicazioni russe rappresenterebbero un ulteriore indebolimento geopolitico per l'Europa: le forze russe potrebbero stabilire nuove basi militari ai confini di Polonia, Slovacchia, Ungheria

5 Fonte: elaborazione TEHA Group su dati Institute for the Study of War, 2024.

6 Si intende i contributi complessivi delle istituzioni europee (Commissione, Consiglio, Banca Europea per gli Investimenti) e dei 27 Paesi Membri, Regno Unito, Norvegia, Svizzera e Islanda.

e Romania, minacciando altresì gli Stati baltici e la Finlandia. Ciò richiederebbe lo schieramento di forze militari di terra e aeree nei Paesi dell'Europa orientale, oltre allo stanziamento di ingenti spese difensive.

In un'altra regione ai confini dell'Europa è in corso un sanguinoso conflitto tra Israele e Hamas. A partire dagli attacchi dei miliziani di Hamas del 7 ottobre 2023, l'esercito israeliano ha avviato un'intensa campagna di bombardamenti, cui ha fatto seguito, a partire dal 26 ottobre, un'invasione di terra. Ad oggi, si stima che sono stati distrutti un numero di edifici compreso fra il 49% e il 61% del totale della Striscia di Gaza. A otto mesi dall'inizio del conflitto, la stima dei morti è pari a 1.500 israeliani (di cui 300 soldati e 1.200 civili) e oltre 37mila palestinesi. Secondo l'OMS la quasi totalità della popolazione di Gaza (2,2 milioni di abitanti) è senza cibo e a rischio carestia.

Il conflitto a Gaza ha provocato una reazione degli Houthi nel Mar Rosso, con ripercussioni sugli scambi commerciali tra l'Europa e il resto del mondo. Infatti, attraverso il Mar Rosso transita quasi il 15% del commercio marittimo globale, compreso l'8% del commercio globale di cereali, il 12% del petrolio commercializzato via mare e l'8% del gas naturale liquefatto. A causa della crisi nel Mar Rosso, molte navi hanno modificato le proprie rotte, prediligendo il passaggio da Capo di Buona Speranza rispetto a Suez, comportando in media 10-12 giorni aggiuntivi per una navigazione tra l'Italia e l'Asia. Tra ottobre 2023 e marzo 2024 la media di navi merci transitate da Capo di Buona Speranza è aumentata del 42%, mentre quella per il Canale di Suez si è ridotta del 56%, comportando una riduzione dei traffici nei maggiori porti italiani pari a -9% nel periodo dicembre 2023 – gennaio 2024, rispetto all'anno precedente[7]. I costi del trasporto marittimo dall'Asia all'Europa a metà gennaio erano superiori di 4,5 volte rispetto a quelli di novembre 2023. Dalla seconda metà di gennaio hanno però iniziato a diminuire (c.a. -41% dall'Asia al Nord Europa e –22% dall'Asia al Mediterraneo tra metà gennaio e fine marzo 2024)[8].

Inoltre, **si teme il rischio di escalation e allargamento del conflitto nella macroregione.** Lungo il confine libanese-israeliano si stanno verificando schermaglie quotidiane tra Israele e la milizia sciita Hezbollah, supportata dall'Iran, con il rischio di trasformarsi in un nuovo conflitto dopo gli scontri del 2006. In Siria, si stanno verificando attacchi alle catene logistiche e ai depositi di armi iraniane da parte delle Forze di Difesa Israeliane. Ad aprile 2024, l'Iran ha lanciato un attacco (preventivamente comunicato) con missili e droni contro Israele, aumentando ulteriormente il rischio di future escalation.

Nel continente africano si susseguono conflitti e tensioni politiche, con 8 colpi di stato riusciti tra il 2020 e il 2023 (e 3 tentativi falliti) in Niger, Burkina Faso (due volte), Sudan, Guinea, Mali, Gabon e Chad. Alla base ci sono la forte instabilità politica delle aree coinvolte, oltre che la diffusa corruzione e la debolezza delle istituzioni democratiche, anche a causa della presenza di gruppi jihadisti. I

7 Fonte: elaborazione TEHA Group su dati UN Global Platform (IMF PortWatch), 2024.
8 Fonte: elaborazione TEHA Group su dati Oxford University, Institute of Shipping Economics and Logistics e Freightos, 2024.

colpi di stato militari sono stati favoriti dalla presenza del gruppo Wagner (recentemente rinominato Africa Corps), compagnia di mercenari affiliata al governo russo con uno schieramento di circa 5.000-7.000 soldati. I golpe militari sembrano essere favoriti da un sempre maggiore "immobilismo" della comunità internazionale, che si limita a isolare i nuovi regimi, senza adottare misure incisive. In termini di confronto, le forze militari francesi in Africa ammontano a circa 4.000 unità, mentre quelle italiane a meno di 1.000 unità. Il continente africano è guardato con interesse anche dalla Cina, dove esercita un soft power attraverso prestiti finanziari. I creditori cinesi rappresentano il 12% del debito estero privato e pubblico dell'Africa, che è aumentato di oltre cinque volte a 696 miliardi di dollari dal 2000 al 2020[9].

Infine, nella regione del Pacifico Occidentale, **Taiwan rappresenta un tassello fondamentale per lo scenario geopolitico e geoeconomico attuale e futuro.** Fin dalla sua indipendenza nel 1949, Pechino la rivendica come una parte inalienabile del suo territorio e considera la riunificazione «un'inevitabilità storica», come dichiarato da Xi Jinping nel corso del Discorso di fine anno il 31 dicembre 2023. Oltre alle motivazioni ideologiche, questa pretesa è alimentata da fattori strategici, militari ed economici: il controllo su Taiwan offrirebbe alla Cina la possibilità di espandere la propria influenza militare nell'Oceano Pacifico. Inoltre, Taiwan rappresenta la 21° economia a livello mondiale con un prodotto interno lordo pari a 760 miliardi di dollari nel 2022[10] e il 2° produttore di semiconduttori (con una quota pari al 22% della produzione mondiale). Le relazioni tra Taiwan e USA sono regolate attraverso il Taiwan Relation Act approvato nel 1979 con lo scopo di contribuire a preservare la pace, la sicurezza e la stabilità nel Pacifico occidentale. L'atto afferma che «gli Stati Uniti metteranno a disposizione di Taiwan gli articoli di difesa e i servizi di difesa nella quantità necessaria per consentire a Taiwan di mantenere sufficienti capacità di autodifesa». Infatti, se Taiwan venisse conquistata da Pechino, gli Stati Uniti perderebbero un basilare avamposto sul Pacifico, con conseguenze economiche elevate. **Si stima che l'economia mondiale potrebbe perdere fino a 10.000 miliardi di dollari** a causa dell'interruzione delle filiere dei microprocessori, delle sanzioni su Pechino e dell'impatto della guerra sui mercati[11]. Per l'Europa, **ciò implicherebbe inoltre uno spostamento delle forze militari statunitensi verso il Pacifico, rendendo l'Europa più vulnerabile e isolata rispetto alle minacce provenienti dalle altre regioni**.

9 Fonte: elaborazione TEHA Group su dati Chatham House e MIF, 2024.
10 Fonte: elaborazione TEHA Group su dati IMF, 2024.
11 Fonte: elaborazione TEHA Group su dati Bloomberg Economics, 2024.

L'Unione Europea si trova di fronte a sfide significative di dipendenza di energia, materie prime e terre rare per soddisfare le proprie esigenze, con impatti sul settore tecnologico e sul settore digitale, fondamentali per la duplice transizione (energetica e digitale), ponendo sfide significative per la sicurezza e l'autonomia strategica

Dipendenza energetica 	Nel 2022, l'UE ha registrato un **aumento dell'importazione dell'energia** pari all'**11,1%** rispetto al 2000; l'incremento maggiore è stato registrato dai combustibili fossili solidi (**+53,3%** tra il 2000 e il 2022) e dal gas naturale (**+48,5%**)	Nonostante gli sforzi verso la transizione energetica e l'utilizzo di energie rinnovabili, nel medio termine l'UE sarà dipendente dai **combustili fossili,** che rappresentano ancora i **2/3 del mix energetico**
Dipendenza tecnologica per la transizione energetica 	L'UE importa **137 categorie di prodotti tecnologici** con un impatto sulla **transizione energetica**: il **52%** proviene dalla Cina, il **15%** da Paesi del Sud-Est Asiatico e il **5%** dal Brasile	L'UE identifica **4 tecnologie con approvvigionamento ad alto rischio** e di cui si prevede che la domanda di import aumenterà entro il 2030: **batterie** (**x49 volte**), l'**eolico** (**x44 volte**), **solare FV** (**x7 volte**) e **veicoli elettrici a celle a combustibile**
Dipendenza tecnologica per la transizione digitale 	**L'Europa è sprovvista** di **terre rare**: nessun Paese europeo è tra i primi 10 Paesi per riserve e la Cina detiene circa il **38%** delle riserve mondiali, seguita da Vietnam e Brasile	Le terre rare sono utilizzate nei **prodotti di consumo ad alta tecnologia** (telefoni, hardware, veicoli elettrici e ibridi, etc.) e nella **difesa** (display elettronici, sistemi di guida, laser, radar, sistemi sonar, etc.)

Figura 4. La dipendenza energetica e tecnologica dell'Unione Europea.

Fonte: elaborazione TEHA Group su fonti varie, 2024.

1.1.3 L'ACCESSO A ENERGIA, TECNOLOGIE E MATERIE PRIME

Nell'attuale panorama geopolitico e tecnologico, l'Unione Europea si trova di fronte a sfide significative relative alla dipendenza da importazioni di energia, di materie prime e di terre rare per soddisfare le proprie esigenze energetiche e tecnologiche. Questa **dipendenza non incide solo sulla sicurezza energetica, ma impatta anche il settore tecnologico e digitale, fondamentali per la duplice transizione** verso un futuro sostenibile e digitalizzato, ponendo sfide significative per la sicurezza e l'autonomia strategica.

Nel 2022, **l'Unione Europea ha registrato un aumento dell'importazione di energia pari all'11,1% rispetto al 2000**, con un incremento dei combustibili fossili solidi (+53,3%) e del gas naturale (+48,5%), importando il 62,5% dell'energia disponibile lorda[12]. Nel quarto trimestre del 2023, l'Unione Europea ha ridotto la sua dipendenza dalla Russia sul gas (attualmente pari a 12,7% del totale, rispetto al 48% registrato nel 2021) e dal petrolio (attualmente pari a 3,5% del totale, rispetto al 24,8% registrato nel 2021), ma ha aumentato la sua dipendenza da altri Paesi come Algeria, Azerbaijan, Libia e Arabia Saudita[13]. Nonostante gli sforzi e gli ambiziosi obiettivi per la transizione energetica e l'adozione di fonti rinnovabili, **i combustibili fossili rappresentano ancora due terzi del mix energetico dei Paesi europei**.

L'Unione Europea è anche dipendente da importazioni di materie prime per componenti ad alta tecnologia: **sono 137 le categorie di prodotti tecnologici importati e impiegati per lo sviluppo delle Clean Tech**, di cui il 52% proviene dalla Cina, il 15% dai Paesi del Sud-Est Asiatico e il 5% dal Brasile[14]. In particolare, la Commissione Europea identifica **quattro tecnologie dipendenti da materiali della catena di approvvigionamento ad alto rischio**, e di cui si prevede che la domanda di importazioni crescerà entro il 2030: le batterie (con un aumento pari a 49 volte in più), l'eolico (pari a 44 volte), il solare fotovoltaico (pari a 7 volte) e i veicoli elettrici a celle a combustibile. Inoltre, l'Europa si trova in una posizione di svantaggio anche per le terre rare, non avendo nessun Paese europeo tra i primi dieci per riserve mondiali. La Cina ne detiene circa il 38%, seguita da Vietnam e Brasile[15]. Questi materiali sono cruciali per i prodotti di consumo (per es. telefoni, hardware, veicoli elettrici e ibridi) e per il settore della difesa (per es. display elettronici, sistemi di guida, laser, radar e sistemi sonar). **Materiali come cobalto, litio, silicio, titanio, grafite, platino e le terre rare, sono inclusi nell'elenco dei materiali critici dell'UE** e costantemente monitorati per l'alto rischio di approvvigionamento.

12 Fonte: elaborazione TEHA Group su dati Eurostat, 2024.
13 Fonte: elaborazione TEHA Group su dati Comext, 2024.
14 Fonte: elaborazione TEHA Group su dati Commissione Europea, 2024.
15 Fonte: TEHA Group su dati US Geological Survey, 2024.

Da un mondo bipolare, sta emergendo un mondo sempre più multipolare, con una complessa rete di alleanze regionali con diversi schemi di integrazione economica e politica

Figura 5. Le alleanze multilaterali e le organizzazioni regionali.

Fonte: elaborazione TEHA Group su fonti varie, 2024.

1.1.4 IL NUOVO ORDINE GLOBALE

L'attuale scenario geopolitico è sempre più multipolare, con una **complessa rete di alleanze regionali**, integrate economicamente e politicamente in maniera differenziata. Tra le principali alleanze multilaterali figurano, oltre all'Unione Europea, l'Unione Africana, l'European Free Trade Association (EFTA), la Lega Araba, il Mercosur, il North American Free Trade Agreement (NAFTA), la Shangai Cooperation Organization, l'Association of South-East Asian Nations (ASEAN) e l'Asia-Pacific Economic Cooperation (APEC).

Tra queste, alcune sono sempre più rilevanti da un punto di vista economico, demografico e geopolitico, in particolare l'ASEAN (che comprende 10 paesi), l'Unione Africana (54 paesi) e la Lega Araba (23 paesi) e adottano un **approccio di politica estera definito di non-allineamento**, nonostante le azioni e le decisioni rivelino una complessità più profonda che riflette più spesso una posizione di **multi-allineamento**.

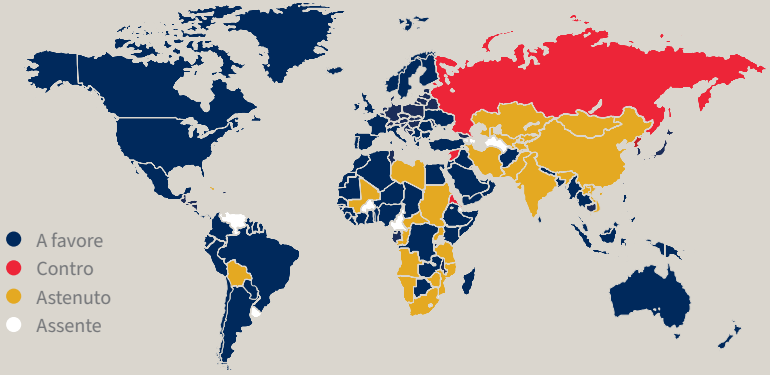
Il **gruppo dei BRICS (Plus) vuole posizionarsi come un crescente contrappeso al gruppo del G7**: nato con l'obiettivo di costruire un ordine economico, commerciale e finanziario alternativo a quello creato alla fine della Seconda Guerra Mondiale. Nel 2020, per la prima volta, i cinque Paesi BRICS hanno superato il G7 in termini di PIL e oggi rappresentano il 35,3% del PIL globale, superando la quota del G7 (29,4%). Tuttavia, i BRICS (Plus) non esprimono un posizionamento allineato strategicamente ed economicamente paragonabile a quello dei Paesi del G7; ciascun Paese BRICS (Plus) adotta, nelle diverse occasioni, decisioni in linea con l'interesse nazionale e senza un vero e proprio coordinamento con gli altri Paesi del Gruppo.

Si prevede inoltre che il divario si amplierà ulteriormente entro il 2028, quando i BRICS rappresenteranno il 36,6% e il G7 il 27,8% dell'economia mondiale[16]. Da anni richiedono, senza successo, la riforma del Consiglio di Sicurezza delle Nazioni Unite, con l'apertura di nuovi membri permanenti per garantire una maggiore rappresentanza.

16 Fonte: elaborazione TEHA Group su dati Banca Mondiale, 2024.

Lo scenario che emerge è una accentuata contrapposizione tra il blocco dei Paesi occidentali e i diversi poli che si configurano nel mondo, che prendono posizioni guidate da situazioni contingenti e orientate verso i propri interessi geopolitici e geoeconomici

Risultati delle votazioni all'Assemblea Generale dell'ONU alle 4 risoluzioni sull'invasione russa dell'Ucraina*, 2022-2023



Paesi che non hanno applicato sanzioni alla Russia dal 22 febbraio 2022 (evidenziati in arancio), febbraio 2024

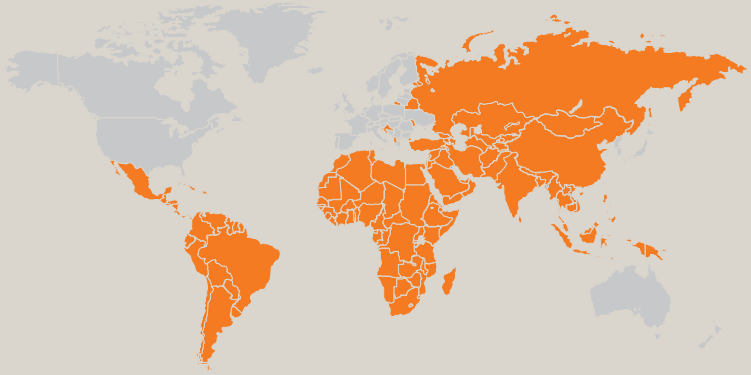


Figura 6. Posizionamento dei Paesi alle votazioni all'Assemblea Generale delle Nazioni Unite* sull'invasione russa in Ucraina (immagine a sinistra) e Paesi che non hanno applicato sanzioni alla Russia tra il 22 febbraio 2022 e febbraio 2024 (evidenziati in arancio, immagine a destra).

Fonte: elaborazione TEHA Group su dati Nazioni Unite, 2024.

* Risoluzione 11/1 del 2/3/2022 (Aggressione contro l'Ucraina), 11/2 del 24/3/2022 (Conseguenze umanitarie dell'aggressione contro l'Ucraina), 11/4 del 12/10/2022 (Integrità territoriale dell'Ucraina a difesa dei principi della Carta delle Nazioni Unite), 11/6 del 23/2/2023 (Principi della Carta delle Nazioni Unite per una pace giusta e duratura in Ucraina).

In questo contesto, le **alleanze tra Paesi sono molto fluide e guidate da situazioni contingenti e interessi geopolitici e geoeconomici**. Quello che emerge è una accentuata contrapposizione tra il blocco dei Paesi occidentali e i diversi poli che si configurano nel mondo, che prendono posizioni di volta in volta orientate rispetto ai propri interessi.

Questa dinamica è evidente a seguito delle **conseguenze a episodi di tensione tra Paesi appartenenti a diversi schieramenti**. L'invasione russa dell'Ucraina, ad esempio, è stata condannata solo dai Paesi Occidentali, che hanno imposto sanzioni e restrizioni commerciali alla Russia. Infatti, **oltre 16.000 sanzioni sono state applicate alla Russia, ma solo da 46 Paesi**[17]. Tuttavia, i paesi che non hanno adottato sanzioni contro la Russia rappresentano il 41,2% del PIL e ospitano l'84,5% della popolazione globale[18].

In merito alla Corea del Nord, soggetta a sanzioni dal 2006 su voto unanime del Consiglio di Sicurezza, il 26 maggio 2022 **Cina e Russia hanno posto il veto a una risoluzione, redatta dagli Stati Uniti, che avrebbe imposto ulteriori sanzioni alla Corea del Nord** al fine di limitare ulteriormente i suoi programmi di armi nucleari e missili balistici.

Infine, nel caso del conflitto a Gaza, il 25 marzo 2024 **il Consiglio di sicurezza delle Nazioni Unite ha approvato la prima risoluzione che chiede il cessate il fuoco immediato per il mese del Ramadan, il rilascio immediato e incondizionato degli ostaggi e "l'urgente necessità di aumentare il flusso" di aiuti a Gaza**. Quattrodici Paesi si sono schierati a favore, **con astensione degli Stati Uniti** perché la risoluzione non condannava in maniera esplicita Hamas. L'accordo arriva dopo cinque mesi di stallo durante i quali gli Stati Uniti hanno bloccato tre risoluzioni mentre la quarta, proposta dagli Stati Uniti, era stata bloccata dal veto di Cina e Russia (con l'Algeria che aveva espresso voto contrario e la Guyana astenuta).

Un punto di attenzione per la stabilità dello scenario internazionale è legato ai risultati delle elezioni programmate in più di 50 Paesi nel corso del 2024, durante le quali è chiamato a votare oltre il 50% della popolazione globale (pari a oltre 4 miliardi di persone) – in sette dei dieci Paesi più popolosi del mondo e in otto delle dieci principali economie del mondo, che rappresentano complessivamente il 58% del PIL mondiale. **I risultati delle elezioni svoltesi fino ad agosto 2024** (tra cui, India, Unione Europea, Francia, Regno Unito) **non hanno mostrato ripercussioni circa l'orientamento geopolitico dei singoli stati**. **Le elezioni più attese per la seconda metà del 2024 sono le presidenziali negli Stati Uniti,** in programma il 5 novembre 2024, **soprattutto per gli effetti sul piano economico e geopolitico e sulla ridefinizione degli schemi di sostegno all'Ucraina e alla presenza militare in Europa,** oltre alla posizione verso la Cina.

17 Fonte: elaborazione TEHA Group su dati Nazioni Unite, 2024.
18 Fonte: elaborazione TEHA Group su dati Banca Mondiale, 2024.

In questo mutato scenario internazionale, l'Unione Europea ha una rilevanza sempre più marginale rispetto al resto del mondo, sia in termini demografici sia in termini economici, con una crescente difficoltà ad esercitare un ruolo geopolitico di rilievo

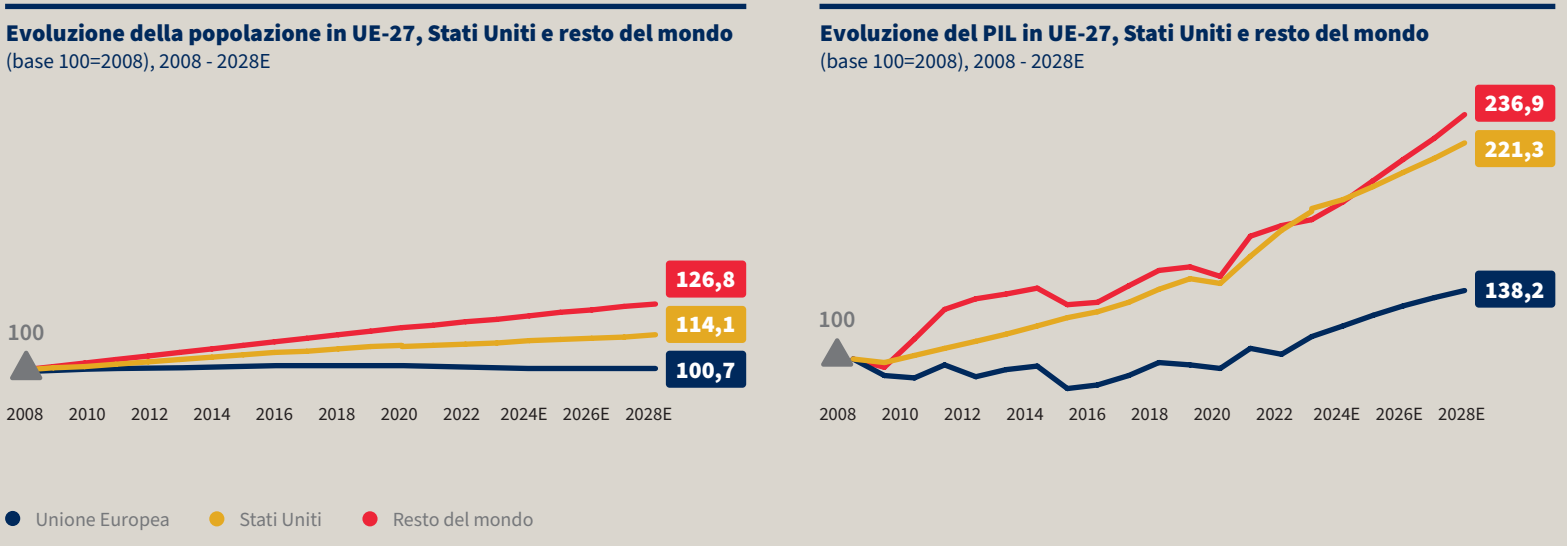


Figura 7. Evoluzione della popolazione (grafico a sinistra) e del Prodotto Interno Lordo (grafico a destra) in UE-27, Stati Uniti e resto del mondo, (anno base 100 = 2008), 2008 – 2028E.

Fonte: elaborazione TEHA Group su dati Banca Mondiale, 2024.

1.1.5 IL POSIZIONAMENTO DELL'UNIONE EUROPEA NEL NUOVO ORDINE GLOBALE

In questo scenario complesso, **l'Unione Europea si trova in una posizione di sempre minore rilevanza rispetto al resto del mondo, sia in termini di popolazione che di PIL**, con una crescente difficoltà ad esercitare un ruolo geopolitico di rilievo.

In termini demografici, mentre la popolazione dei 27 Paesi europei rimarrà pressoché stabile fino al 2028, con un leggero aumento pari a 0,7% rispetto al 2008, sia gli Stati Uniti che il resto del mondo mostrano una crescita significativa, con valori rispettivamente pari a +14,1% e +26,8% rispetto al 2008. In termini economici, le stime di crescita del PIL indicano una traiettoria positiva nei Paesi europei pari a +38,2% tra il 2008 e 2028. Tuttavia, nello stesso arco temporale, il PIL degli Stati Uniti è previsto più che raddoppiare rispetto al livello del 2008 (+121,3%) così come nel resto del mondo (+136,9%)[19]. Queste dinamiche accentueranno ancora di più la posizione di debolezza dell'Unione Europea rispetto al resto del mondo.

Pertanto, **l'Unione Europea ha bisogno fin da subito di potenziare la propria politica estera, di cui il settore della difesa è un elemento cardine**. In un contesto di integrazione europea, è fondamentale superare le divisioni interne e dedicare maggiori risorse per garantire la sicurezza e la crescita economica dell'Unione Europea e dei suoi Stati Membri. Allo stesso tempo, la frammentazione della politica estera e di difesa dell'UE è un ostacolo significativo per la sicurezza del continente. La recente crisi in Ucraina ha ulteriormente accentuato la necessità di sviluppare una politica estera unica attraverso cui l'Unione Europea possa essere percepita come un unico attore sulla scena internazionale.

19 Fonte: elaborazione TEHA Group su dati Banca Mondiale, 2024.

La spesa dell'Unione Europea in difesa è significativamente inferiore rispetto a quella degli Stati Uniti che, nel 2023, hanno speso circa 704 miliardi di dollari in difesa, pari al 3,23% del loro PIL. La Cina ha destinato l'1,7% del PIL alla difesa (i dati reali potrebbero essere di gran lunga maggiori rispetto a quelli dichiarati), mentre la Russia il 5,9% del PIL[20]. I paesi dell'UE aderenti alla NATO hanno allocato complessivamente 312 miliardi di euro, pari all'1,85% del PIL[21]. Anche a fronte delle continue pressioni per un aumento della spesa in difesa in Europa, **la NATO stima per il 2024 il superamento del target del 2,0% per i Paesi Europei**[22], come primo passo per colmare il divario con le altre potenze globali per garantire una difesa comunitaria più robusta e autonoma. Nel confronto tra le spese in difesa dei vari attori, inoltre, è importante considerare anche il differente 'potere d'acquisto' nei diversi contesti economici.

Se dal 2006 al 2020 tutti gli Stati membri avessero speso il 2% del PIL per la difesa, destinando il 20% di tale somma agli investimenti, sarebbero ora disponibili 1.100 miliardi di euro aggiuntivi per la difesa, di cui circa 270 miliardi di euro di investimenti. Questi investimenti non solo migliorerebbero le capacità difensive, ma stimolerebbero anche l'innovazione tecnologica e la crescita economica, dimostrando che la difesa è un elemento cardine non solo per la politica estera, ma anche per il benessere economico dell'Europa.

L'errore che l'Europa non deve fare è agire «in ordine sparso» in risposta alle sfide attuali e future: il dominio delle innovazioni tecnologiche è chiave sia per la leadership in ambito civile sia in ambito militare.

20 La spesa totale effettivamente destinata alla difesa dalla Cina e dalla Russia è stimata e probabilmente sottovalutata.
21 Fonte: elaborazione TEHA Group su dati Sipri, 2024.
22 Fonte: elaborazione TEHA Group su dati NATO, 2024.

Figura 8. Spesa totale per la difesa (in valori percentuali sul PIL) nei Paesi europei della NATO, Regno Unito, Stati Uniti, Cina e Russia, 2023.

Fonte: elaborazione TEHA Group su dati NATO e Sipri, 2024.

Le nuove minacce ibride e gli strumenti per contrastarle

CAPITOLO 2

Il secondo capitolo dello Studio Strategico si propone l'obiettivo di illustrare il panorama attuale delle nuove minacce ibride, caratterizzate da una continua evoluzione e da una crescente diversificazione, rapidità e capacità di estensione a più domini. In questo contesto, la democrazia e la prosperità economica dell'Europa sono sempre più vulnerabili a minacce ibride di natura imprevedibile e non convenzionale, che sfruttano specifiche vulnerabilità per infliggere danni a infrastrutture critiche, settori governativi, economici e sociali.

Nel corso del capitolo verranno analizzate l'evoluzione delle minacce militari, economiche, cognitive e di salute. Da questa panoramica emergerà la **necessità di un approccio alla difesa di total security**, che sarà illustrato nel dettaglio esaminando i paesi che hanno riformato la governance nazionale in materia di sicurezza per facilitare un maggiore coordinamento tra i diversi strumenti di difesa.

In particolare, verrà presentato il funzionamento del National Security Council degli Stati Uniti, istituito dal presidente Truman, che consiglia e assiste il Presidente e coordina le questioni di sicurezza nazionale tra le agenzie governative. Inoltre, saranno illustrati i consigli di sicurezza nazionale del Regno Unito (il National Security Council, istituito nel 2010), della Francia (il Conseil de Défense et de Sécurité Nationale, istituito nel 2009) e della Svezia (il National Security Council of Sweden, istituito nel 2022).

CONSAPEVOLEZZA 2

I Paesi sono esposti a minacce ibride di natura imprevedibile e non convenzionale, che sfruttano vulnerabilità specifiche per infliggere danni a infrastrutture critiche, a settori governativi, economici e sociali

2.1 Minacce Militari, Economiche, Cognitive e di Global Health

Il presente Studio si concentra su una consapevolezza cruciale: la democrazia e la prosperità economica dell'Europa sono esposte a **minacce ibride** di natura imprevedibile e non convenzionale. Queste minacce sfruttano vulnerabilità specifiche per infliggere danni a infrastrutture critiche, settori governativi, economici e sociali. Esse si manifestano in diverse forme, tra cui minacce militari, economiche, cognitive e sanitarie.

Le minacce militari stanno diventando sempre più diversificate e si estendono a più domini, con sistemi di attacco che sono sempre più rapidi e la comparsa di strumenti di attacco non convenzionali. Inoltre, la crescente sfida posta dagli attacchi cyber verso infrastrutture militari richiede un'attenzione particolare alla cyberwarfare.

Anche le minacce economiche evolvono nella loro natura, con una crescente rilevanza, anche in questo caso, in ambito cibernetico. Gli attacchi cyber sono in aumento e sono sempre più cross-border e cross-sector (governo, utilities, telecomunicazioni, finanza, sanità, etc.).

La guerra dell'informazione, costituita da fake news e deep-fake, inoltre, rappresenta una chiara minaccia alla democrazia, diventando sempre più attuale.

Il mutato contesto socio-demografico, il cambiamento climatico e la globalizzazione, infine, hanno contribuito ad aumentare la diffusione di malattie infettive. La resistenza antimicrobica continua a rappresentare una delle principali minacce per la salute pubblica a livello globale.

Le minacce militari sono in continua evoluzione rispetto a tre caratteristiche chiave: Diversificazione, Velocità ed Estensione

Figura 1. Principali caratteristiche dell'evoluzione delle minacce militari.

Fonte: elaborazione TEHA Group su fonti varie, 2024.

2.1.1 LE MINACCE MILITARI

Alle **minacce ad alta tecnologia**, con un grande potere distruttivo e con sviluppi tecnologici tendenzialmente prevedibili, come i cyber attacchi avanzati e le armi biologiche, si stanno affiancando sempre di più **minacce basate su tecnologie general purpose**. Queste ultime, pur avendo una capacità distruttiva limitata, sono imprevedibili e disponibili in grande quantità. Ne sono un esempio i razzi artigianali e i droni commerciali, facilmente reperibili e di facile utilizzo, che li rendono accessibili a una vasta gamma di attori e aumentano il rischio di utilizzi difficili da prevedere.

In questo contesto, sta emergendo una **contrapposizione tra armi sviluppate con tecnologie general purpose e a basso costo e sistemi di difesa sofisticati e molto costosi.** I razzi di fabbricazione russa modello Katyusha, ad esempio, utilizzati abitualmente da Hezbollah e da Hamas su Israele, costano circa 300 dollari l'uno. I missili Tamir utilizzati da Israele per intercettare i Katyusha, invece, costano tra 20.000 e 100.000 dollari ciascuno, con uno squilibrio finanziario che arriva fino a 333 volte a favore dell'attacco. L'attacco diretto dall'Iran contro Israele tramite missili e droni nella notte del 13-14 aprile 2024, invece, ha avuto un costo totale stimato tra 75 e 100 milioni di dollari, mentre il costo totale per difendersi dall'attacco di una sola notte è stato stimato in circa 1 miliardo di dollari, con uno squilibrio finanziario di almeno 10 volte a favore dell'attacco. Da ultimo, i droni armati utilizzati dagli Houthi contro i mercantili nel Mar Rosso hanno un costo stimato tra i 20.000 e i 50.000 dollari l'uno, mentre le munizioni utilizzate da americani ed europei per fermare gli attacchi (Standard Missile-2) sono dotate di sistemi di inseguimento elettronico e costano quasi 2 milioni di dollari l'una. Lo squilibrio finanziario è di almeno 40 volte a favore dell'attacco[23].

Per quanto costosi possano essere i sistemi di difesa, tuttavia, **le intercettazioni degli attacchi rimangono economicamente necessarie rispetto ai danni potenziali** che questi possono causare all'economia e alle infrastrutture, oltre alle perdite di vite umane. Le infrastrutture critiche (centrali elettriche, impianti di trattamento delle acque, infrastrutture stradali e ferroviarie), infatti, possono costare decine di miliardi di dollari. Il costo di una singola nave commerciale, allo stesso tempo, può variare da decine di milioni a centinaia di milioni di dollari, a cui occorre aggiungere il valore del carico trasportato (i cui costi di assicurazione sono triplicati dall'inizio degli attacchi). Le rotte alternative, inoltre, aggiungono 1 milione di dollari di costi solo di carburante per ogni tratta[24].

In questo scenario, emergono anche **minacce non convenzionali** difficilmente prevedibili. La "Sindrome dell'Avana", ad esempio, è una misteriosa malattia che ha colpito diplomatici e agenti segreti americani, primariamente basati a Cuba, ma anche in Cina

23 Fonte: TEHA Group su fonti varie, 2024
24 Fonte: Ibid.

e Germania, a partire dal 2014. Le vittime hanno riportato di aver sperimentato senza preavviso un'intensa pressione intracranica o l'esposizione a un rumore acuto, seguita da una serie di sintomi debilitanti, tra cui nausea, vertigini severe e, in alcuni casi, una perdita temporanea dei sensi. Sebbene la natura precisa e le cause della Sindrome dell'Avana rimangano oggetto di dibattito e indagine, una recente inchiesta realizzata da Insider in collaborazione con Der Spiegel e 60Minutes ha portato alla luce prove che suggeriscono che la Sindrome dell'Avana potrebbe avere origine dall'uso di armi a energia diretta utilizzate dai membri dell'Unità 29155 del servizio segreto militare russo (Gru)[25].

I **sistemi di attacco**, inoltre, sono **sempre più rapidi**, richiedendo la definizione di sistemi di monitoraggio e risposta in grado di attivarsi e rispondere entro pochi secondi. Se i missili balistici, con una velocità che può raggiungere i 6.000 Km/h, possono essere rilevati fino a 3.700 km di distanza dalle stazioni radar a terra (consentendo un tempo di preallarme di 25 minuti), i missili ipersonici possono raggiungere una velocità di 12.000 Km/h e possono essere rilevati solo fino a 600 km di distanza, riducendo il tempo di preallarme a 2,5 minuti (10 volte meno rispetto al tempo necessario per rilevare i missili balistici). Inoltre, i missili ipersonici sono caratterizzati da maggiore manovrabilità e da traiettorie più basse, rendendone l'intercettazione ancora più complessa. Allo stesso tempo, si registra una crescente obsolescenza dei sistemi di difesa, mentre i cicli di innovazione delle minacce sono sempre più veloci[26].

Le minacce militari sono in continua evoluzione, estendendosi anche al dominio spaziale. Con oltre 8.000 satelliti attivi, al 2023, nell'orbita terrestre che supportano la sicurezza militare e permettono il funzionamento di infrastrutture civili, la crescente dipendenza dallo spazio espone le infrastrutture spaziali a crescenti attacchi fisici e cyber. Nel 2024, la Russia ha lanciato un satellite in orbita terrestre bassa, considerato un'arma contro-spaziale in grado di attaccare altri satelliti. Prima dell'invasione dell'Ucraina, hacker del governo russo hanno attaccato la società Viasat, utilizzata anche dall'esercito ucraino per il comando delle forze armate. Questo attacco ha avuto ripercussioni su altre nazioni europee, interrompendo i servizi di internet satellitare a utenti civili e aziende. Durante la guerra, gli attacchi ai sistemi di comunicazione satellitare sono continuati, colpendo anche Starlink e rappresentando una crescente preoccupazione per i potenziali impatti a cascata. Inoltre, nel 2023, gli USA hanno avvistato e abbattuto un pallone spia cinese. I palloni spia presentano vantaggi specifici rispetto ai satelliti in termini di spionaggio: la strategia di Pechino sembrerebbe essere quella di assicurarsi il dominio del c.d. "near space", ossia quella parte di spazio a un'altitudine da terra compresa tra le 12 e la 62 miglia[27].

25 Fonte: TEHA Group su dati Insider, Der Spiegel e 60Minutes, 2024.
26 Fonte: TEHA Group su dati Congressional Research Service, 2024.
27 Fonte: TEHA Group su dati ENISA e fonti varie, 2024.

Infine, la crescente minaccia e potenza dei cyberattacchi richiede un'attenzione particolare alla **cyberwarfare**. In Ucraina, la guerra ibrida è cominciata almeno 45 giorni prima di quella fisica, con attacchi di Distributed Denial-of-Service (DDoS)[28] e di defacement che hanno avuto come target infrastrutture critiche, entità governative e finanziare presenti sul suolo ucraino. Alla vigilia dell'offensiva militare si è poi registrato un aumento dell'aggressività sul fronte cyber con un'escalation di attacchi. Attività distruttive collegate ad operazioni di sabotaggio sono iniziate a partire dal 23 febbraio 2022, attraverso la diffusione di un wiper, ovvero un tipo di malware con l'obiettivo di eliminare tutti i dati presenti sulle memorie dei dispositivi, provocando gravi danni alle infrastrutture coinvolte[29].

In questo contesto, la relazione annuale 2023 del Dipartimento delle Informazioni per la Sicurezza sulla politica dell'informazione per la sicurezza evidenzia come la Russia, a causa del perdurante isolamento verso l'Occidente, impieghi proprio il suo arsenale ibrido per cercare di recuperare parte della propria influenza internazionale. Ciò include le attività di spionaggio e di compromissione e l'eventuale sabotaggio di infrastrutture critiche, nonché metodi innovativi come lo sfruttamento (c.d. weaponization) del fenomeno migratorio, ossia la strumentalizzazione in chiave destabilizzante dei flussi di persone verso i Paesi europei connessi anche al conflitto in Ucraina[30].

28 Un attacco DDoS prende di mira sistemi digitali e servizi di rete nel tentativo di esaurire le risorse di un'applicazione. Questo tipo di attacco è realizzato attraverso l'invio di una quantità enorme di traffico, causando problemi alle funzionalità del sistema o mettendolo offline del tutto.

29 Fonte: TEHA Group su dati Security Operation Centre, 2024.

30 Fonte: TEHA Group su Relazione annuale 2023 sulla politica dell'informazione per la sicurezza, 2024.

Le nuove minacce militari generano preoccupazioni crescenti su possibili attacchi di elevata portata e intensità

Un **attacco cyber ai sistemi di trattamento idrico è in grado di minacciare gravemente la salute pubblica** alterando i livelli delle sostanze chimiche nell'acqua a livelli letali.

Il 19 aprile 2024 un cyber-attacco all'infrastruttura di trattamento dell'acqua a Tipton, Indiana, da parte di hacker russi, ha compromesso il funzionamento automatizzato dell'impianto.

Un **attacco cyber alle strutture sanitarie può compromettere il funzionamento del sistema sanitario**, aumentando complicazioni mediche, mortalità e pressione su altre infrastrutture ospedaliere.

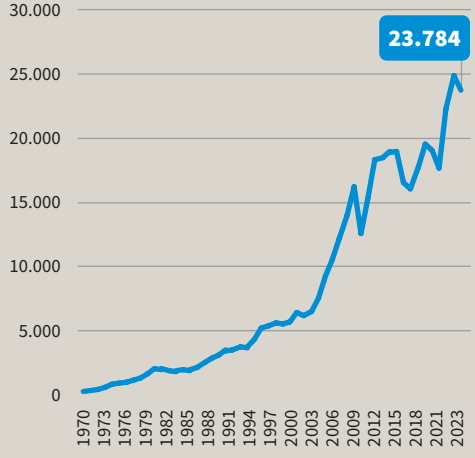
Tra il 10 e il 16 giugno 2024 sono stati rinviati 1.294 appuntamenti ambulatoriali e 320 interventi chirurgici programmati a causa di un attacco hacker a due ospedali di Londra.

Nel maggio 2023, l'ASL 1 Abruzzo ha subito un grave attacco cyber che ha bloccato tutti i sistemi dell'azienda sanitaria e ha esfiltrato i dati personali dei pazienti, rilasciando circa 520 GB di dati, tra cui referti e cartelle cliniche.

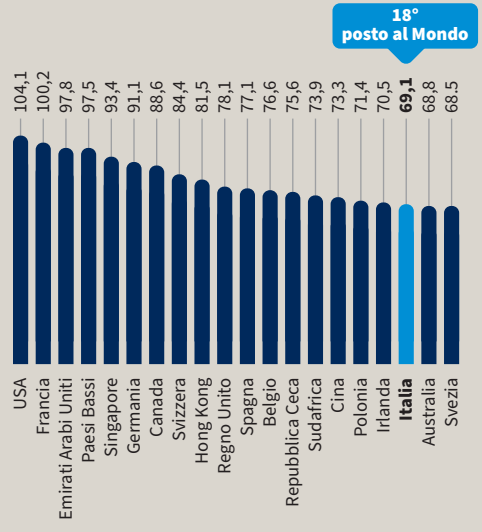
Con una gittata massima tra i 1.500 e i 2.000 Km e una velocità massima durante l'avvicinamento finale al bersaglio compresa tra 10.620 e 12.250 km/h, **il missile ipersonico russo Kinzhal è in grado di raggiungere Milano in meno di 10 minuti** se lanciato da Kaliningrad.

La globalizzazione è inarrestabile, con le esportazioni che hanno sfiorato i 25.000 miliardi di dollari nel 2022 e un'alta esposizione a eterogeneità geografica degli approvvigionamenti per ogni Paese. Ciò espone a rischi di instabilità: le restrizioni economiche e commerciali sono diventate uno strumento di potere e controllo per gli Stati: nell'ultimo quinquennio, le restrizioni commerciali sono più che triplicate

Volume delle esportazioni mondiali di beni
(miliardi di Dollari), 1970 - 2023



Top 20 Paesi al Mondo per eterogeneità geografica delle catene di approvvigionamento
(numero medio di Paesi partner per Euro di import), 2021



Numero di restrizioni al commercio,
2009-2023

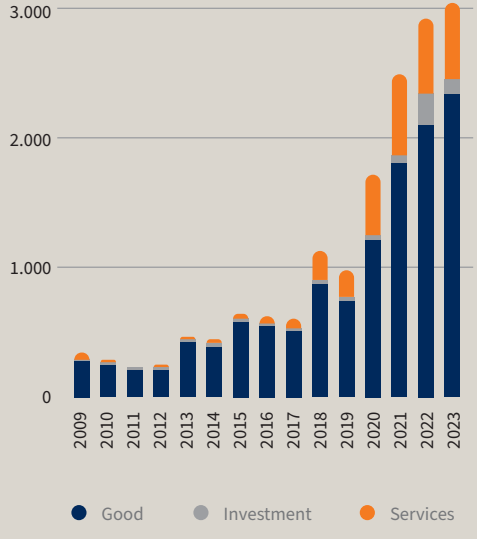


Figura 2. La crescita del commercio globale e delle restrizioni commerciali.

Fonte: elaborazione TEHA Group su dati UNCTAD, CEPII e Fondo Monetario Internazionale, 2024.

2.1.2 LE MINACCE ECONOMICHE

Il commercio globale è in costante crescita, con le **esportazioni** che nel 2022 hanno **sfiorato i 25.000 miliardi di dollari**[31]. Questo aumento è evidente anche nei flussi di container a livello globale, che hanno raggiunto i massimi storici, quasi raddoppiando dal 2007[32] a oggi[33]. Inoltre, tutti i Paesi sono esposti a una significativa **eterogeneità geografica degli approvvigionamenti**. Al primo posto si trovano gli Stati Uniti, con ogni euro di import proveniente in media da oltre 104 Paesi diversi, seguiti da Francia (100,2) ed Emirati Arabi Uniti (97,8). L'**Italia** si posiziona al 18° posto al mondo, con **ogni euro di import proveniente in media da oltre 69 Paesi diversi**[34].

Sebbene la globalizzazione sembri inarrestabile, essa espone a significativi rischi di stabilità: **nell'ultimo quinquennio le restrizioni commerciali sono più che triplicate**. I Paesi stanno così rivalutando i loro partner commerciali sulla base di preoccupazioni economiche e di sicurezza nazionale, con i flussi commerciali e di investimento che vengono reindirizzati tenendo in sempre maggiore considerazione valutazioni geopolitiche. Ciò espone a rischi ancora più rilevanti per i paesi che devono garantire sicurezza con nuove tecnologie digitali.

In questo scenario, già nel 2020 **quasi la metà (44,6%) delle imprese italiane con insediamenti produttivi all'estero** aveva **iniziato a cambiare strategia di localizzazione**. Tra queste, il 28,9% aveva annunciato un processo di backshoring (rientro in Italia), il 14,0% era intenzionato a effettuare un reshoring (rilocalizzazione in un altro Paese) e solo l'1,7% aveva previsto un nearshoring (rilocalizzazione in un Paese vicino)[35]. **La regione asiatica (Cina in particolare) è quella da cui rientrano più aziende sia in Italia che nell'UE**. Nello specifico, delle imprese rientranti in UE e in Italia, rispettivamente il 45% e il 43% rientrano dall'Asia (di cui, rispettivamente, il 34% e il 32% dalla Cina). In queste dinamiche, anche il reshoring intra-europeo gioca un ruolo di rilievo, con il 26% delle imprese rientranti in UE e il 25% delle imprese rientranti in Italia che rientrano dall'Europa occidentale[36].

31 Fonte: TEHA Group su dati UNCTAD, 2024.
32 Prima rilevazione disponibile
33 Fonte: TEHA Group su dati Institute for Shipping Economics and Logistics e WTO, 2024.
34 Fonte: TEHA Group su dati CEPII, 2024.
35 Fonte: TEHA Group su survey realizzata da Re4it, 2024.
36 Fonte: TEHA Group su dati UniCLUB MoRe reshoring, 2024.

Tutti i settori sono vulnerabili ad attacchi informatici, i quali possono mettere fuori uso, o trasformare in minaccia, infrastrutture civili fondamentali. Pertanto, è sempre più importante predisporre un sistema di prevention e detection delle minacce cyber completo, adeguato e resiliente

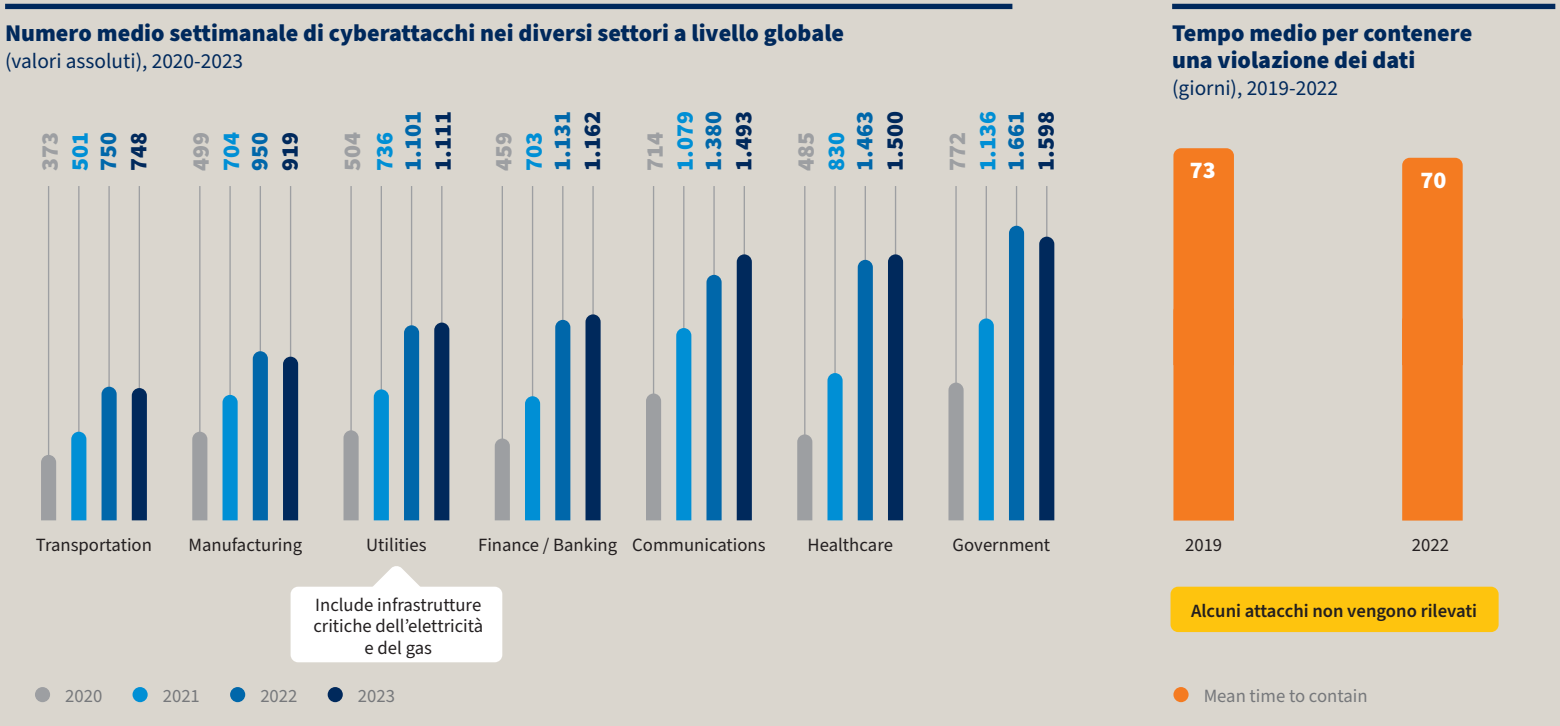


Figura 3. Numero medio settimanale di cyberattacchi nei diversi settori a livello globale (grafico a sinistra, valori assoluti), 2020-2023 e tempo medio per contenere una violazione dei dati (grafico a destra, giorni), 2019-2022.

Fonte: elaborazione TEHA Group su dati Checkpoint e IBM, 2024.

Gli attacchi cyber sono in crescita e sempre più cross-border e cross-sector. La pubblica amministrazione e il settore sanitario continuano a essere obiettivi primari, colpiti in media da oltre 1.500 attacchi settimanali[37]. In questo contesto, **cresce il numero di attacchi informatici che prendono di mira le infrastrutture critiche**. Nel 2022, un attacco informatico in Ucraina ha tentato di provocare un blackout che avrebbe colpito 2 milioni di persone. Nel 2023, diversi siti web tedeschi, inclusi alcuni legati al Partito Socialdemocratico, sono stati colpiti. Nel febbraio 2024, una violazione di dati delle compagnie di assicurazione sanitaria francesi ha compromesso le informazioni sensibili di 33 milioni di cittadini. Nell'aprile 2024, in Italia, un fornitore di servizi diagnostici e di laboratorio, è stato colpito da un attacco che ha temporaneamente sospeso le operazioni in 380 laboratori e centri medici, con dati esfiltrati e successivamente diffusi nel dark web[38].

Ad oggi, il tempo medio per contenere una violazione dei dati è di circa 70 giorni. Questo lungo periodo di esposizione evidenzia la **necessità di implementare sistemi efficaci per la gestione delle minacce cyber**, inclusi piani, test e training specifici. Inoltre, molti attacchi non vengono rilevati, aumentando il rischio di danni prolungati[39]. Un aspetto ancora più importante è il tempo necessario per diffondere un ransomware che negli ultimi due anni è passato **da circa 2 mesi a meno di 4 giorni** (-94%)[40].

Il diritto internazionale non consente di lanciare attacchi preventivi per bloccare attacchi cyber. La dottrina dell'autodifesa preventiva incorporata nel diritto internazionale consente a uno stato di usare la forza in previsione di un attacco armato e imminente. In questo contesto, secondo il Manuale di Tallinn, che si concentra sulle norme del diritto internazionale applicabili alle operazioni cyber, riconosciuto come testo di riferimento in materia anche se senza valore giuridico vincolante, «qualsiasi uso della forza che ferisce o uccide persone o danneggia o distrugge proprietà» soddisferebbe il requisito di attacco armato cyber. Secondo il Manuale di Tallinn, nel contesto cibernetico, deve presentarsi «l'ultima possibile finestra di opportunità» per fermare un attacco armato. Determinare quando la finestra si stia chiudendo è una stima di diverse probabilità e gli attacchi preventivi devono rispettare i principi di proporzionalità e non discriminazione. Assicurare che queste condizioni siano rispettate è particolarmente difficile nel contesto cyber. Emerge quindi la **necessità di un intervento legislativo che normi il cyberattacco** insieme a un potenziamento di misure difensive di sicurezza informatica come la resilienza della sicurezza delle reti e la condivisione di informazioni sulle minacce[41].

37 Fonte: TEHA Group su dati Checkpoint, 2024.
38 Fonte: TEHA Group su fonti varie, 2024.
39 Fonte: TEHA Group su fonti varie, 2024.
40 Fonte: TEHA Group su dati IBM, 2024

41 Fonte: TEHA Group su Manuale di Tallin, 2024.

La guerra dell'informazione è sempre più attuale e costituisce una chiara minaccia alla democrazia

1 Deep fakes e contenuti generati con AI

Contenuti creati attraverso l'utilizzo di Intelligenza Artificiale che permettono di **comunicare informazioni distorte per influenzare l'opinione pubblica** attraverso la **riproduzione di voci di personaggi pubblici e familiari**

2 Manipolazione dei social media

Utilizzo di account di social network per **amplificare eventi su argomenti divisivi come immigrazione o guerre**. Questa strategia mira a sfruttare le tensioni sociali esistenti per seminare discordia

3 Influenza sulle elezioni

Tecniche di disinformazione concentrate sullo **screditare le istituzioni democratiche**, creando narrazioni che legano questioni politiche e locali a situazioni internazionali, come guerra, economia e alleanze internazionali

Obiettivo comune: **interferire nelle dinamiche politiche e nei processi decisionali, influenzando, alterando la realtà percepita e fomentando un clima di incertezza e di sfiducia**

Figura 4. Principali rischi alla democrazia.

Fonte: elaborazione TEHA Group su dati Eurobarometro e fonti varie, 2024.

2.1.3 LE MINACCE COGNITIVE

La disinformazione rappresenta una sfida crescente: le informazioni false e fuorvianti, sia online che offline, sono percepite dai cittadini europei come il principale rischio per la democrazia, seguite dalla crescente sfiducia nelle istituzioni democratiche e dalla mancanza di impegno e interesse per la politica.

Tra le minacce cognitive più rilevanti vi sono i **deepfake e i contenuti generati con l'utilizzo dell'Intelligenza Artificiale**. Questi strumenti permettono di diffondere informazioni distorte, influenzando l'opinione pubblica attraverso la riproduzione di voci e immagini di personaggi pubblici e familiari. Ad esempio, un falso documentario Netflix con un deepfake di Tom Cruise è stato progettato per screditare il Comitato Olimpico Internazionale in vista delle Olimpiadi di Parigi 2024, ed è stato diffuso dalla propaganda russa sui media nazionali. Similmente, è stato utilizzato un robocall con un deepfake di Joe Biden per esortare gli elettori a non partecipare alle primarie del New Hampshire del 2024, suggerendo di riservare il voto per le elezioni di novembre 2024. In un altro caso, una registrazione audio diffusa online pochi giorni prima delle elezioni generali in Slovacchia del 2023, creata con l'Intelligenza Artificiale, presentava Michal Simecka, leader del partito progressista, mentre discuteva dell'acquisto di voti. Inoltre, a marzo 2024 la seconda TV russa ha trasmesso un video in cui Oleksiy Danilov, segretario del Consiglio di Sicurezza dell'Ucraina, ammetteva il coinvolgimento di Kiev nell'attacco terroristico al Crocus City Hall; questo video, creato con l'intelligenza artificiale, è stato ampiamente condiviso sui social[42].

Un'altra minaccia cognitiva significativa è la **manipolazione dei social media**, che comporta l'utilizzo di account sui social network per amplificare notizie su argomenti divisivi come l'immigrazione o le guerre. Questa strategia mira a sfruttare le tensioni sociali esistenti per seminare discordia.

Inoltre, **l'influenza sulle elezioni** costituisce un'ulteriore grave minaccia cognitiva. Le tecniche di disinformazione sono spesso concentrate sullo screditare le istituzioni democratiche, creando narrazioni che collegano questioni politiche locali a situazioni internazionali come guerre, economia e alleanze.

L'**obiettivo comune** di queste minacce cognitive è **interferire nelle dinamiche politiche e nei processi decisionali, alterando la percezione della realtà e fomentando un clima di incertezza e sfiducia**.

42 Fonte: TEHA Group su fonti varie, 2024.

Il mutato contesto socio-demografico, il cambiamento climatico e la globalizzazione hanno contribuito ad aumentare la diffusione delle malattie infettive. La resistenza antimicrobica (AMR), tuttavia, continua a rappresentare una delle principali minacce per la salute pubblica a livello globale. In questo contesto, diventa cruciale implementare efficacemente le misure di contrasto all'AMR in un'ottica «One Health»

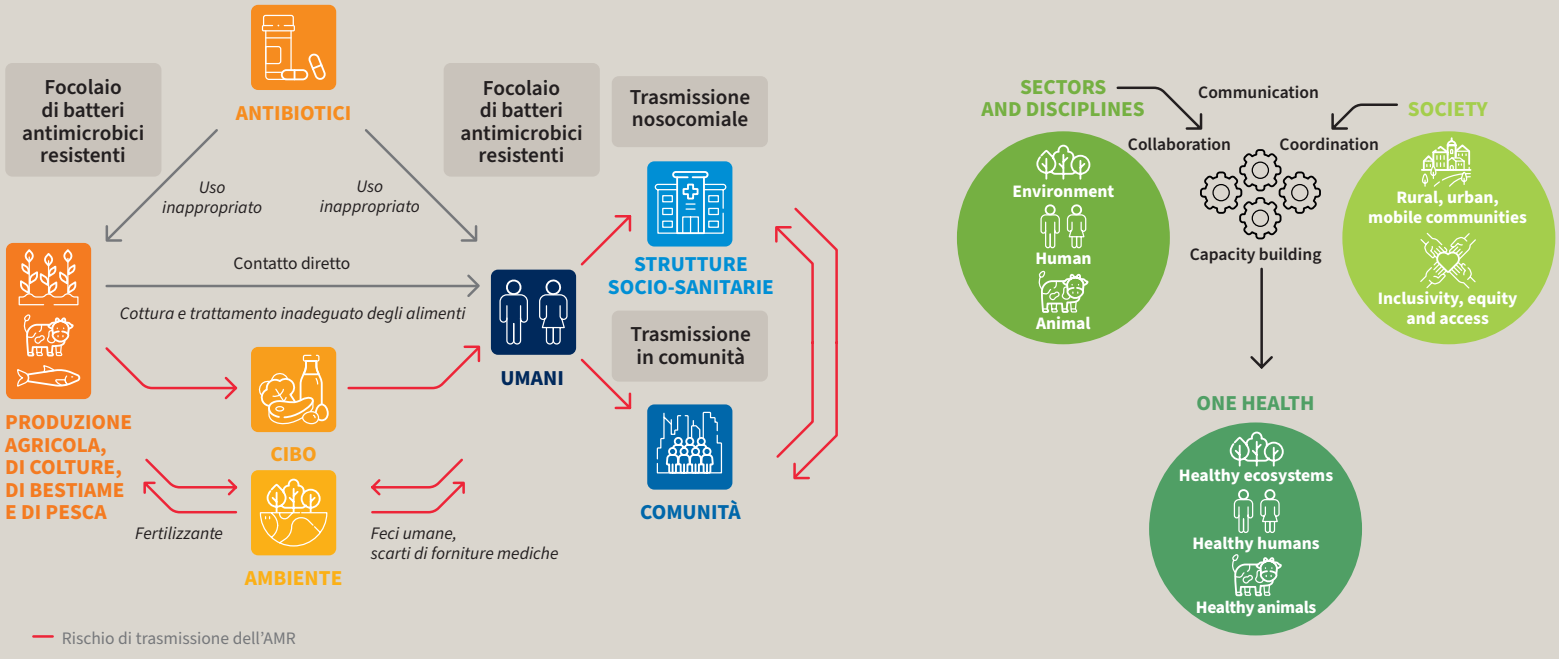


Figura 5. Focolai di batteri resistenti agli antimicrobici e vie di trasmissione (immagine di sinistra) e approccio "One Health" (immagine di destra).

Fonte: elaborazione TEHA Group su dati *OMS, FAO, WOAH e UNEP*, 2024.

2.1.4 LE MINACCE DI GLOBAL HEALTH

L'intensificazione degli scambi e degli spostamenti, i cambiamenti nella destinazione del suolo, l'espansione e l'intensificazione dell'agricoltura e degli allevamenti come conseguenza dello sviluppo socio-economico e demografico, l'urbanizzazione incontrollata e, soprattutto, il cambiamento climatico hanno contribuito ad aumentare la diffusione delle malattie infettive.

In questo senso, estati umide e inverni miti, hanno favorito la proliferazione delle zanzare e la diffusione di malattie endemiche dei Paesi caldi, come la Dengue, la cui incidenza globale è decuplicata negli ultimi 20 anni; l'aumento delle temperature ha facilitato anche la diffusione delle malattie infettive trasmesse dai pappataci e dalle zecche. Infatti, l'incidenza globale delle malattie trasmesse da zecche è raddoppiata in 12 anni[43].

Più della metà delle malattie infettive conosciute e circa il 75% delle nuove infezioni che hanno colpito l'uomo negli ultimi 10 anni, come la SARS, il COVID-19 o l'influenza Suina, **hanno origine zoonotica**[44].

Il quadro è reso ancor più complesso dall'**aumento della resistenza antimicrobica** (*antimicrobial resistance*, AMR), una pandemia silenziosa da oltre **1,3 milioni di decessi a livello globale**, che, senza adeguati interventi, si stima raggiungeranno i **10 milioni nel 2050**[45].

Pur essendo determinata dalla selezione naturale e dalla mutazione genetica, il consumo inappropriato di antibiotici nell'uomo, negli animali e nelle piante, oltre a condizioni igieniche e misure di controllo delle infezioni inadeguate, inquinamento, cambiamenti climatici e biodiversità, possono accelerare il rischio di sviluppare e diffondere le resistenze. L'insieme di questi fenomeni riduce la durata di vita utile degli antibiotici oggi in commercio: per gli antibiotici introdotti dagli anni '30 agli anni '50, il tempo medio di resistenza è stato di circa 11 anni, mentre per gli antibiotici lanciati dagli anni '70 agli anni 2000, il **tempo medio di resistenza è sceso a 2-3 anni**[46].

In questo contesto, emerge la **necessità di implementare efficacemente le misure di contrasto all'AMR in un'ottica «One Health»**, introducendo programmi e piani di azione per migliorare la collaborazione, la comunicazione, il coordinamento e lo sviluppo delle capacità per proteggere e accrescere la salute umana, animale e dell'ambiente[47].

43 Fonte: TEHA Group su "Polymicrobial nature of tick-borne diseases", Sanchez-Vicente S, Tagliafierro T, Coleman JL et al (2019), 2024.
44 Fonte: TEHA Group su dati United Nations Environment Programme, 2024.
45 Fonte: Ibid.
46 Fonte: TEHA Group su dati OCSE, 2024.
47 Fonte: TEHA Group su dati OMS, FAO, WOAH E UNEP, 2024.

CONSAPEVOLEZZA 3

Emerge la necessità di un approccio alla difesa di total security che coordini gli strumenti di influenza sia militare che politico-economica

2.2 La necessità di un approccio alla difesa di Total Security

La terza consapevolezza riguarda la necessità di adottare un **approccio alla difesa in chiave di total security**. A fronte di minacce ibride, per loro natura complesse, multidimensionali e imprevedibili, serve un approccio olistico a protezione degli interessi europei, agendo su più strumenti di influenza in maniera coordinata. Le sfide attuali, infatti, impongono una concezione più ampia della sicurezza nazionale, capace di favorire il coordinamento tra politica interna ed estera, e tra sicurezza tradizionale, economica, sanitaria e ambientale.

In tal senso, diversi paesi occidentali hanno riformato la governance nazionale in materia di sicurezza al fine di facilitare un maggiore coordinamento tra i diversi strumenti di difesa. Tra questi, vi sono gli Stati Uniti, il Regno Unito, la Francia e la Svezia.

L'adozione di un approccio alla difesa in chiave di total security a livello comunitario passa dalla consapevolezza, insita in ciascun cittadino europeo, che la difesa degli interessi comuni sia parte integrante del processo di integrazione europeo. Non è più sufficiente, infatti, guardare alla protezione dei soli interessi nazionali in un contesto globale così mutato.

Per far fronte alle minacce ibride, per loro natura complesse, multidimensionali e imprevedibili, è necessario rispondere con un approccio di sistema, mettendo in campo tutti gli strumenti di cui dispone un paese per tutelare la propria integrità territoriale, sociale ed economica

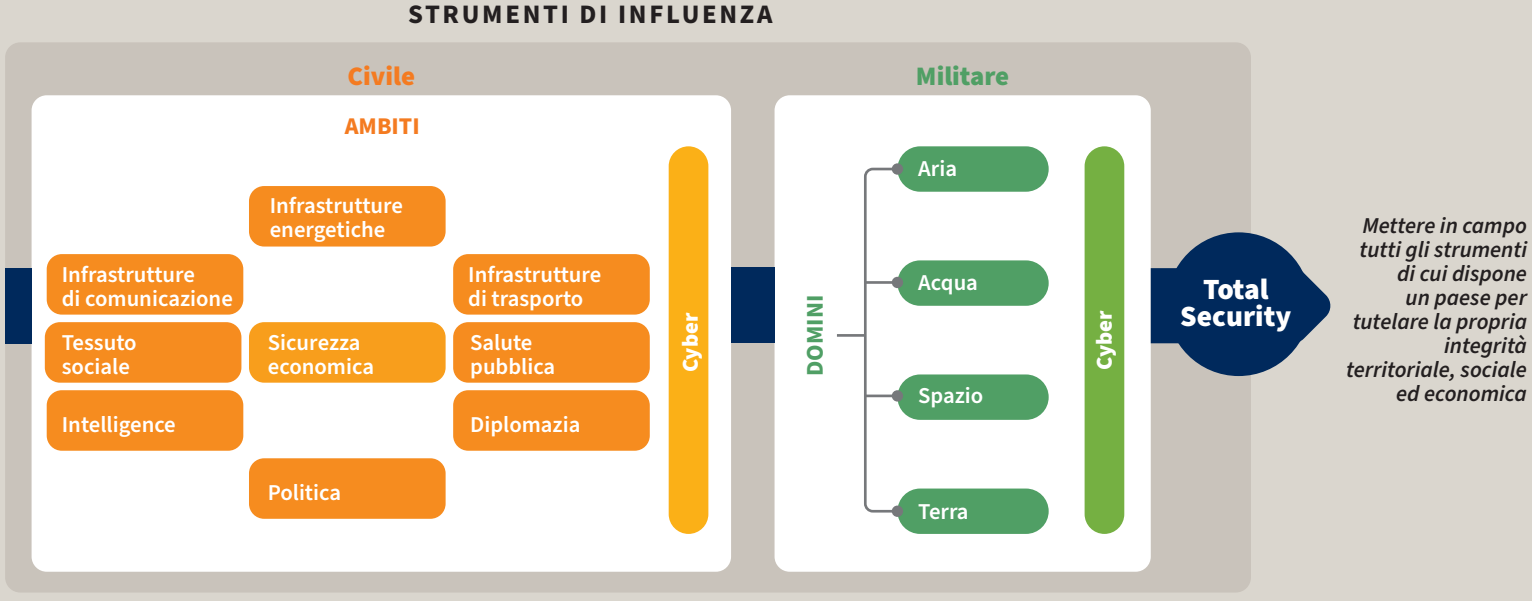


Figura 6. Approccio di "Total Security".

Fonte: elaborazione TEHA Group, 2024.

Le sfide odierne richiedono una comprensione più ampia della sicurezza nazionale, che faciliti il coordinamento tra politica interna ed estera, e tra sicurezza nazionale tradizionale, economica, sanitaria e ambientale. **Il National Security Council (NSC) degli Stati Uniti riflette questa realtà**. Istituito sotto il presidente Truman, il NSC consiglia e assiste il Presidente e coordina le questioni di sicurezza nazionale tra le agenzie governative.

Il NSC è presieduto dal Presidente e riunisce il Vicepresidente, il Segretario di Stato, il Segretario del Tesoro, il Segretario della Difesa, il Segretario dell'Energia, il Procuratore Generale, il Segretario della Sicurezza Interna, il Rappresentante presso le Nazioni Unite, l'Amministratore dell'Agenzia per lo Sviluppo Internazionale, il Capo di Gabinetto del Presidente e l'Assistente per gli Affari di Sicurezza Nazionale. Il Presidente del Joint Chiefs of Staff è il consigliere militare del Consiglio, mentre il Direttore dell'Intelligence Nazionale è il consigliere per l'intelligence. Altri partecipanti aggiuntivi, come il Coordinatore per la Risposta al COVID-19 e l'Inviato Speciale per il Clima, sono invitati a partecipare alle riunioni quando necessario, per affrontare la natura trasversale di molte questioni critiche di sicurezza nazionale.

Il NSC degli Stati Uniti ha avuto un **ruolo centrale nella tutela dell'industria nazionale dei semiconduttori**. Tra le azioni intraprese vi sono la restrizione alle importazioni di device Huawei nel 2019 per timori di spionaggio e per rallentare lo sviluppo tecnologico cinese e le restrizioni alle esportazioni di prodotti elettronici verso la Cina nel 2022 per rallentare lo sviluppo di tecnologie avanzate. Inoltre, un effetto della politica di sicurezza nazionale sono i dazi introdotti su specifiche tecnologie, con l'obiettivo di tutelare filiere industriali critiche per la difesa[48].

Altri paesi occidentali hanno riformato la governance della sicurezza per facilitare un maggiore coordinamento. Nel 2010, il **Regno Unito** ha istituito il National Security Council, presieduto dal Primo Ministro, che coordina la politica di sicurezza nazionale e prende decisioni strategiche su sicurezza, politica estera, difesa, commercio, relazioni internazionali, sviluppo, resilienza e sicurezza delle risorse. In **Francia**, il Conseil de Défense et de Sécurité Nationale, istituito nel 2009 e presieduto dal Presidente della Repubblica, definisce le linee guida per programmazione militare, deterrenza, operazioni esterne, intelligence, sicurezza economica ed energetica, sicurezza interna e lotta al terrorismo. In **Svezia**, il National Security Council, istituito nel 2022, discute le questioni di sicurezza nazionale e organizza la cooperazione tra i dipartimenti di giustizia, esteri, difesa ed economia. Tutti questi organi operano principalmente con membri governativi; tuttavia, recenti riforme prevedono che esperti esterni possano essere invitati a partecipare per facilitare la collaborazione tra governo e settore privato su questioni di sicurezza nazionale, come infrastrutture critiche, sicurezza finanziaria, cybersecurity o resilienza energetica[49].

48 Fonte: TEHA Group su dati White House, 2024.
49 Fonte: TEHA Group su fonti varie, 2024.

La centralità delle tecnologie digitali per la competitività internazionale e la difesa

CAPITOLO 3

Nel corso del terzo capitolo verrà illustrato come la leadership nelle tecnologie digitali avanzate stia diventando sempre più cruciale per il posizionamento geopolitico e come l'Europa si trovi in secondo piano rispetto alle grandi potenze.

L'accesso alle tecnologie digitali, infatti, rappresenta una leva geopolitica fondamentale per gli Stati, influenzando le dinamiche di potere globali. A tale riguardo, verranno esaminati gli ambiti civili di influenza delle tecnologie digitali e come quest'ultime siano essenziali per garantire la ricerca e la supremazia militare.

Inoltre, verrà evidenziato come lo sviluppo delle tecnologie digitali per la difesa richieda un nuovo modello di collaborazione con il settore privato. Lo sviluppo tecnologico è sempre più supportato dell'impulso dato dalle aziende digitali in ambito civile, caratterizzate da maggiori capacità di investimento rispetto a quelle della difesa; questo rende necessario confrontarsi con il settore privato per presidiare il progresso tecnologico. Nel corso del capitolo, saranno presentati diversi aspetti che sostanziano come sia prioritaria tale collaborazione.

CONSAPEVOLEZZA 4

La leadership nelle tecnologie digitali avanzate è un **elemento sempre più centrale per il posizionamento geopolitico**. In questo, l'Europa risulta più debole rispetto alle altre grandi potenze mondiali

3.1 L’importanza della leadership nelle tecnologie digitali

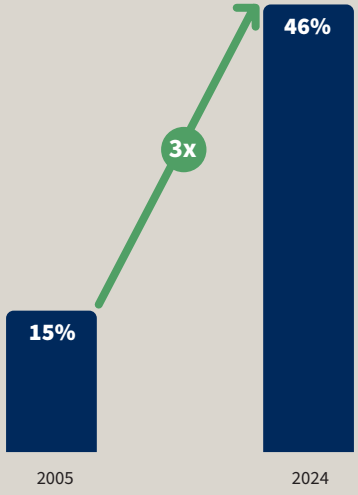
La quarta consapevolezza riguarda l’importanza della leadership nelle tecnologie digitali. Questo aspetto è diventato sempre più centrale per il posizionamento geopolitico. La leadership nelle tecnologie digitali avanzate, infatti, permette di esercitare un’influenza significativa in ambiti civili, come il controllo delle infrastrutture ICT per l’accesso ai dati e alle comunicazioni, oltre a sostenere la ricerca e il mantenimento della superiorità militare. Nelle piattaforme di difesa, in particolare, la componente tecnologica (elettronica) assume un ruolo sempre più rilevante, con il digitale che è fondamentale per connettere i cinque domini della difesa (Terra, Acqua, Aria, Spazio e Cyber) e garantire la cybersecurity.

Tuttavia, in questo scenario, l’Europa si trova in una posizione subordinata rispetto alle grandi potenze mondiali. Negli ultimi dieci anni, la sua quota di mercato nelle tecnologie digitali si è dimezzata e, nel 2021, il valore aggiunto totale del settore ICT dell’UE rappresentava solo il 4,9% del PIL totale, a fronte del 9,8% negli Stati Uniti[50].

50 Fonte: TEHA Group su dati Commissione Europea, 2024.

Le aziende tecnologiche sono una delle componenti più importanti dell'economia, ma l'Europa ha visto una contrazione della propria quota di mercato nell'ultimo decennio

Peso delle aziende tecnologiche nel Fortune 500* tra le prime 100 per capitalizzazione di mercato (% di capitalizzazione), 2005-2024



Quota UE nel mercato ICT globale
(%), 2013-2022

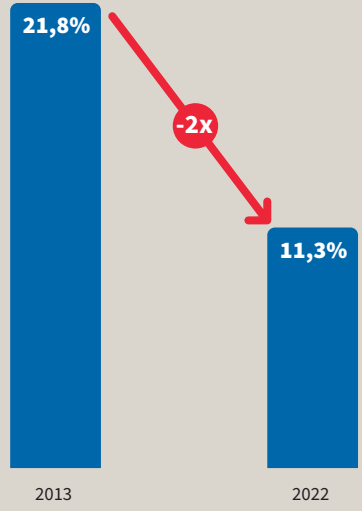


Figura 1. Peso delle aziende tecnologiche nel Fortune 500 tra le prime 100 per capitalizzazione di mercato (grafico di sinistra, % di capitalizzazione), 2005-2024 e Quota UE nel mercato ICT globale (grafico di destra, %), 2013-2022.

(*) Le aziende della classifica Fortune 500 sono classificate in base al fatturato totale dei rispettivi anni fiscali. Sono incluse nell'indagine le società costituite negli Stati Uniti, che operano negli Stati Uniti e che depositano i bilanci presso un'agenzia governativa.

Fonte: elaborazione TEHA Group su dati Fortune 500 e Commissione Europea, 2024.

L'ascesa delle aziende tecnologiche nell'economia globale è ormai inarrestabile, con aziende come Alphabet, Amazon, Apple, Meta, Microsoft e Nvidia che hanno raggiunto in pochi anni le prime posizioni nella classifica Fortune 500[51]. Queste aziende hanno mostrato una notevole capacità di adattamento, innovazione ed espansione globale, consolidando la loro presenza tra le prime aziende per fatturato. Questa evoluzione riflette non solo il loro successo economico, ma anche l'influenza crescente nel panorama economico globale.

Parallelamente, **il peso delle aziende tecnologiche nel Fortune 500 è cresciuto in modo esponenziale**. Dal 2005 al 2024, la percentuale di capitalizzazione di mercato delle aziende tecnologiche del Fortune 500 tra le prime 100 aziende per capitalizzazione è triplicata, passando **dal 15% al 46%**[52].

Tuttavia, mentre le aziende tecnologiche statunitensi hanno visto una crescita robusta, **la quota di mercato europea nelle tecnologie digitali è diminuita significativamente negli ultimi dieci anni**. Nel 2013, l'Unione Europea deteneva una quota del 21,8% nel mercato ICT globale. Questo valore si è dimezzato nel 2022, raggiungedo l'11,3%, evidenziando una perdita di competitività rispetto ad altre regioni del mondo[53].

Nel 2021, inoltre, il **valore aggiunto totale del settore ICT dell'UE** rappresentava il **4,9% del PIL totale** (604 miliardi di euro), **contro il 9,8% negli Stati Uniti** (2.300 miliardi di euro)[54].

Per l'Europa, si aggiunge anche il problema della scarsa propensione agli investimenti in innovazione, con una spesa interna lorda per Ricerca e Sviluppo pari al 2,11% del PIL, -1,48 punti percentuali rispetto a quella degli Stati Uniti[55].

51 Le aziende della classifica Fortune 500 sono classificate in base al fatturato totale dei rispettivi anni fiscali. Sono incluse nell'indagine le società costituite negli Stati Uniti, che operano negli Stati Uniti e che depositano i bilanci presso un'agenzia governativa. Alphabet è passata dalla 241esima posizione nel 2007 all'ottava nel 2023, Amazon è passata dalla 482esima posizione nel 2002 alla seconda nel 2023, Apple dalla 113esima posizione nel 1996 alla quarta nel 2023, Meta dalla 462esima posizione nel 2013 alla 31esima nel 2023, Microsoft dalla 215esima posizione nel 1996 alla tredicesima nel 2023 e Nvidia dalla 306esima posizione nel 2018 alla 152esima nel 2023.

52 Fonte: TEHA Group su dati Fortune 500 e mercati azionari globali, 2024.

53 Fonte: TEHA Group su dati Commissione Europea, 2024.

54 Fonte: Ibid.

55 Ultimi dati disponibili (2022). Fonte: TEHA Group su dati OECD, 2024.

L’accesso alle tecnologie digitali rappresenta una leva geopolitica, influenzando le dinamiche di potere globale

1 Controllo sulle Infrastrutture delle tecnologie dell’informazione e della comunicazione	*Esempio:* una crescente percentuale (oltre il 60%) di cavi sottomarini, essenziali per il funzionamento dei settori digitali con il trasporto di quasi il 99% dei dati intercontinentali, è di proprietà di aziende private
2 Consolidamento di alleanze politiche attraverso l’esportazione di tecnologie digitali	*Esempio:* aziende cinesi, tra cui Huawei, Hikvision, Dahua e ZTE, forniscono tecnologia di sorveglianza IA in più di 63 paesi con crescenti preoccupazioni riguardanti la privacy e i diritti umani
3 Definizione di standard tecnologici internazionali	*Esempio:* la competizione tra USA e Cina per il controllo degli standard del 5G è sempre più forte: Huawei partecipa attivamente al processo di definizione degli standard, fornendo proposte tecniche e registrando Standard Essential Patent (SEP)
4 Manipolazione delle informazioni e persuasione dell’opinione pubblica	*Esempio:* diffusione di un «robocall» con deepfake di Joe Biden in cui chiede ai propri elettori di non partecipare alle primarie del New Hampshire del 2024
5 Accordi tecnologici bilaterali/multilaterali	*Esempio:* la Digital Silk Road (DSR) è la dimensione tecnologica della Belt and Road Initiative e prevede investimenti in infrastrutture digitali nei paesi partecipanti, per esempio il Pakistan East Asia Africa Cable Express lungo oltre 15.000 Km
6 Restrizioni all’esportazione e controllo sulle supply chain delle tecnologie digitali	*Esempio:* a partire da maggio 2024, l'amministrazione Biden ha revocato le licenze di esportazione che permettevano a produttori di semiconduttori statunitensi di fornire chip essenziali a Huawei

Figura 2. Gli ambiti civili di influenza delle tecnologie digitali.

Fonte: elaborazione TEHA Group su fonti varie, 2024.

L'accesso alle tecnologie digitali rappresenta anche una leva geopolitica per gli stati, alla luce della loro influenza in vari ambiti della società civile.

Il controllo delle Infrastrutture ICT, ad esempio, **può influenzare l'accesso globale ai dati e alle comunicazioni**. Una crescente percentuale di cavi sottomarini (oltre il 60%), essenziali per il funzionamento dei settori digitali con il trasporto di quasi il 99% dei dati intercontinentali, è oggi di proprietà di aziende private, incluse grandi multinazionali tecnologiche come Google, Meta, Amazon e Huawei, con l'obiettivo di soddisfare le crescenti esigenze di trasporto di crescenti quantità di dati in modo sempre più veloce. Le aziende che possiedono e gestiscono i cavi sottomarini, in particolare, sono in grado di supportare politiche geoeconomiche dei governi del Paese di appartenenza, grazie al potere negoziale che possono esercitare nei confronti dei Paesi che ospitano le infrastrutture. Inoltre, gli stati possono utilizzare la prominenza nel mercato dei cavi sottomarini per influenzare il flusso delle comunicazioni globali, monitorando e potenzialmente interrompendo il traffico internet, con potenziali danni per cittadini e imprese[56]. Analogamente, anche il controllo delle infrastrutture spaziali può influenzare l'accesso ai dati e alle comunicazioni, rappresentando un ulteriore strumento di influenza geopolitica.

L'esportazione di tecnologie digitali, inoltre, **consente ai paesi di estendere la loro influenza oltre i confini nazionali e di consolidare alleanze politiche**. Le aziende cinesi, tra cui Huawei, Hikvision, Dahua e ZTE, ad esempio, forniscono tecnologia di sorveglianza di intelligenza artificiale in più di 63 paesi, oltre 35 dei quali hanno aderito alla Belt and Road Initiative (BRI). Sebbene la Cina non sia l'unico Paese a fornire tecnologie di sorveglianza avanzate, le proposte di prodotti cinesi sono spesso accompagnate da prestiti agevolati per incoraggiare i governi ad acquistarne apparecchiature. Queste tattiche sono particolarmente diffuse in paesi come Kenya, Laos, Mongolia, Uganda e Uzbekistan, che altrimenti non potrebbero accedere a questa tecnologia. L'esportazione di tecnologie digitali, soprattutto verso regimi autoritari o paesi in via di sviluppo, crea dipendenze tecnologiche che possono facilmente tradursi in influenze politiche e geopolitiche. La crescente sofisticazione e diffusione dell'intelligenza artificiale e delle tecnologie di sorveglianza digitale, tuttavia, ha sollevato significative preoccupazioni riguardanti la privacy e i diritti umani.

56 Fonte: TEHA Group su dati TeleGeography e report «Submarine Cables and the Risks to Digital Sovereignty", 2024.

Anche **la dominanza nella definizione degli standard tecnologici internazionali consente ai paesi di influenzare l'infrastruttura digitale globale e creare dipendenze**. Il processo di definizione degli standard tecnologici è una componente essenziale della competizione tecnologica globale. Un esempio di questa dinamica è la competizione tra Stati Uniti e Cina per il controllo degli standard del 5G. Gli Stati Uniti hanno storicamente guidato la definizione degli standard tecnologici internazionali, contribuendo a stabilire protocolli fondamentali come TCP/IP, che sono alla base del funzionamento di Internet. Negli ultimi due decenni, però, la Cina ha aumentato significativamente la sua partecipazione nelle organizzazioni internazionali di standardizzazione, soprattutto nell'ambito del 5G, e la sua burocrazia si è concentrata sempre di più sugli standard tecnici. Huawei ha partecipato attivamente al processo di definizione degli standard 5G, fornendo proposte tecniche al 3rd Generation Partnership Project (3GPP)[57] e registrando molti Standard Essential Patent (SEP), brevetti che proteggono un'invenzione essenziale per l'implementazione di specifici standard tecnologici. In questo contesto, la definizione di questi standard risulta cruciale per stabilire una posizione di vantaggio economico e geopolitico. I paesi che adottano gli standard di una nazione, infatti, possono essere inclini a seguirne le linee politiche e diplomatiche[58].

Le tecnologie digitali, inoltre, **possono essere utilizzate dagli stati anche per influenzare l'opinione pubblica globale attraverso campagne di disinformazione**. Un esempio di questo fenomeno è la diffusione di un "robocall" con deepfake di Joe Biden nel New Hampshire a gennaio 2024, in cui si chiede agli elettori di non partecipare alle primarie del Partito Democratico e di conservare, erroneamente, il voto per le elezioni di novembre. Queste tecniche possono distorcere i processi democratici e minare la fiducia nel sistema elettorale.

Allo stesso tempo, **gli accordi tecnologici bilaterali e multilaterali per le tecnologie digitali permettono ai paesi di creare alleanze strategiche e dipendenze tecnologiche con altri stati.** Gli accordi tecnologici, infatti, permettono di condividere risorse, conoscenze e competenze, consentendo ai paesi coinvolti di raggiungere livelli più elevati di sviluppo economico e tecnologico, ma possono anche generare significative dipendenze tecnologiche. La Digital Silk Road (DSR) della Cina, la dimensione tecnologica della Belt and Road Initiative che prevede investimenti in infrastrutture digitali nei paesi partecipanti, rappresenta un esempio emblematico di come gli accordi tecnologici possano essere utilizzati per estendere l'influenza di una nazione su scala globale. Tra i progetti più significativi della DSR vi è il cavo sottomarino Pakistan East Asia Africa Cable Express (PEACE). Lungo oltre 15.000Km, il PEACE è stato progettato per facilitare la trasmissione di dati tra Asia, Europa e Africa[59]. Investendo in infrastrutture critiche nei paesi partecipanti, la Cina crea una dipendenza tecnologica, stabilisce standard tecnologici cinesi e rafforza i legami economici e politici con queste nazioni.

57 3GPP (3rd Generation Partnership Project) è un'organizzazione collaborativa che sviluppa protocolli per le comunicazioni mobili, inclusi gli standard per le tecnologie 3G, 4G e 5G.

58 Fonte: TEHA Group su dati LexisNexis, 2024.

59 Fonte: TEHA Group su dati PeaceCable, 2024.

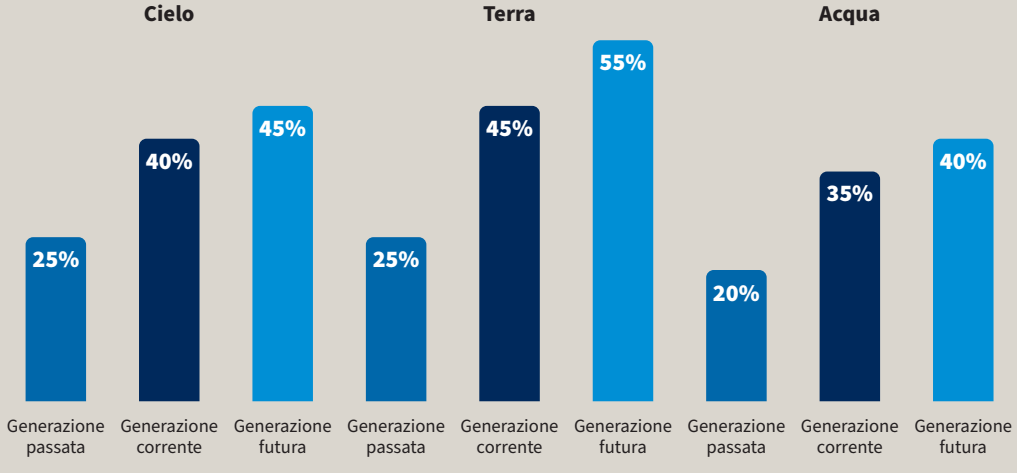
Imponendo restrizioni alle esportazioni di tecnologie avanzate, infine, **si può ostacolare la capacità di altri Paesi di sviluppare tecnologie all'avanguardia in settori strategici**. A partire da maggio 2024, ad esempio, l'amministrazione Biden ha revocato le licenze di esportazione che permettevano ai produttori di semiconduttori statunitensi di fornire chip avanzati a Huawei. Già in passato gli Stati Uniti avevano imposto restrizioni alle esportazioni di semiconduttori USA verso Huawei. A maggio del 2019, il Bureau of Industry and Security (BIS) del Dipartimento del Commercio USA ha aggiunto Huawei e molte delle sue affiliate non statunitensi alla Entity List[60]. A maggio 2020, il BIS ha ulteriormente esteso le restrizioni, impedendo a Huawei di acquistare semiconduttori prodotti con software e tecnologia statunitensi, anche se fabbricati all'estero. Ad agosto 2020 sono state aggiunte altre 38 affiliate di Huawei alla "Entity List", espandendo ulteriormente le restrizioni. Ad ottobre 2022, il BIS ha implementato nuovi controlli sulle esportazioni di articoli per il calcolo avanzato e la produzione di semiconduttori verso la Repubblica Popolare Cinese. Le restrizioni sui chip hanno influenzato in modo significativo l'ecosistema cinese dei semiconduttori, limitando l'accesso alle apparecchiature essenziali per la produzione di tecnologie di ultima generazione[61].

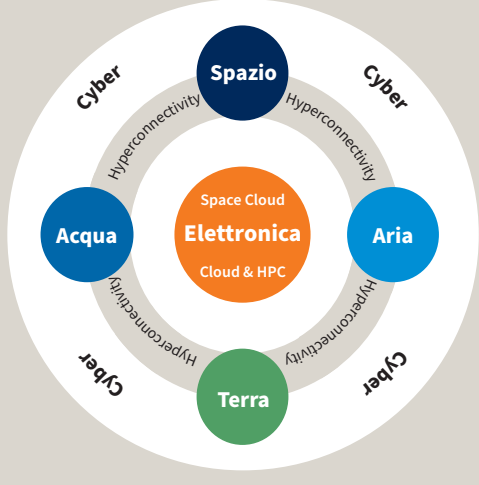
60 La Entity List contiene i nomi di individui, organizzazioni e aziende a cui vengono imposte restrizioni specifiche riguardo all'acquisto di beni, software e tecnologie statunitensi. Le entità incluse in questa lista sono ritenute coinvolte in attività contrarie agli interessi di sicurezza nazionale o di politica estera degli Stati Uniti.

61 Fonte: TEHA Group su fonti varie, 2024.

Nelle piattaforme di difesa, la componente tecnologica (elettronica) ricopre un valore sempre maggiore, con una crescita esponenziale della complessità. Il digitale, inoltre, svolge un ruolo centrale nel mettere in comunicazione tutti i cinque domini della difesa e nell'assicurare la cybersecurity

Evoluzione del valore della componente elettronica all'interno delle piattaforme di difesa nei tre domini
(valori % sul totale), generazione passata, generazione corrente, generazione futura





Digital Continuum per la Difesa
Ricevere il maggior numero di **dati**, trasformarli in **informazioni** per prendere **decisioni corrette** nel più breve tempo possibile

Figura 3. Evoluzione del valore della componente elettronica all'interno delle piattaforme di difesa nei tre domini (grafico a sinistra, valori % sul totale), generazione passata, corrente e futura e Rappresentazione del Digital Continuum per la Difesa (grafico di destra).

Fonte: elaborazione TEHA Group su dati Leonardo, 2024.

L'accesso alle tecnologie digitali consente di influenzare significativamente anche la ricerca e il mantenimento della superiorità militare, incidendo sulle dinamiche di potere globale.

Nelle piattaforme di difesa, la componente tecnologica (elettronica) ha acquisito un ruolo sempre più centrale. Nel dominio aereo, la componente elettronica è passata dal 25% nelle piattaforme della generazione passata, al 40% in quelle della generazione corrente, con un aumento previsto al 45% nelle piattaforme della generazione futura. Nel dominio terrestre, la percentuale di componente elettronica è cresciuta dal 25% nelle piattaforme di generazione passata al 45% in quelle di generazione corrente, raggiungendo il 55% nella generazione futura. Per quanto riguarda il dominio marittimo, la componente elettronica è aumentata dal 20% nella generazione passata al 35% nella generazione corrente, e si prevede che raggiungerà il 40% nella generazione futura[62].

Allo stesso tempo, **vi è stata una crescita esponenziale della complessità digitale nelle nuove piattaforme tecnologiche di difesa**. L'F-16 (1974) utilizzava un numero relativamente basso di linee di codice, che si stimano essere pari a 150.000. Con l'introduzione dell'F-22 (1990), questo numero è aumentato a circa 2 milioni e l'F-35-I (2011) ha ulteriormente incrementato le linee di codice a circa 4,5 milioni. Questa tendenza è proseguita con l'F-35-II (2019) che ha raggiunto circa 8 milioni di linee di codice e con l'F-35-III (2025) che ne prevede circa 24 milioni. Il Next Generation Air Dominance (2030s), infine, rappresenta un salto significativo con circa 85 milioni di linee di codice, rendendolo una piattaforma estremamente sofisticata con capacità avanzate di intelligenza artificiale e gestione autonoma[63].

Il digitale, inoltre, **svolge un ruolo centrale** nel mettere in comunicazione tutti i cinque domini della difesa (Terra, Acqua, Aria, Spazio, Cyber) e **nell'assicurare** la cybersecurity e **il Digital Continuum**. Il Digital Continuum rappresenta un'infrastruttura integrata e continua che consente la raccolta, l'elaborazione e l'analisi dei dati provenienti da diverse fonti in tempo reale. Questo sistema è fondamentale per garantire una risposta rapida e informata in situazioni critiche, migliorando la capacità decisionale attraverso l'uso di tecnologie avanzate come l'intelligenza artificiale e l'apprendimento automatico. Inoltre, facilita la collaborazione tra i vari domini della difesa, permettendo una condivisione sicura e tempestiva delle informazioni. Questo approccio integrato non solo rafforza la cybersecurity, ma assicura anche che le operazioni siano coordinate e efficienti, riducendo i tempi di reazione e aumentando l'efficacia complessiva delle missioni.

62 Fonte: TEHA Group su dati Leonardo, 2024.

63 Il numero di linee di codice è stimato sulla base delle informazioni pubbliche analizzate. Fonte: TEHA Group su dati Aerospace Vehicle Systems Institute e DoD, 2024.

CONSAPEVOLEZZA 5

Lo sviluppo delle tecnologie digitali per la difesa richiede un **nuovo modello di collaborazione con il settore privato**

3.2 Il nuovo paradigma della difesa

L'evoluzione delle minacce a cui assistiamo richiede un nuovo paradigma della difesa che presidi costantemente cinque ambiti tecnologici:

- ***AI, Big Data, e Digital Twin***: permettono di **analizzare grandi quantità di dati e prevedere potenziali minacce**. Un Digital Twin di una rete, ad esempio, può simulare attacchi e identificare vulnerabilità prima che vengano sfruttate;
- ***Cloud Computing e HPC***: consentono di **scalare rapidamente le risorse di calcolo** necessarie per gestire grandi quantità di dati e rispondere alle minacce in modo flessibile;
- ***Connectivity***: garantisce la sicurezza dei dispositivi attraverso **protocolli di comunicazione sicuri** e aggiornamenti continui;
- ***Cybersecurity***: utilizza strumenti avanzati per **prevenire, rilevare e neutralizzare le minacce** prima che possano causare danni;
- ***Quantum Technologies***: impiegano la crittografia basata su principi quantistici per creare **comunicazioni sicure e ininterrompibili**, impossibili da decifrare con i metodi tradizionali.

In questo contesto, **lo sviluppo delle tecnologie digitali per la difesa richiede un nuovo modello di collaborazione con il settore privato.** Lo sviluppo delle tecnologie digitali, in particolare, proviene sempre più dal settore privato, dove le aziende hanno una capacità di investimento maggiore rispetto alle aziende della difesa. Di conseguenza, risulta prioritario confrontarsi con il settore privato per presidiare l'innovazione, attuare iniziative di collaborazione tra difesa e settori tecnologici, avviare programmi di attrazione di talenti nei comparti della difesa, affidare a personale civile ruoli chiave per lo sviluppo tecnologico e approfondire le crescenti considerazioni etiche sugli strumenti di difesa con tecnologie avanzate.

Lo sviluppo delle tecnologie digitali proviene sempre più dal settore privato, dove le aziende hanno una capacità di investimento maggiore rispetto alle aziende della difesa. Inoltre, vi sono aspetti che sostanziano come sia prioritario confrontarsi con il settore privato per presidiare l'innovazione

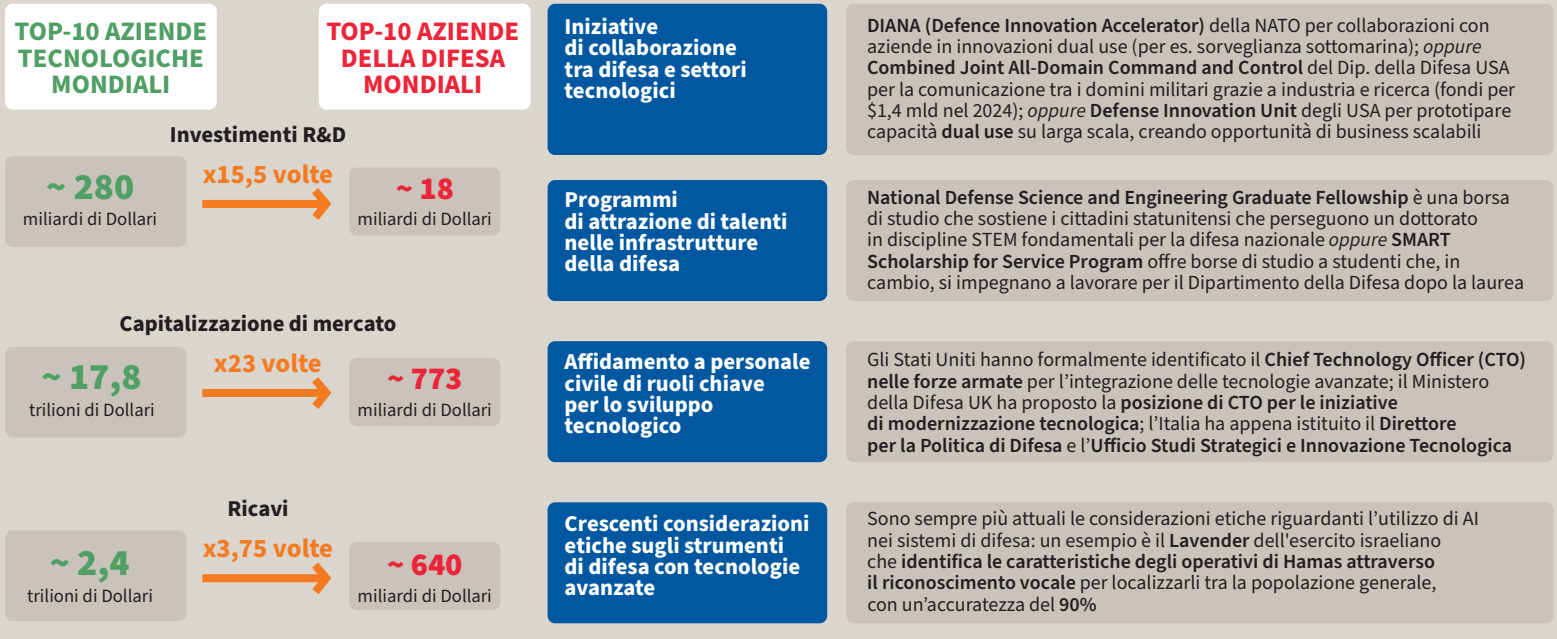


Figura 4. Confronto tra le prime 10 aziende tecnologiche e della difesa mondiali per investimenti in ricerca e sviluppo, capitalizzazione di mercato e ricavi (immagine a sinistra) e gli aspetti che sostanziano l'importanza di collaborare con il settore privato per sostenere l'innovazione (immagine a destra). N.B.: i dati relativi alle aziende cinesi potrebbero essere non del tutto veritieri.

Fonte: elaborazione TEHA Group su fonti aziendali, dati Defense news top 100 e mercati azionari globali, 2024.

Le aziende tecnologiche digitali possiedono una capacità di investimento significativamente maggiore rispetto alle aziende della difesa. Questa differenza è particolarmente evidente quando si confrontano gli investimenti in ricerca e sviluppo (R&D), la capitalizzazione di mercato e i ricavi tra le principali aziende tecnologiche e le principali aziende della difesa mondiali.

Le dieci maggiori aziende tecnologiche mondiali investono complessivamente circa 280 miliardi di dollari in **R&D**, una cifra **15,5 volte superiore** rispetto ai 18 miliardi di dollari[64] investiti dalle dieci maggiori aziende della difesa[65]. Questo divario si riflette anche nella **capitalizzazione** di mercato, con le prime dieci aziende tecnologiche che raggiungono complessivamente 17,8 trilioni di dollari, contro i 773 miliardi di dollari delle prime dieci aziende della difesa, un rapporto di **23 volte superiore**[66]. Anche i **ricavi** delle dieci maggiori aziende tecnologiche, pari a circa 2,4 trilioni di dollari, **superano di quasi 4 volte** quelli delle dieci maggiori aziende della difesa, che ammontano a circa 640 miliardi di dollari[67].

64 Fonte: TEHA Group su dati Janes, 2024.
65 Fonte: TEHA Group su fonti aziendali, 2024.
66 Fonte: TEHA Group su dati mercati azionari globali, 2024.
67 Fonte: TEHA Group su dati Defense news top 100 e fonti aziendali, 2024. N.B.: Ricavi totali, non generati solo dal settore difesa. I dati relativi alle aziende cinesi potrebbero non essere del tutto veritieri.

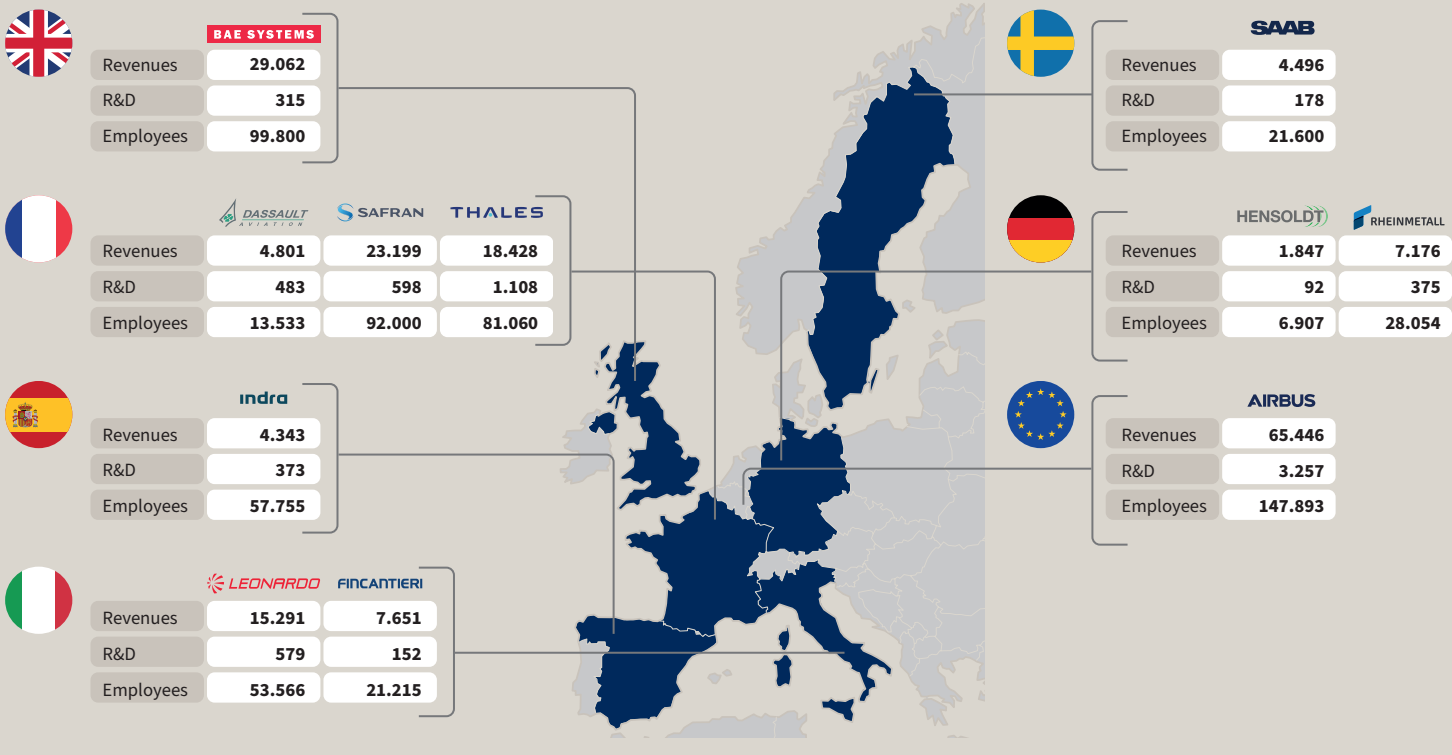


Figura 5. Rappresentazione delle maggiori aziende della difesa in Europa per ricavi complessivi, R&D e numero di occupati.
N.B. I valori dei ricavi sono relativi ai risultati complessivi dell'anno 2023, espressi in M€. I valori di R&D sono relativi alle spese di R&D autofinanziata, espressi in M€

Allo stesso tempo, le aziende tecnologiche possono contare su un mercato di riferimento (quello civile) di gran lunga maggiore rispetto a quello delle aziende di difesa; possono inoltre avvalersi di approcci di innovazione tipici dell'Open Innovation, che sono flessibili e rapidi, e di un più facile accesso al mercato dei capitali. Ottenere l'accreditamento come fornitore di tecnologie per la difesa può imporre significative restrizioni nell'azione di mercato e sulla capacità di raccogliere capitali, limitazioni che possono a volte scoraggiare le aziende dall'investire in questo settore a fronte delle maggiori opportunità del settore civile. In questo contesto, **lo sviluppo di nuove tecnologie digitali nasce sempre più spesso dai settori civili, rendendo necessario lo sviluppo di partnership tra la difesa e le aziende del digitale**.

Con l'obiettivo di presidiare l'innovazione, sono nate numerose **iniziative di collaborazione tra la difesa e le aziende tecnologiche**. Ad esempio, **DIANA (Defence Innovation Accelerator for the North Atlantic)** della NATO è un progetto che ha l'obiettivo di migliorare l'innovazione tecnologica dell'Alleanza promuovendo le tecnologie dual use (per esempio, sorveglianza sottomarina) attraverso la collaborazione con ricercatori, imprenditori e aziende. Il **Combined Joint All-Domain Command and Control** è un'iniziativa del Dipartimento della Difesa USA volta a migliorare la comunicazione e il coordinamento in tutti i domini militari. L'obiettivo è quello di integrare sensori, dati e capacità di comando in una rete unificata, fornendo ai comandanti capacità decisionali ed efficacia operativa superiori. Esso prevede collaborazioni tra Dipartimento della Difesa, industria, ricerca e le nazioni alleate; il budget per il 2024 è di $1,4 miliardi. La **Defence Innovation Unit**, invece, è l'unità del Dipartimento della Difesa degli Stati Uniti che collabora con il settore privato per prototipare e mettere in campo capacità dual use che risolvano le sfide operative delle missioni in modo rapido e su larga scala, creando anche opportunità di business scalabili per le aziende private.

Alla base del processo di introduzione di tecnologie digitali nella difesa, inoltre, vi sono lo **sviluppo delle competenze e l'attrazione dei talenti**. In tal senso, sono stati creati programmi di scholarship come il **National Defense Science and Engineering Graduate Fellowship**, una borsa di studio che sostiene i cittadini statunitensi che perseguono un dottorato in discipline scientifiche e ingegneristiche fondamentali per la difesa nazionale. Copre le tasse scolastiche, fornisce uno stipendio e include un'indennità di assicurazione sanitaria. Lo **SMART Scholarship for Service Program**, invece, è un programma che offre borse di studio a studenti universitari e laureati in settori STEM che, in cambio si impegnano a lavorare per il Dipartimento della Difesa dopo la laurea.

Israele è un esempio di paese all'avanguardia nell'integrare talenti nel settore militare, in particolare attraverso unità come la 8200 delle Israel Defence Forces (IDF). Questa unità di intelligence è un motore di innovazioni informatiche, composta principalmente da giovani che svolgono il servizio militare, appositamente selezionati. L'Unit 8200 è nota per la sua capacità di formare e sviluppare alcuni dei migliori talenti tecnologici al mondo. Molti membri di questa unità, dopo il servizio militare, hanno fondato startup di successo, contribuendo significativamente all'ecosistema tecnologico e imprenditoriale israeliano. Esempi includono Palo Alto Networks, azienda leader nella cybersecurity conosciuta per le sue soluzioni di firewall di nuova generazione, Waze, applicazione di navigazione e traffico

basata sulla comunità ed acquisita da Google nel 2013 per circa $1.3 miliardi, AIM Security, startup che offre una piattaforma di sicurezza basata sull'IA generativa per proteggere le aziende dalle minacce informatiche, e Gem Security, startup di sicurezza informatica acquisita da Wiz per $350 milioni. Ciò rappresenta un esempio efficace di come l'integrazione di talenti nel settore militare possa essere utilizzato come trampolino di lancio per il loro progresso professionale, attraverso un'istruzione avanzata e un'esperienza diretta. Israele, inoltre, promuove attivamente la collaborazione tra le forze armate, le università e le industrie tecnologiche per sviluppare soluzioni avanzate, colmando lacune operative e producendo alcuni dei sistemi d'arma più efficaci al mondo. Un esempio significativo di questo approccio è il modello Be'er Sheva. La città di Be'er Sheva ospita un ecosistema di innovazione tecnologica, incentrato su cybersecurity e tecnologia avanzata, grazie alla collaborazione tra università, grandi multinazionali, unità militari e governo. Questo modello di **cooperazione pubblico-privata ha reso Be'er Sheva un hub globale per la sicurezza informatica**, attirando investimenti internazionali e creando numerose opportunità lavorative.

Un ulteriore aspetto fondamentale è **l'affidamento a personale civile di ruoli chiave per lo sviluppo tecnologico**. Gli Stati Uniti hanno formalmente identificato il Chief Technology Officer (CTO) nelle forze armate per l'integrazione delle tecnologie avanzate. Nel Regno Unito, il Ministero della Difesa ha identificato la necessità di una **posizione di CTO nel contesto delle sue iniziative di modernizzazione tecnologica**, come delineato nel «Defence Command Paper 2023». Anche l'Italia, con il DPCM approvato il 20 giugno 2024 per la riorganizzazione del Ministero della Difesa, ha istituito due figure che avranno un ruolo nell'**integrare la difesa con il sistema industriale e della ricerca**:

- Il Direttore per la Politica di Difesa che fornirà consulenza e assistenza ai massimi vertici del Ministero su questioni militari e industriali;
- L'Ufficio Studi Strategici e Innovazione Tecnologica che svolgerà attività di ricerca scientifica nei settori della sicurezza e dell'innovazione tecnologica.

Infine, la **crescente importanza delle tecnologie digitali per la difesa deve necessariamente essere accompagnata da considerazioni etiche sull'uso di strumenti avanzati**. Sono sempre più attuali le considerazioni etiche riguardanti l'utilizzo di AI nei sistemi di difesa: un esempio è il drone STM Kargu-2, un'arma autonoma di fabbricazione turca che, come riporta un rapporto del Gruppo di esperti delle Nazioni Unite sulla Libia, nel 2020 in Libia potrebbe aver "dato la caccia e ingaggiato da remoto" soldati in ritirata fedeli al generale libico Khalifa Haftar.

Le criticità dell'Europa nella gestione della difesa e nello sviluppo di tecnologie digitali

CAPITOLO 4

Il quarto capitolo dello Studio strategico si propone l'obiettivo di identificare le aree di debolezza dell'Unione Europea per quanto concerne la difesa: verrà approfondito (I) il posizionamento dell'Europa nello sviluppo delle tecnologie digitali per la difesa, attraverso un indicatore realizzato ad hoc (il TEHA - Digital Technologies Security Index), (II) la frammentazione della governance, della gestione degli asset e della capacità industriale, (III) gli esigui investimenti pubblici e privati a supporto dell'industria della difesa, (IV) l'eccessiva dipendenza strategica dell'Europa dalle forniture militari extra-UE (in particolare statunitensi) e (V) le difficoltà sul piano dell'accettazione della popolazione degli investimenti pubblici in difesa.

Dal capitolo emerge come l'Europa, se vuole davvero puntare ad avere una strategicità geopolitica a livello internazionale, debba risolvere queste criticità attraverso una visione unica di interesse europeo e non di singoli Paesi membri.

Le 5 aree di debolezza legate alla difesa che l'Europa deve affrontare

1.
Debolezza nel settore digitale

2.
Frammentazione politica, militare, industriale e della ricerca

3.
Limitati investimenti pubblici e difficoltà per gli investimenti privati

4.
Dipendenza strategica

5.
Social acceptance

4.1 Le 5 aree di debolezza legate alla difesa europea

Alla luce delle evidenze presentate nei capitoli precedenti di questo Studio strategico, è chiara la necessità per l'Europa di dotarsi di strumenti e meccanismi che la aiutino a recuperare il gap creatosi nei confronti delle altre grandi potenze mondiali, Stati Uniti in primis, relativamente ad ambiti che svolgono un ruolo centrale nel determinare il posizionamento strategico e il ruolo sul piano geopolitico internazionale di un Paese.

DEBOLEZZA 1

Debolezza nel settore digitale

4.2 Debolezza nel settore digitale

La prima area di debolezza della difesa europea concerne il settore digitale. Come mostrato nei capitoli precedenti, infatti, le tecnologie digitali svolgono un ruolo strategico nel garantire un vantaggio competitivo nei domini civili e della difesa; tuttavia, l'Unione Europa è in ritardo nello sviluppare, produrre e diffondere le tecnologie digitali avanzate. Come mostrano i risultati del **TEHA-Digital Technologies Security Index** progettato da TEHA Group per valutare il posizionamento dell'Europa rispetto ad altre geografie mondiali in cinque ambiti chiave dello sviluppo delle tecnologie digitali (AI, Big Data e Digital Twin, Cloud Computing e HPC, Connectivity, Cybersecurity, Quantum Technologies), l'UE27, sebbene competitiva in alcune aree, presenta una performance complessiva bassa, suggerendo, in particolare, la necessità di maggiori investimenti e strategie di implementazione più efficaci.

TEHA Group ha creato un indice per valutare la dipendenza dell'Europa nelle tecnologie digitali per la difesa: il TEHA - Digital Technologies Security Index (TEHA - DTSI)

Il TEHA - Digital Technologies Security Index (TEHA - DTSI) è uno **strumento informativo e di orientamento decisionale** che valuta il posizionamento dell'Europa a confronto con altre geografie rispetto a **5 ambiti di sviluppo delle tecnologie digitali**

5 AMBITI TECNOLOGICI

1. AI, Big Data, e Digital Twin
2. Cloud Computing e HPC
3. Connectivity
4. Cybersecurity
5. Quantum Technologies

3 AMBITI DI VALUTAZIONE

- **Develop** → Capacità di un'economia di fare ricerca e sviluppo
- **Produce** → Capacità di un paese di produrre tecnologie digitali
- **Deploy** → Forza di un'economia nella diffusione di una tecnologia

13 GEOGRAFIE

Il TEHA - Digital Technologies Security Index indica il **posizionamento di 13 Paesi**:

1. Cina
2. Francia
3. Germania
4. India
5. Iran
6. Italia
7. Paesi Bassi
8. Regno Unito
9. Russia
10. Spagna
11. Stati Uniti
12. Svezia
13. UE-27

Posizionamento di 5 Paesi selezionati nel TEHA – Digital Technologies Security Index rispetto a tecnologia e dimensione

(punteggio da 0 a 10), 2024

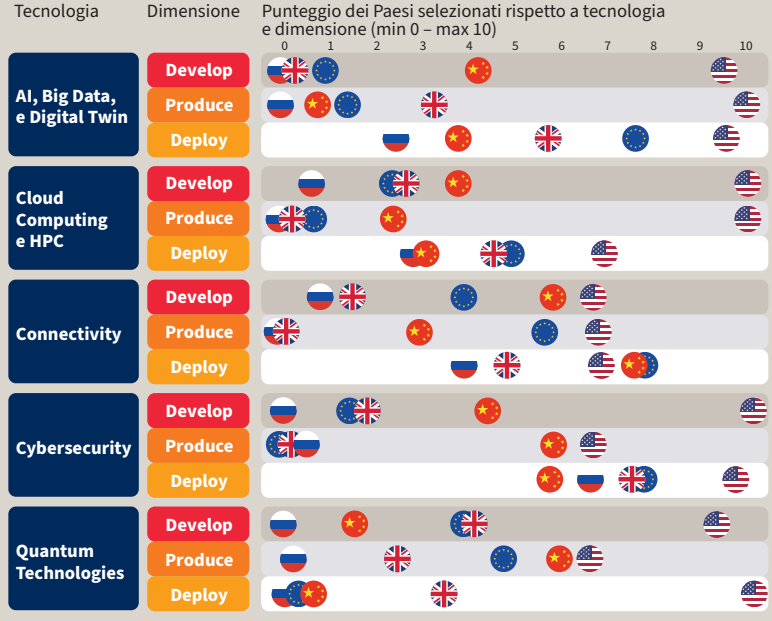


Figura 1. Il TEHA - Digital Technologies Security Index 2024 (punteggio da 0 a 10).

Fonte: elaborazione TEHA Group, 2024.

A fronte della centralità delle tecnologie digitali per gli equilibri geopolitici internazionali e la competitività dell'Europa, TEHA Group ha sviluppato il **TEHA - Digital Technologies Security Index (TEHA-DTSI)**. Il TEHA – DTSI è uno **strumento informativo e di orientamento decisionale** progettato per valutare il posizionamento dell'Europa rispetto ad altre geografie mondiali in cinque ambiti chiave dello sviluppo delle tecnologie digitali: AI, Big Data e Digital Twin, Cloud Computing e HPC, Connectivity, Cybersecurity, Quantum Technologies. Queste tecnologie avranno un ruolo strategico nel garantire un vantaggio competitivo nei domini civili e della difesa.

Il TEHA-DTSI valuta le performance dei paesi in tre dimensioni principali:

- **Develop**: indica la capacità di un'economia di fare R&S e di trasferirne i risultati sul mercato;
- **Produce**: coglie la capacità di un paese di produrre o la dipendenza da altri paesi per la produzione tecnologica;
- **Deploy**: dimostra l'attuale forza e resilienza di un'economia rispetto alla diffusione di una tecnologia.

Il TEHA-DTSI è composto da **38 KPI monitorati in 13 Paesi e regioni** (Cina, Francia, Germania, India, Iran, Italia, Paesi Bassi, Regno Unito, Russia, Spagna, Stati Uniti, Svezia e UE-27) per gli anni 2019 e 2024.

L'Indice TEHA-DTSI 2024 mostra gli Stati Uniti al primo posto nella classifica complessiva, considerando tutti e cinque gli ambiti tecnologici, in tutte e tre le dimensioni. Con un punteggio di 9,1 nella dimensione Develop, gli Stati Uniti sono seguiti da Cina (3,8) e UE-27 (2,4), con punteggi significativamente inferiori. L'Italia si posiziona al settimo posto su 13 con un punteggio di 1,2, dopo Regno Unito (1,9), Svezia (1,4) e Paesi Bassi (1,3). Nella dimensione Produce, gli Stati Uniti si posizionano al primo posto con un punteggio di 8,0, seguiti sempre da Cina (3,5) e UE-27 (2,3). In questa dimensione, l'Italia è al nono posto su tredici, con un punteggio di 1,9. Infine, nella dimensione Deploy, gli Stati Uniti si posizionano sempre al primo posto con un punteggio di 8,3, seguiti da Paesi Bassi (7,3) e Svezia e UE-27 a parimerito con un punteggio di 6,4. L'Italia, invece, è all'ottavo posto, con un punteggio di 5,1, mentre la Cina scende al decimo posto, con un punteggio di 4,6.

Analizzando i risultati per ambito tecnologico, **l'UE-27 si posiziona in forte ritardo** – con un punteggio inferiore a 1,5 – **nella capacità di fare R&S e di trasferirne i risultati sul mercato nell'ambito delle tecnologie AI, Big Data, Digital Twin e Cybersecurity** (in linea con Russia e UK, ma indietro rispetto a Cina e, soprattutto, agli Stati Uniti). In questa dimensione, l'UE-27 **rimane significativamente indietro rispetto agli Stati Uniti**, registrando punteggi inferiori a 4, **anche nelle altre tecnologie considerate** (Cloud Computing e HPC, Connectivity e Quantum Technologies).

Il ritardo dell'UE-27 permane anche nella dimensione Produce, con un punteggio inferiore a 1,5 per capacità di produrre tecnologie AI, Big Data, Digital Twin, Cloud Computing, HPC e Cybersecurity. Risultati intermedi, seppure sempre inferiori rispetto a quelli degli Stati Uniti, sono registrati per Connectivity e Quantum Technologies.

L'UE-27, infine, **si posiziona relativamente bene per capacità di diffusione di AI, Big Data e Digital Twin, Connectivity e Cybersecurity**, mentre registra un punteggio intermedio per la diffusione di HPC e Cloud Computing (in linea con il Regno Unito ma indietro rispetto agli Stati Uniti), **registrando tuttavia un forte ritardo nella diffusione delle Quantum Technologies** (in linea con le performance di Cina e Russia).

In conclusione, l'analisi dei dati rivela una chiara superiorità degli Stati Uniti in tutte le dimensioni e tecnologie analizzate, con punteggi massimi o molto alti che riflettono una leadership consolidata nel settore tecnologico. L'UE27, sebbene competitiva in alcune aree, presenta una performance complessiva significativamente inferiore, suggerendo la necessità di maggiori investimenti in R&S e strategie di implementazione più efficaci.

Tabella dei Key Performance Indicators (KPIs) del TEHA-DTSI

	1 AI, Big Data, e Digital Twin	2 Cloud Computing e HPC	3 Connectivity	4 Cybersecurity	5 Quantum Technologies
Develop	**1.1** Quota di spesa in R&S da parte dei 10 principali finanziatori di R&S **1.2** Finanziamenti di venture capital in AI, Big Data e Digital Twin **1.3** Quota di brevetti nei settori AI, Big Data e Digital Twin	**2.1** Quota di spesa in R&S da parte dei 10 principali finanziatori di R&S **2.2** Quota di brevetti nelle tecnologie cloud e informatiche **2.3** Spesa per l'infrastruttura cloud	**3.1** Quota di spesa in R&S da parte dei 10 principali finanziatori di R&S **3.2** N. di brevetti riusciti pro capite (telecomunicazioni) **3.3** Pubblicazioni / 1000 ricercatori (reti informatiche e comunicazioni)	**4.1** Classifica universitaria **4.2** % quota di pubblicazione della ricerca sulla cybersecurity **4.3** Quota Paese tra le prime 100 aziende di cybersecurity	**5.1** Numero di istituti di ricerca dedicati al Quantum Computing **5.2** Quota di brevetti nella tecnologia quantistica **5.3** N. di sviluppatori di informatica quantistica pro capite
Produce	**1.4** Capitalizzazione di mercato delle prime 5 aziende oltre i $10 miliardi **1.5** Numero di unicorni pro capite	**2.4** Capitalizzazione di mercato delle prime 5 aziende oltre i $10 miliardi **2.5** Numero medio di dipendenti nelle prime 5 aziende per capitalizzazione di mercato	**3.4** Capitalizzazione di mercato delle prime 5 aziende oltre i $10 miliardi **3.5** Spesa del settore pubblico per il 5G	**4.4** Capitalizzazione di mercato delle prime 5 aziende oltre i $10 miliardi **4.5** Numero medio di dipendenti nelle prime 5 aziende per capitalizzazione di mercato	**5.4** Spesa del settore pubblico per l'informatica quantistica **5.5** Quota di aziende di crittografia quantistica / comunicazioni
Deploy	**1.6** Contributo a progetti di IA su GitHub **1.7** Data center pro capite **1.8** Propensione ad adattarsi alle nuove tecnologie	**2.6** Core di supercomputer pro capite **2.7** Supporto governativo per il cloud **2.8** N. di punti di scambio Internet pro capite	**3.6** % di popolazione coperta dal 5G **3.7** Latenza 5G **3.8** Tasso di penetrazione della fibra ottica	**4.6** Server internet sicuri per milione di abitanti **4.7** Sostegno governativo alla sicurezza informatica **4.8** % di utenti attaccati da virus	**5.6** Qubit (potenza di elaborazione quantistica) pro capite

DEBOLEZZA 2

Frammentazione politica, militare, industriale e della ricerca

4.3.1 FRAMMENTAZIONE POLITICA

La difesa rappresenta uno dei settori più delicati e complessi all'interno dell'Unione Europea ed è caratterizzata da una marcata frammentazione politica e da un certo grado di protezionismo industriale. Tale frammentazione può essere attribuita a diversi fattori, tra cui:

- **Sovranità Nazionale**: gli Stati membri sono riluttanti a cedere il controllo sulle proprie capacità di difesa, considerate un elemento chiave della sovranità nazionale;
- **Differenze Strategiche**: gli interessi strategici e le percezioni delle minacce variano notevolmente tra gli Stati membri, rendendo difficile l'adozione di una politica di difesa comune;
- **Protezione delle Industrie Nazionali**: ogni Stato membro si preoccupa di proteggere le proprie industrie della difesa per motivi economici e occupazionali, limitando la concorrenza e la cooperazione transnazionale.

Relativamente alla protezione delle industrie nazionali, questa è in parte legata all'**articolo 346 del Trattato sul Funzionamento dell'Unione Europea** (TFEU), che consente agli Stati membri di derogare alle normative del mercato interno per tutelare gli interessi nazionali essenziali, relativi alla produzione e al commercio di armi, munizioni e materiali bellici con un duplice utilizzo strategico. In particolare, il TFEU permette due approcci distinti:

1. **Protezionismo industriale**: a sostegno delle industrie militari nazionali, permettendo ai singoli Stati membri di imporre restrizioni sulle esportazioni di materiale bellico e di adottare misure protettive. Questo approccio ha contribuito a mantenere una frammentazione del mercato della difesa in Europa, con ogni paese che cerca di proteggere e promuovere le proprie capacità industriali;
2. **Cooperazione e consolidamento industriale transnazionale**: facilita il consolidamento delle capacità industriali di difesa tra gli Stati membri con la creazione di consorzi e programmi congiunti. Questo approccio mira a superare le barriere nazionali e a promuovere una maggiore integrazione europea nel settore della difesa.

Nonostante la prevalente frammentazione industriale, esistono **alcuni esempi virtuosi di cooperazione europea nel settore della difesa**. Uno dei casi più emblematici è rappresentato da MBDA Missile Systems. Nato nel 2001, **MBDA** è il principale consorzio europeo costruttore di missili e tecnologie per la difesa. È una joint venture che coinvolge Airbus (37,5%), BAE Systems (37,5%) e Leonardo (25%), con oltre 15.000 dipendenti in sei paesi.

MBDA è leader europeo nel mercato dei missili e occupa il terzo posto a livello mondiale, dopo Lockheed Martin e RXT. L'azienda è coinvolta in numerosi **programmi di cooperazione**, come il sistema di difesa aerea a base Aster, impiegato su fregate e su sistemi terrestri come il SAMP/T, il Future Cruise/Anti-Ship Weapon (FC/ASW) tra Francia e Regno Unito, e il programma di combattimento aereo del futuro (Future Air Combat), che include il FCAS (Future Combat Air System) e il GCAP (Global Combat Air Programme).

Al 2023 impiega oltre **15.000 dipendenti in 6 Paesi.**

L'esperienza di MBDA dimostra che la **cooperazione transnazionale è possibile** e può portare a risultati significativi. Tuttavia, questi esempi sono ancora rari rispetto alla prevalenza del protezionismo e della frammentazione politica.

Un altro caso virtuoso di cooperazione industriale nel settore della difesa europeo è quello del programma FREMM. **Le Fregate Europee Multi-Missione (FREMM) rappresentano un esempio di cooperazione multinazionale, sviluppato congiuntamente da Italia e Francia**.

Il 16 novembre 2005 è stato firmato il contratto relativo alla fase di sviluppo, costruzione e accettazione in servizio delle unità, inclusa la fornitura di supporto logistico. Il progetto prevede la costruzione di 18 navi, suddivise tra 10 fregate italiane (6 di tipo "General Purpose" e 4 antisommergibile) e 8 francesi (tipi antisommergibile e attacco contro costa).

Nonostante sia considerato come un esempio virtuoso di collaborazione multinazionale a livello industriale, il progetto stesso mette in luce una debolezza strutturale del processo di procurement europeo: nonostante siano progettate per essere una piattaforma comune a due Stati, **ciascun Paese ha dettato requisiti diversi** per il proprio ordine di fornitura, derivante dalle diverse esigenze della flotta. Questo ha portato, così, alla realizzazione di navi con diverse differenze:

- Lunghezza: 144,6 m (Italia) vs 142,0 m (Francia)
- Larghezza: 19,7 m (Italia) vs 20,0 m (Francia)
- Ponti: 1 in più per FREMM italiana
- Elicotteri: 2 (Italia) vs 1 (Francia)
- Difesa missilistica di area: 10/10 unità (Italia) vs 2/8 unità (Francia)
- Sistemi di bordo: variazioni specifiche per ogni nazione

Anche **Leonardo e Rheinmetall** hanno da poco firmato un accordo per avviare una collaborazione nello sviluppo di piattaforme di difesa comune. Questi possono essere visti come i primi passi verso l'integrazione europea delle aziende della difesa.

Il 3 luglio 2024, **Leonardo e Rheinmetall hanno firmato un Memorandum of Understanding** (MoU) volto alla creazione di una nuova Joint Venture paritetica che ha l'obiettivo di sviluppare un approccio industriale e tecnologico di respiro europeo nel campo dei sistemi di difesa Terrestre. L'accordo è finalizzato allo sviluppo industriale e alla successiva commercializzazione del nuovo Main Battle Tank (MBT) e della nuova piattaforma Lynx per il programma Armoured Infantry Combat System (AICS) in seno ai programmi dei sistemi terrestri dell'Esercito italiano. Questo accordo è un esempio concreto di come alcune aziende europee stiano cercando di **superare le barriere nazionali per affrontare le sfide comuni**, contribuendo così a una maggiore integrazione e coesione del mercato della difesa europeo. Attraverso tali collaborazioni, **l'Europa può rafforzare la propria autonomia strategica** e migliorare l'efficacia delle proprie capacità difensive.

Presi singolarmente, gli Stati membri dell'UE sono molto lontani dalla forza militare delle altre grandi potenze

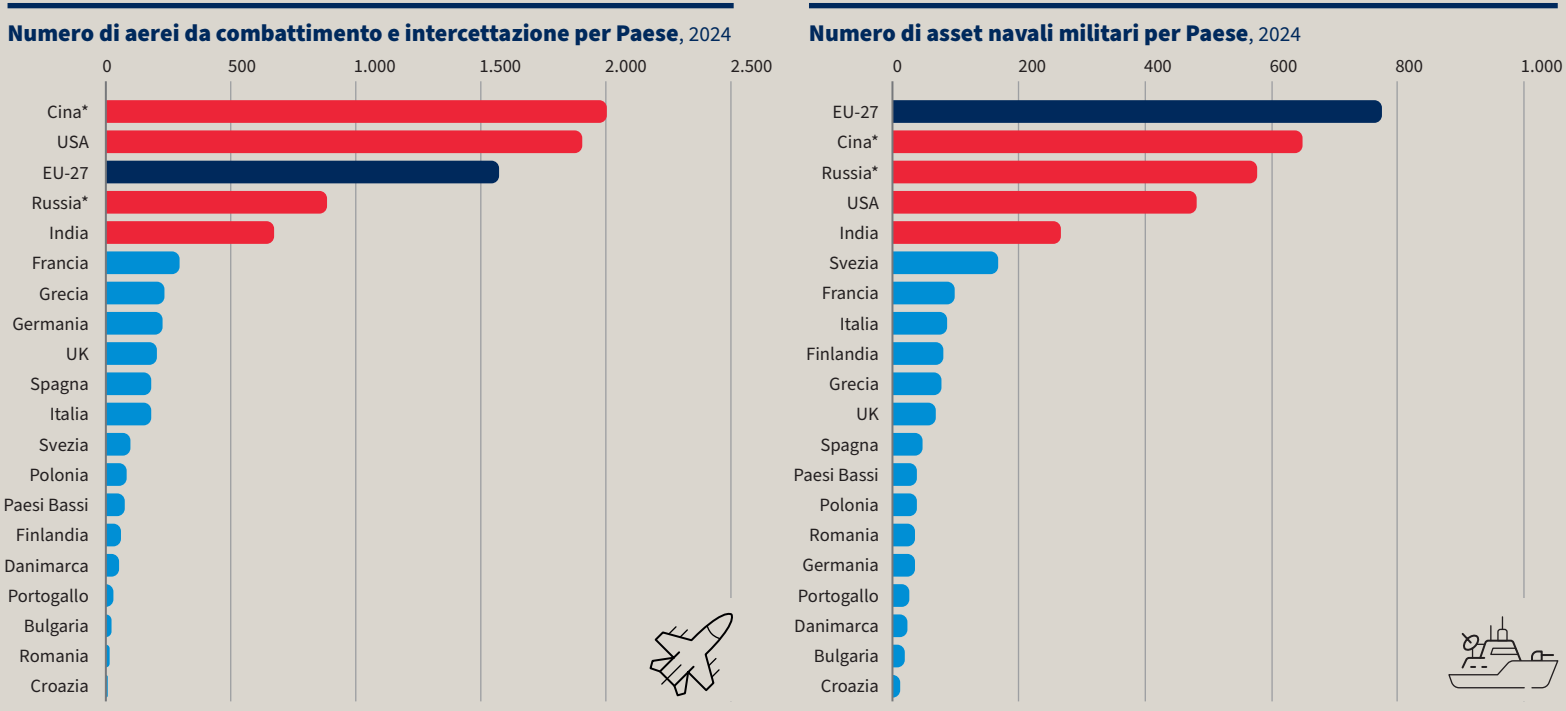


Figura 2. Numero di aerei da combattimento e intercettazione per Paese (grafico a sx), 2024 e Numero di asset navali militari per Paese (grafico a dx), 2024. (*) i valori di Cina e Russia sono stimati e probabilmente sottovalutati.

Fonte: TEHA Group su dati IISS, 2024.

4.3.2 FRAMMENTAZIONE MILITARE

La frammentazione militare dell'Unione Europea rappresenta una delle principali sfide per la sua rilevanza geopolitica e la capacità di difesa collettiva. I singoli Stati membri mostrano capacità militari poco significative mentre, **solo se l'UE viene presa nel suo insieme** è in grado di mostrare una quantità di asset paragonabile a quella delle altre grandi potenze, come gli Stati Uniti, la Cina e la Russia. Questo divario è evidente quando si esamina il numero di asset aerei e navali militari per paese, come mostrato nelle tabelle a fianco.

I due grafici di seguito mettono a confronto i diversi Paesi sul piano degli asset di aerei militari e navali:

- Nel primo, Cina e Stati Uniti dominano con circa 2.000 aerei da combattimento e intercettazione, seguiti dall'UE-27 con poco più di 1.500, e poi da Russia e India con circa la metà degli asset di Cina e USA (circa 800 e 600 rispettivamente). I paesi europei presi singolarmente hanno una forza militare non paragonabile rispetto alle prime quattro potenze internazionali.
- Analogamente, nel secondo grafico l'UE-27 nel suo complesso mostra una cifra significativa di circa 800 asset, superando significativamente Paesi come Cina, Russia, USA e India, che si posizionano tra i circa 600 della Cina e i 200 dell'India. Tuttavia, presi singolarmente i Paesi hanno capacità molto limitate.

La frammentazione militare è anche il risultato di una **mancanza di visione e allineamento politico degli interessi comunitari**; ne è un esempio il caso dell'European Rapid Operational Force (EUROFOR), nato nel 1995 con la Dichiarazione di Lisbona, come iniziativa congiunta di Italia, Spagna, Francia e Portogallo, con l'obiettivo di dotare l'Europa di una capacità militare propria e autonoma. L'iniziativa rispondeva alla necessità di avere una forza militare in grado di intervenire rapidamente in situazioni di crisi, partecipare alle missioni di mantenimento della pace e contribuire alla sicurezza internazionale. Nonostante le buone intenzioni, l'EUROFOR ha incontrato diverse difficoltà che ne hanno limitato l'efficacia. Una delle principali sfide è stata la mancanza di una visione politica comune tra i paesi membri. Questa frammentazione politica ha avuto conseguenze significative sulla capacità operativa della forza, come evidenzia l'episodio del Kosovo dove la dichiarazione unilaterale di indipendenza del 2008 ha portato al veto da parte spagnola al suo impiego in quella circostanza e alla conseguente decisione di sciogliere EUROFOR.

La mancata cooperazione per la difesa a livello comunitario causa, infine, un **aumento significativo dei costi per il dispiegamento delle truppe**. Un'analisi del 2020 dell'European Parliamentary Research Service ha evidenziato che una maggiore cooperazione tra i Paesi potrebbe ridurre questa spesa fino a 32 miliardi di euro, pari al 46% del totale.

A livello europeo si registra una inefficienza della spesa in difesa a causa della moltiplicazione dei progetti che impediscono lo sfruttamento di rendimenti di scala

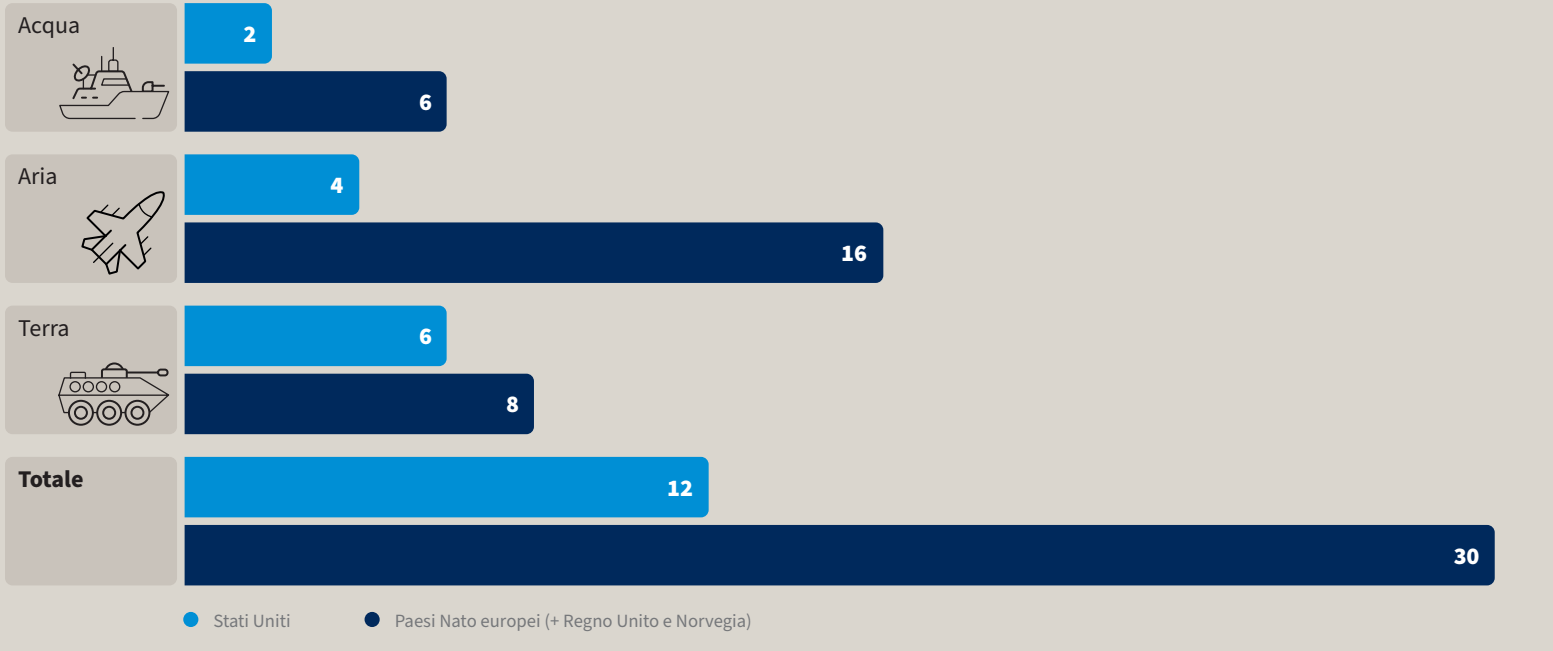


Figura 3. Numero di piattaforme militari in dotazione per dominio nei Paesi Nato europei e negli Stati Uniti (valori assoluti), 2024.

Fonte: TEHA Group su fonti varie, 2024.

4.3.3 FRAMMENTAZIONE INDUSTRIALE E DELLA RICERCA

La frammentazione industriale della difesa nell'Unione Europea rappresenta un problema significativo che ha ripercussioni dirette sulla **capacità dei Paesi membri di sviluppare e mantenere capacità militari efficienti ed economicamente sostenibili**. Questo problema emerge chiaramente quando si analizza la dispersione delle risorse nella produzione di un numero di piattaforme militari significativamente superiore rispetto agli Stati Uniti: i Paesi NATO europei dispongono di un numero molto più elevato di piattaforme rispetto agli Stati Uniti, senza tuttavia raggiungere gli stessi livelli di efficienza e capacità operativa. Per esempio, nell'ambito delle piattaforme navali, gli Stati Uniti utilizzano solo 2 tipi di piattaforme contro le 6 dei Paesi europei. Questa dinamica si ripete nelle piattaforme aeree (4 negli USA contro 16 in Europa) e terrestri (6 negli USA contro 8 in Europa), portando ad un totale di 12 piattaforme americane contro le 30 europee[68]. Questa frammentazione comporta una **dispersione di risorse** e una **duplicazione degli sforzi**, che potrebbero essere evitati con una maggiore standardizzazione e cooperazione.

Inoltre, la mancanza di cooperazione provoca una **bassa efficienza della spesa in ricerca e sviluppo** nel settore e la **moltiplicazione dei contratti di fornitura**. Con una maggiore cooperazione in questi ambiti, **l'efficienza potrebbe ridurre i costi di procurement fino a 12,7 miliardi di euro** (pari al 50% del totale)[69].

Un ulteriore dato significativo è quello fornito dall'Agenzia Europea per la Difesa: dei 3,5 miliardi di euro investiti nel 2022 in ricerca e sviluppo, **meno del 10% è stato speso su progetti che coinvolgono più di un Paese**. Questo dato sottolinea l'urgenza di promuovere programmi congiunti per massimizzare l'efficienza e i benefici economici.

68 Fonte: TEHA Group da dati vari, 2024

69 Fonte: TEHA Group su dati European Parliamentary Research Service, 2024

Lo sviluppo di sistemi d'arma sofisticati richiede tempi di sviluppo sempre più lunghi e investimenti che un solo paese difficilmente riesce a sostenere

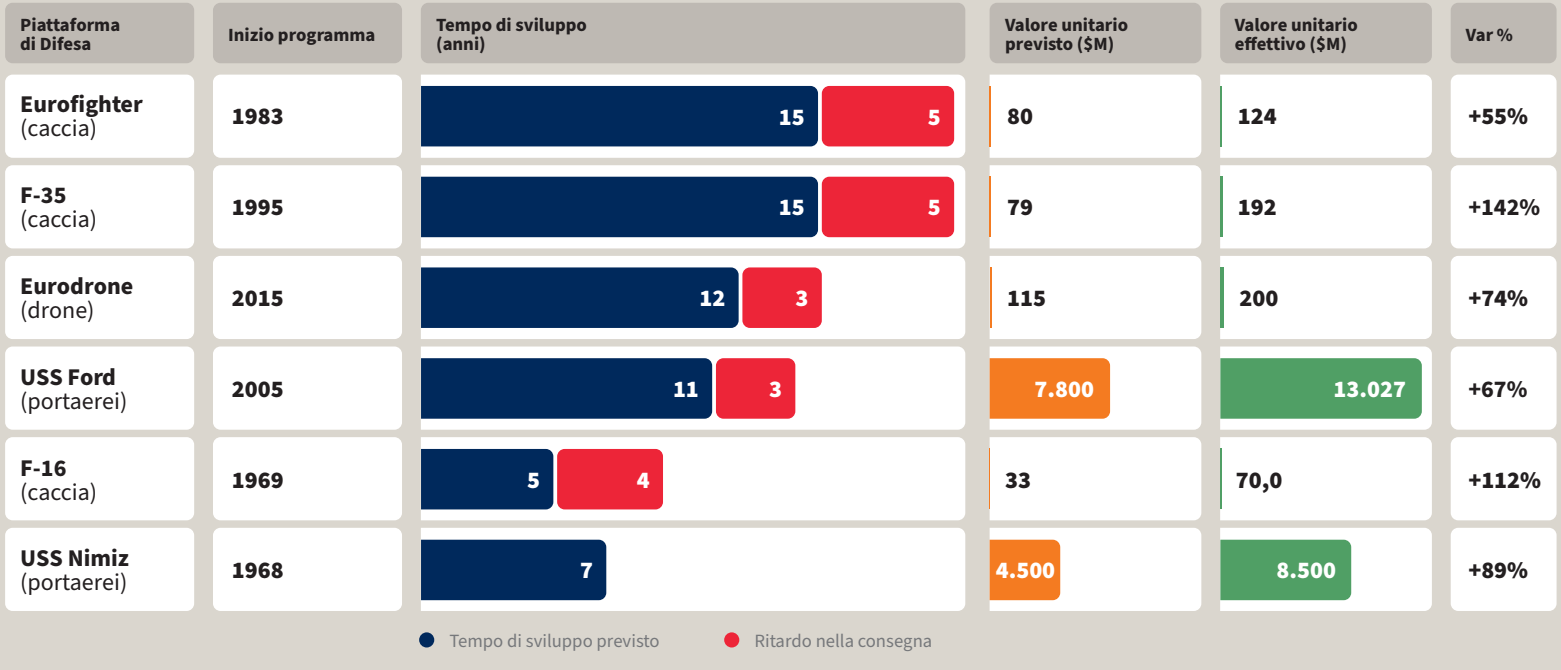


Figura 4. Tempo di sviluppo e incremento di costi dei nuovi sistemi di Difesa militare, 2024.

Fonte: TEHA Group su dati dei programmi delle piattaforme di difesa, 2024.

Un altro aspetto fondamentale da tenere in considerazione riguarda il **tempo e il costo necessari allo sviluppo di nuove piattaforme di difesa**.

Lo **sviluppo di sistemi d'arma sofisticati richiede periodi sempre più lunghi**. Ad esempio, la progettazione e realizzazione dell'Eurofighter ha richiesto 15 anni, con un ritardo di cinque anni rispetto ai tempi previsti. Un'altra piattaforma, l'F-35, ha anch'essa impiegato 15 anni per lo sviluppo, subendo un ritardo analogo. Questo prolungamento dei tempi di sviluppo non solo ritarda l'entrata in servizio di nuovi sistemi, ma ne aumenta anche i costi complessivi a causa dell'accumularsi delle spese di ricerca e sviluppo nel corso degli anni.

Il prolungarsi dei tempi di sviluppo è strettamente legato a un **aumento esponenziale dei costi di questi programmi**: l'Eurofighter, inizialmente previsto con un valore unitario di circa 80 milioni di dollari, ha visto il suo valore effettivo salire a 124 milioni di dollari, con un incremento del 55%. L'F-35 ha subito un aumento ancora più marcato, passando da un valore previsto di 79 milioni di dollari a un valore effettivo di 192 milioni di dollari, pari a un incremento del 142%. Questo trend è evidente anche per altre piattaforme, come l'Eurodrone, le cui spese sono aumentate del 74%, e le portaerei USS Ford e USS Nimitz, con incrementi rispettivamente del 67% e dell'89%.

Le cause di questi ritardi e aumenti dei costi sono molteplici. In primo luogo, la **complessità tecnologica** dei nuovi sistemi d'arma richiede ricerche approfondite e test rigorosi, che spesso rivelano problemi non previsti durante la fase di progettazione. Inoltre, la **necessità di integrare tecnologie avanzate e innovative** può portare a difficoltà tecniche che richiedono ulteriori investimenti per essere risolte.

Un altro fattore è rappresentato dal cambio di **requisiti operativi durante lo sviluppo del programma**. Spesso, durante i lunghi periodi di sviluppo, emergono nuove esigenze operative o vengono introdotte nuove tecnologie, che richiedono aggiornamenti e revisioni dei progetti iniziali. Questi cambiamenti aumentano i costi e allungano i tempi di sviluppo.

Infine, è necessario segnalare che la frammentazione nella formulazione dei requisiti comporta anche difficoltà nel far dialogare i sistemi, rendendo più difficile il controllo comune degli strumenti di difesa.

Alla luce di queste evidenze, è chiaro come sia **sempre più difficile, per i singoli Paesi, sostenere questi costi crescenti e gestire i ritardi nello sviluppo**. La dispersione delle risorse su più progetti indipendenti, senza una cooperazione efficace a livello europeo, impedisce la realizzazione di economie di scala e la condivisione dei costi tra più nazioni. Di conseguenza, molti Paesi si trovano a dover scegliere tra ridurre le proprie ambizioni in termini di capacità difensive o aumentare significativamente il proprio budget militare, con inevitabili ripercussioni su altri settori della spesa pubblica.

DEBOLEZZA 3

Limitati investimenti pubblici e difficoltà per gli investimenti privati

4.4.1 LIMITATI INVESTIMENTI PUBBLICI E DIFFICOLTÀ PER GLI INVESTIMENTI PRIVATI

L'impegno finanziario è fondamentale per lo sviluppo di progetti legati alla difesa che, come abbiamo visto, sono caratterizzati da tempi di sviluppo sempre più lunghi (e incerti) e da costi che risultano molto maggiori rispetto a quanto preventivato inizialmente. I fondi pubblici e la disponibilità della finanza privata rappresentano, di conseguenza, un fattore critico per il successo di interi ecosistemi che sviluppano innovazione per la difesa. Come evidenziato di seguito, l'Europa mostra debolezze sia sul piano degli investimenti pubblici in difesa, cronicamente al di sotto di quanto raccomandato in ambito NATO, sia sul piano del sostegno della finanza privata, che incontra limitazioni proprie dei mercati dei capitali, come i criteri ESG per gli investimenti.

Con l’1,7% del PIL investito nella difesa, l’UE è ancora lontana dall’obiettivo del 2% della NATO e molto indietro rispetto a USA e Russia

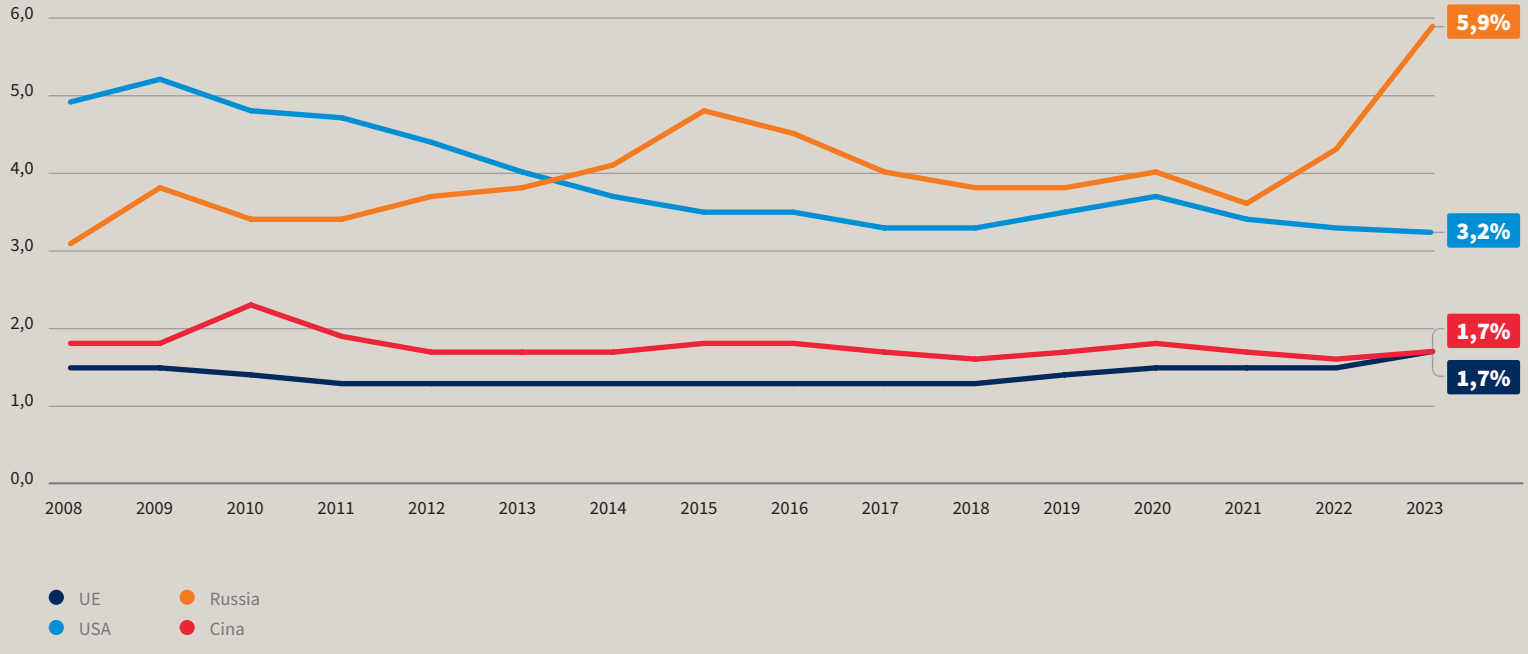


Figura 5. Spesa totale per la Difesa (% sul PIL), 2008-2023.
N.B.: la spesa totale effettivamente destinata alla difesa dalla Cina e della Russia è stimata e probabilmente sottovalutata.
Fonte: TEHA Group su dati NATO e Sipri, 2024.

4.4.2 LIMITATI INVESTIMENTI PUBBLICI

Gli investimenti pubblici sono centrali quando si parla di difesa, in quanto rappresentano la leva per il potenziamento della capacità militare e degli avanzamenti tecnologici; grazie a questi investimenti si hanno anche importanti ripercussioni sul mondo civile, come vedremo più avanti in questo capitolo. L'Europa, in questo indicatore ha una performance di molto inferiore rispetto ai propri peers: **la spesa totale per la difesa in percentuale del PIL nell'Unione Europea (UE) si attesta attualmente all'1,7%, un valore significativamente inferiore all'obiettivo del 2% raccomandato dalla NATO**. Questo valore è altresì molto indietro rispetto a quello di altre grandi potenze come gli Stati Uniti (3,2%) e la Russia (5,9%), evidenziando una discrepanza marcata nella distribuzione delle risorse per la difesa. Se i Paesi membri dell'UE avessero investito il 2% del PIL nella difesa dal 2006 al 2020, destinando il 20% di tale somma agli investimenti in R&S, **oggi sarebbero disponibili 1.100 miliardi di euro supplementari per la difesa**, di cui circa 270 miliardi per investimenti in innovazione.

Inoltre, se le risorse pubbliche europee investite in difesa fossero paragonabili a quelle americane, vi sarebbero enormi benefici anche sul piano della ricerca e sviluppo di nuove tecnologie: gli **Stati Uniti investono in Ricerca, Sviluppo, Test e Valutazione** (RDT&E) il 17,2% **($145 miliardi**) del budget della difesa ($842 miliardi). Se l'Unione Europea investisse la stessa quota, avrebbe a disposizione, ogni anno, **tra i €65 e gli €80 miliardi**, che potrebbe investire nello **sviluppo di tecnologie digitali avanzate** che, non solo migliorano le capacità difensive, ma stimolano anche l'innovazione tecnologica e la crescita economica.

Negli Stati Uniti, il Dipartimento della Difesa gioca un **ruolo cruciale nel finanziare programmi per lo sviluppo di tecnologie di difesa**, attirando significativi investimenti privati. Aziende come **SpaceX** e **Palantir** hanno beneficiato di contratti di importo rilevante con il Pentagono, che non solo supportano lo sviluppo di nuove capacità ma aumentano anche l'attrattività di queste aziende per gli investitori privati. Ad esempio, SpaceX ha ottenuto numerosi contratti per il lancio di satelliti militari e tracciamento dei missili, mentre Palantir ha ricevuto fondi per sviluppare sistemi di intelligenza artificiale per uso militare.

In contrasto, i fondi messi a disposizione dall'UE per finanziare programmi tecnologici sono significativamente inferiori rispetto a quelli degli Stati Uniti. L'Agenzia Spaziale Europea (ESA) ha avviato iniziative per creare un servizio cargo per orbita bassa (simile a quanto avviene in US, fornito tra le altre anche da SpaceX), firmando contratti con l'industria europea per sviluppare servizi di trasporto verso la Stazione Spaziale Internazionale. Tuttavia, i **fondi** disponibili sono **significativamente minori: l'ESA ha stanziato solo €50 milioni per la prima fase del progetto** (The Exploration Company con sede in Germania e Thales Alenia Space con sede in Italia), **rispetto ai $400 milioni iniziali garantiti dalla NASA a SpaceX** e altri fornitori, con successivi contratti fissi per importi ingenti.

4.4.3 DIFFICOLTÀ DEGLI INVESTIMENTI PRIVATI NEL SETTORE DELLA DIFESA

Le aziende del settore della difesa nell'UE affrontano difficoltà significative nell'**accesso ai finanziamenti**, dovute in parte a un mercato dei capitali che **disincentiva gli investimenti privati**. Tra le cause principali di queste difficoltà si annoverano:

- politiche di esclusione degli investimenti, con molti investitori istituzionali che adottano criteri ESG (ambientali, sociali e di governance) escludendo le aziende della difesa;
- credit ratings che incorporano fattori ESG nelle valutazioni del credito, penalizzando le aziende del settore con scarse performance ESG, rendendo più costoso e difficile il reperimento di capitali per queste aziende;
- preferenze degli investitori che incidono negativamente, con una crescente domanda di prodotti conformi alle norme ESG. I mercati dei capitali tendono quindi a offrire condizioni meno favorevoli alle società di difesa rispetto a quelle con migliori rating ESG;
- ambiente normativo dell'UE, che attraverso regolamenti come l'EU Sustainable Finance Disclosure Regulation, impone maggiore trasparenza su come gli operatori finanziari integrano i criteri ESG, creando ulteriori barriere per le aziende con profili ESG inadeguati.

Infine, un aspetto da mettere in luce è l'importante presenza degli **investimenti in venture capital statunitensi nelle startup della difesa che, negli ultimi dieci anni sono cresciuti del 538%**, raggiungendo un picco di **39 miliardi di dollari nel 2021**. Questo trend positivo è sostenuto dalla capacità delle startup di attrarre fondi significativi per le innovazioni in difesa e dal ruolo degli investimenti pubblici che agiscono da catalizzatore degli investimenti privati.

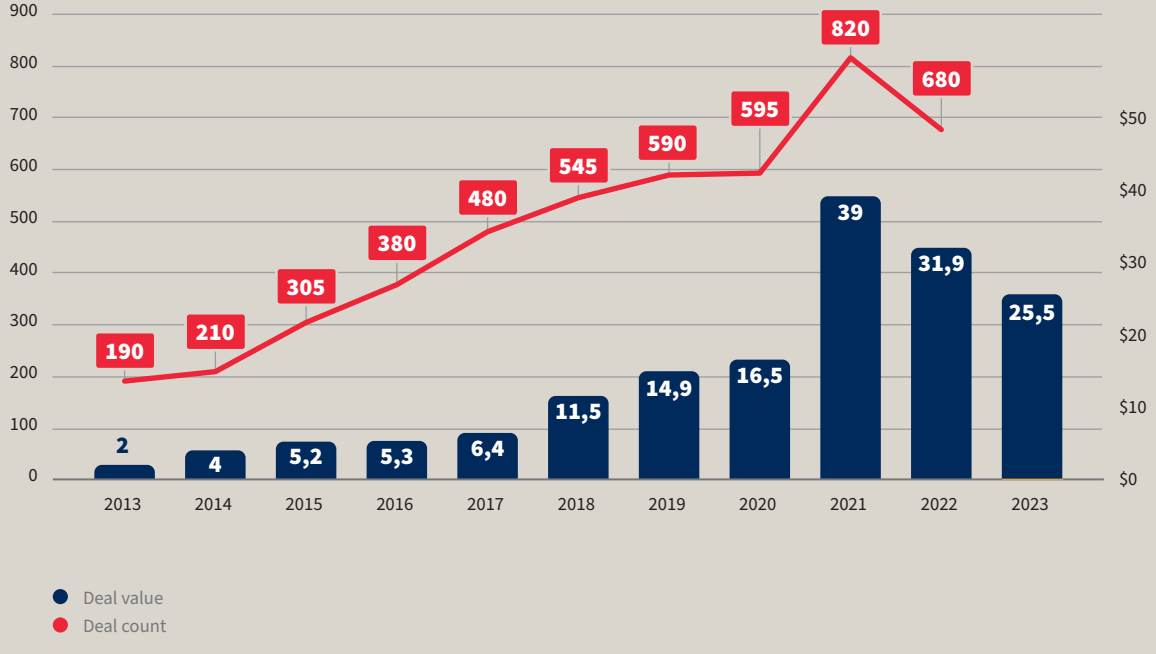


Figura 6. Investimenti Venture Capital in startup defense tech negli Stati Uniti (grafico a sinistra, numero di deal e valore in miliardi di $), 2013-2023E e Alcuni esempi di aziende USA che hanno ricevuto sostegno da fondi di investimento (grafico a destra).

Fonte: elaborazione TEHA Group su dati Pitchbook, 2024

DEBOLEZZA 4

Dipendenza strategica

4.5 Dipendenza strategica

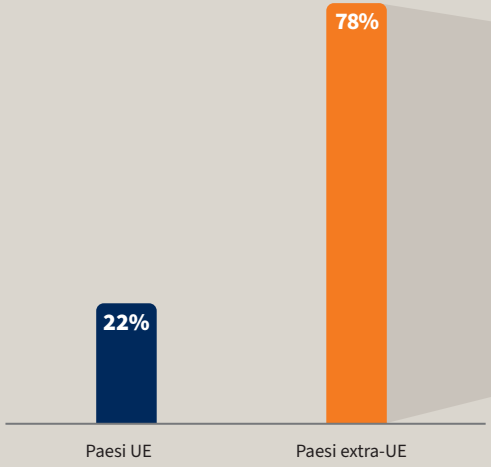
La sfida dell'Unione Europea nel settore della difesa è amplificata dalla sua significativa dipendenza da fornitori esteri per le attrezzature di difesa. L'UE destina risorse limitate alla ricerca e sviluppo nel settore della difesa, il che la pone in una posizione di svantaggio competitivo rispetto ad altre potenze globali, come gli Stati Uniti, che investono massicciamente in innovazione e sviluppo tecnologico per la difesa e presentano varie agenzie dedicate al supporto dell'innovazione in settori strategici per la superiorità tecnologica del Paese.

Nonostante l'istituzione del Fondo Europeo per la Difesa (FED) nel 2021 e la presentazione della prima strategia industriale europea della difesa (EDIS) nel marzo 2024, gli sforzi per promuovere una base industriale e tecnologica di difesa europea sono ancora limitati.

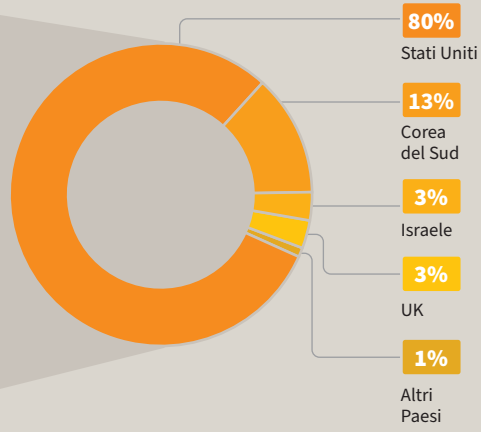
Gli obiettivi futuri delineati dall'UE, volti a incrementare gli acquisti collaborativi, gli scambi commerciali intra-UE nel settore della difesa e la quota di bilancio di ciascun paese membro destinata agli appalti nella difesa in prodotti fabbricati in Europa, rappresentano un passo importante verso una maggiore competitività della base industriale e tecnologica della difesa europea. Tuttavia, per realizzare questi obiettivi, sarà necessario un incremento delle risorse e un coordinamento più efficace tra i paesi membri.

Ad oggi, l'UE è fortemente dipendente da Paesi extraeuropei per l'acquisto di attrezzature per la difesa, in particolare dagli Stati Uniti. Le risorse messe a disposizione per promuovere iniziative di ricerca e sviluppo collaborative nella difesa, inoltre, sono limitate e sottodimensionate rispetto ad altri Paesi

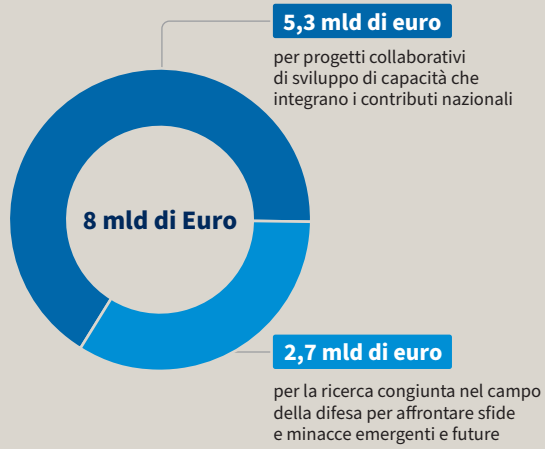
Acquisti in attrezzature per la difesa da parte dell'UE per provenienza
(% sul totale), febbraio 2022 - giugno 2023



Acquisti extra-UE in attrezzature per la difesa da parte dell'UE per Paese
(% sul totale), febbraio 2022 - giugno 2023



Risorse del Fondo Europeo per la Difesa (EDF)
(valori assoluti), 2021-2027



In termini di confronto, le risorse per il budget federale USA nel 2024 per la R&S sono pari a $210 miliardi, **di cui $97 miliardi destinate alla difesa**

Figura 7. Acquisti in attrezzature per la difesa da parte dell'UE per provenienza (grafico a sinistra, % sul totale), febbraio 2022 – giugno 2023 e Risorse del Fondo Europeo per la Difesa (grafico a destra, miliardi di euro), 2021-2027.

Fonte: TEHA Group su dati IRIS, Consiglio europeo e Commissione europea, 2024.

Ad oggi, l'UE dipende in modo significativo dai paesi extra-europei per l'acquisto di attrezzature per la difesa. Dei circa **100 miliardi** di euro di spesa militare addizionale introdotti o annunciati dai Paesi UE dallo scoppio della guerra in Ucraina a giugno 2023, il **78%** è stato **utilizzato per acquistare armamenti da paesi extraeuropei**. Gli Stati Uniti sono il principale fornitore, rappresentando l'80% degli acquisti extra-UE in attrezzature per la difesa[70].

In questo scenario, le risorse allocate dall'UE per promuovere iniziative collaborative di ricerca e sviluppo nel settore della difesa sono limitate e sottodimensionate rispetto a quelle di altri paesi. Il **Fondo Europeo per la Difesa** (FED), istituito nel 2021, per sostenere la ricerca e lo sviluppo collaborativo nel campo della difesa e promuovere una base industriale della difesa innovativa e competitiva, ha un budget contenuto. Il FED dispone di circa **8 miliardi di euro per il periodo 2021-2027**, con 5,3 miliardi di euro destinati a progetti collaborativi di sviluppo delle capacità che integrano i contributi nazionali e 2,7 miliardi di euro destinati alla ricerca congiunta nel campo della difesa per affrontare sfide e minacce emergenti e future. Questa **capacità è limitata se paragonata agli Stati Uniti**, dove le risorse proposte per il budget federale 2024 per la R&S **destinata alla difesa sono pari a $97 miliardi**.

Negli Stati Uniti, inoltre, esistono diverse agenzie dedicate al supporto dell'innovazione in settori strategici per la superiorità tecnologica del Paese, tra cui la Defense Advanced Research Projects Agency (DARPA), con una dotazione per il 2024 di $4,122 miliardi, che finanzia e gestisce progetti di ricerca e sviluppo per far progredire le capacità tecnologiche delle forze armate statunitensi, e l'Office of the Under Secretary of Defense for Research and Engineering, che supervisiona la ricerca, l'ingegneria e lo sviluppo tecnologico all'interno del Dipartimento della Difesa, coordinando gli sforzi tra i vari rami e agenzie.

In UE, inoltre, **a marzo 2024 è stata presentata la prima strategia industriale europea della difesa (EDIS),** che propone di istituire il Programma europeo per l'Industria della difesa (EDIP) per rafforzare la competitività della base industriale e tecnologica di difesa europea (EDTIB). Entro il 2030, i Paesi dell'UE sono invitati ad acquistare almeno il 40% delle attrezzature per la difesa in modo collaborativo (vs 18% oggi), a provvedere affinché il valore degli scambi commerciali intra-UE nel settore della difesa rappresenti almeno il 35% del valore del mercato della difesa dell'UE (vs 15% oggi) e a spendere almeno il 50% del loro bilancio per gli appalti nella difesa in prodotti fabbricati in Europa, aumentando al 60% entro il 2035 (vs 22% oggi). Il sostegno finanziario aggiuntivo sarà pari a **1,5 miliardi di euro per il periodo 2025-2027**, **un valore circa 200 volte inferiore rispetto al totale investito dai 27 Paesi UE nel 2023 in spesa militare**, pari a quasi 300 miliardi di euro[71].

70 Fonte: TEHA Group su dati IRIS, 2024.

71 Fonte: TEHA Group su dati Commissione europea, 2024.

DEBOLEZZA 5

Social Acceptance

4.6 Social Acceptance

Una delle debolezze strutturali della difesa europea è la scarsa accettazione sociale, che varia significativamente tra gli Stati membri. Questa mancanza di consenso pubblico rappresenta un ostacolo alla capacità del settore della difesa di attrarre nuovi talenti e di collaborare efficacemente con il settore privato e l'accademia. La percezione negativa del pubblico nei confronti del settore della difesa ha portato diverse aziende di alta tecnologia a rifiutare lo sviluppo di prodotti per uso militare, influenzate dalle opinioni pubbliche prevalenti.

In uno scenario geopolitico internazionale sempre più multipolare e caratterizzato da minacce crescenti, la difesa riveste un ruolo fondamentale nella protezione degli interessi europei. Gli investimenti in difesa, inoltre, hanno generato innovazioni tecnologiche che sono diventate essenziali per la società moderna. Tecnologie come Internet, il GPS, i droni e i laser, originariamente sviluppate per scopi militari, sono ora diffuse nella vita quotidiana e utilizzate in vari settori, dalla navigazione e comunicazione alla medicina e alla logistica.

La difesa è anche oggetto di social acceptance: l'80% dei cittadini UE è favorevole all'aumento della cooperazione in materia di difesa, ma la quota scende al 66% in fatto di incremento della spesa per la difesa (con notevoli differenze tra gli Stati Membri)

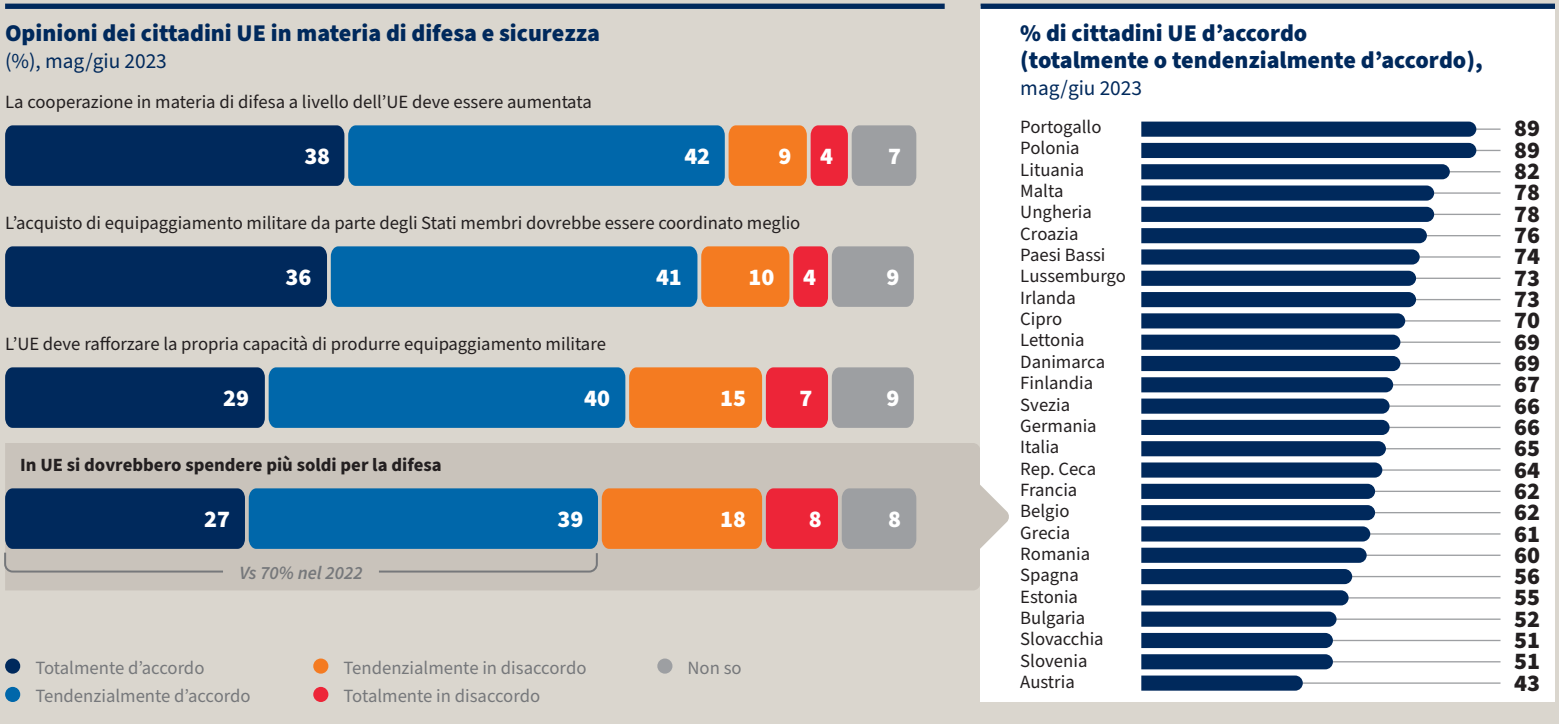


Figura 8. Opinioni dei cittadini UE in materia di difesa e sicurezza (valori percentuali), maggio/giugno 2023.

Fonte: TEHA Group su dati Eurobarometro, 2024.

Sebbene l'80% dei cittadini dell'Unione Europea sia favorevole all'aumento della cooperazione in materia di difesa, **il supporto per l'incremento della spesa per la difesa scende al 66%**. In particolare, meno del 30% dei cittadini europei è totalmente d'accordo sul fatto che l'UE dovrebbe spendere maggiori risorse per la difesa, mentre il 39% è tendenzialmente d'accordo. Il sostegno alla cooperazione in materia di difesa, inoltre, varia significativamente tra gli Stati Membri. Paesi come il Portogallo e la Polonia mostrano un elevato grado di consenso, con l'89% dei cittadini totalmente o tendenzialmente d'accordo. Al contrario, l'Austria presenta il livello più basso di consenso, con solo il 43% dei cittadini a favore. L'Italia si posiziona nella seconda metà della classifica, con il 65% dei cittadini totalmente o tendenzialmente d'accordo ad aumentare la spesa per la difesa[72].

La scarsa accettazione sociale nel settore della difesa non è limitata all'UE. Anche negli Stati Uniti, **diverse aziende di alta tecnologia hanno rifiutato di sviluppare prodotti nel settore della difesa a causa delle posizioni dell'opinione pubblica**. Un esempio è **Boston Dynamics**, che ha scritto una lettera aperta intitolata "*I robot general purpose non dovrebbero essere armati*", impegnandosi a non armare le soluzioni robotiche. Inoltre, le alleanze tecnologiche con la difesa sono spesso oggetto di critica: ad esempio, i dipendenti di **Google** e **Palantir** hanno protestato contro i contratti delle aziende per cui lavorano con Israele. **Questa tendenza incide anche sui tassi di retention dei dipendenti nel settore aerospaziale e della difesa**, con una forza lavoro in continuo invecchiamento. Negli Stati Uniti, ad esempio, il tasso di turnover dei dipendenti nel settore aerospaziale e della difesa è aumentato del 24,5% dal 2021 al 2022, passando dal 5,7% al 7,1%. Inoltre, il 29% della forza lavoro in questo settore in US ha più di 55 anni, creando un potenziale vuoto di 3,5 milioni di lavoratori entro il 2026 al momento del pensionamento. Questo nonostante le retribuzioni siano del 40% superiori alla media nazionale[73].

Nonostante le controversie, **gli investimenti in difesa hanno portato a innovazioni centrali per la società**. Tecnologie come **Internet, GPS, droni e laser**, originariamente sviluppate per scopi militari, sono diventate fondamentali per molti aspetti della vita quotidiana. Internet, inizialmente sviluppato per scopi militari, è ora uno strumento essenziale per tutti gli ambiti della vita quotidiana. Il GPS, creato per la navigazione militare, è ora indispensabile per la navigazione civile. I droni, sviluppati per la ricognizione militare, sono utilizzati in campi civili come la ricerca e il soccorso, la fotografia aerea e la consegna di pacchi. Infine, i laser, originariamente sviluppati per applicazioni militari, hanno numerosi utilizzi medici, inclusa la chirurgia per la correzione della vista e le procedure minimamente invasive.

72 Fonte: TEHA Group su dati Eurobarometro, 2024.

73 Fonte: TEHA Group su dati Aerospace Industry Association, 2024.

Proposte per rafforzare lo sviluppo delle tecnologie digitali per la difesa

CAPITOLO 5

Il quinto capitolo presenta le proposte necessarie per **potenziare il posizionamento dell'Europa nella leadership internazionale** relativamente allo sviluppo di innovazione di frontiera e di tecnologie digitali per la difesa e, più in generale, per dotarla di autonomia strategica nella più ampia gestione della difesa a livello comunitario. Tali proposte sono scaturite dal lavoro di analisi e di confronto con gli stakeholder coinvolti.

Il ritardo accumulato nel settore delle tecnologie digitali e nella governance della difesa rappresenta un rischio significativo per la tenuta della democrazia e la prosperità economica europea.

In questo contesto, è utile che l'Unione Europea segua tre linee di indirizzo strategiche fondamentali:

1. Definire una chiara **governance europea per la difesa**, che sia capace di esprimersi sul piano internazionale con una voce univoca;
2. Riprendere e ampliare il più possibile la **sovranità industriale** nel campo della difesa, dove un forte sviluppo digitale è cruciale;
3. Fare leva sugli **investimenti nella difesa** per costruire filiere europee delle tecnologie digitali, promuovendo la crescita economica e il perseguimento di un'autonomia strategica.

N.B. Le proposte 3,5 e 8 sono strettamente legate tra loro.

Prima di addentraci nella descrizione di dettaglio delle proposte, è doveroso fare una premessa sugli strumenti messi a disposizione dall'Unione Europea, sui fondi destinati al supporto dell'industria e dell'innovazione e sulla governance degli stessi, che risultano attualmente frammentati e caratterizzati da sovrapposizioni e inefficienze. È essenziale intraprendere una profonda razionalizzazione delle strutture esistenti e unificare i vari organismi sotto una governance centralizzata per garantire un utilizzo più strategico e coordinato delle risorse.

Proposta 1

La **proposta 1** è, infatti, trasversale e alla base di tutte le altre e si focalizza sulla necessità di riorganizzare e ottimizzare il quadro istituzionale e finanziario della difesa europea, migliorando la coerenza, l'efficacia e l'efficienza delle politiche di difesa e sicurezza.

Attualmente, **diverse strutture e programmi operano in parallelo con obiettivi spesso sovrapposti**. Tra questi, il Capability Development Plan (CDP) fornisce una visione a lungo termine delle capacità militari necessarie, mentre la Cooperazione Strutturata Permanente (PESCO) promuove progetti di cooperazione tra gli Stati membri per sviluppare capacità comuni. L'Agenzia Europea per la Difesa (EDA) supporta questi sforzi con attività di ricerca e sviluppo, ma il coordinamento tra questi organismi risulta spesso complesso e inefficiente. Il Fondo Europeo per la Difesa (EDF) rappresenta un importante strumento finanziario per sostenere progetti di ricerca e sviluppo nel settore della difesa. Tuttavia, la sua gestione è spesso frammentata e non sempre allineata con le altre iniziative europee. Il Programma Europeo di Sviluppo Industriale della Difesa (EDIDP), il Programma Industriale europeo per la difesa (EDIP) e il Programma Spaziale dell'UE sono ulteriori esempi di iniziative che necessitano di una maggiore integrazione per evitare duplicazioni e migliorare l'efficacia dei finanziamenti.

Per affrontare le nuove sfide, si propone un **coordinamento centrale di tutti gli organismi chiave della difesa europea** (tra cui il CDP, PESCO, EDA, EDF, EDIDP e il Programma Spaziale dell'UE), che venga realizzato dal Commissario alla Difesa (come suggerito in Proposta 2). Questo coordinamento centralizzato permetterà di:

1. Coordinare le politiche e le strategie di difesa.
2. Ottimizzare l'allocazione delle risorse.
3. Migliorare la trasparenza e la rendicontazione.
4. Promuovere la collaborazione tra Stati membri.
5. Semplificare le strutture burocratiche.
6. Garantire una visione a lungo termine.

La riorganizzazione della governance, l'integrazione dei programmi di finanziamento e il rafforzamento delle strutture esistenti sono essenziali in questo mutato scenario internazionale e permetteranno di migliorare l'efficienza e l'efficacia delle politiche di difesa europee, garantendo una risposta coordinata e integrata alle minacce globali.

Proposta 2

Dotare l'Europa di uno strumento di «total security»

Per garantire una protezione completa degli interessi europei, è fondamentale inserire la difesa comune come priorità nel mandato della prossima Commissione Europea. La nomina di un **Commissario europeo per la difesa**, che lavori in stretta collaborazione con l'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, è essenziale. L'istituzione di un **European Security Council** faciliterà la consultazione e il coordinamento in ambito di politica estera, sicurezza economica, energetica, militare, sociale e tecnologica, in modo che vengano monitorate regolarmente le possibili minacce esterne e interne agli interessi dell'Unione Europea e che vengano intraprese rapidamente azioni mirate e integrate per rispondervi. È, inoltre, auspicabile una progressiva convergenza verso una politica comune di intelligence, funzionale all'approccio di total security; spesso, le informazioni di intelligence non vengono condivise, perché legate alla visione di Stato che poco si integra in un processo di integrazione europea.

Lo European Security Council dovrà essere un organo consultivo e di indirizzo che riunirà rappresentanti di tutti i settori coinvolti nella protezione degli interessi europei, alla stregua di come è organizzato il National Security Council americano. Questo consiglio fornirà una valutazione accurata delle minacce, combinando informazioni e prospettive provenienti dai diversi stakeholder, e proporrà azioni di policy e raccomandazioni strategiche per contrastarle. Ad esempio, in ambito economico, potrà affrontare le minacce alle catene di approvvigionamento globali, garantire la sicurezza energetica europea, oppure proteggere la capacità di innovazione tecnologica delle aziende europee.

Come già sollevato in precedenza, è necessario trasferire ai cittadini europei l'importanza di dotare l'Unione di uno strumento, come lo European Security Council, in grado di tutelare gli interessi comunitari a più livelli (ad es. difensivo, economico, energetico, sociale).

Inoltre, è essenziale che il Consiglio sia dotato di strumenti per l'analisi delle minacce in tempo reale, utilizzando tecnologie avanzate di intelligenza artificiale e big data. L'uso di queste tecnologie permetterà di identificare rapidamente le potenziali minacce e di sviluppare strategie di risposta efficaci. La protezione degli interessi comunitari richiede un approccio di sistema che integri tutte le dimensioni della sicurezza, garantendo una risposta coordinata e integrata.

In relazione all'Italia, lo strumento che cura gli interessi nazionali è il Consiglio Supremo di Difesa che, tuttavia, presenta alcune criticità nell'efficacia del proprio funzionamento.
Il Consiglio Supremo di Difesa è un organo di rilevanza costituzionale che si configura come uno strumento di altissima consulenza del Presidente della Repubblica preposto all'esame dei problemi generali politici e tecnici attinenti alla sicurezza e alla difesa nazionale.

Questo organo ha un potere decisionale ridotto e, negli anni, si è limitato alla condivisione di informazioni tra i membri che lo compongono, senza prevedere delle vere e proprie procedure per adottare decisioni vincolanti.

Sarebbe opportuno potenziare il Consiglio Supremo di Difesa, trasformandolo da organo consultivo a organo di indirizzo, e promuovere una integrazione e coordinamento tra gli strumenti di questo tipo presenti nei singoli Stati membri, a servizio dello European Security Council.

Proposta 3

Rafforzare lo strumento militare comune europeo

La gestione centralizzata delle forze armate europee è cruciale. Come previsto dalla Strategic Compass, è necessario rendere **pienamente operativa entro il 2025 l'EU Rapid Deployment Capacity** (RDC), che per il comando e controllo potrà avvalersi della Military Planning and Conduct Capability (MPCC) una volta raggiunta anch'essa la piena capacità operativa. La forza di intervento rapida dell'UE è stata creata nel 2022 per sopperire ad alcune lacune dei Battlegroups che, a causa di impedimenti politici ed economici, in 17 anni non sono mai stati impiegati.

Dotare l'RDC di governance e strumenti autonomi permetterà di semplificare i processi decisionali e garantire un bilancio dedicato per finanziamenti coerenti. Occorre **allineare le forze di intervento rapido alle 60.000 unità previste dall'Helsinki Headline Goal del 1999**, per garantire una capacità di risposta rapida ed efficace.

Il RDC deve essere dotato di una struttura di governance che gli garantisca autonomia strategica e funzionale. Questo include la semplificazione dei processi decisionali, riducendo i livelli burocratici coinvolti e sviluppando mandati pre-approvati per accelerare il dispiegamento delle forze. Inoltre, è necessario stabilire un quartier generale operativo permanente per garantire continuità e competenza nelle operazioni.

Un altro aspetto cruciale è il finanziamento: è necessario un aumento del bilancio dello European Peace Facility (EPF) per garantire il finanziamento adeguato a consentire l'impiego tempestivo della RDC negli scenari operativi. Questo permetterà di evitare interruzioni nelle operazioni e di mantenere un alto livello di prontezza operativa. Come anticipato, la MPCC, opportunamente staffata ed equipaggiata, dovrebbe diventare la struttura di comando e controllo preferenziale, mentre, il Parlamento europeo dovrebbe avere un ruolo di supervisione delle operazioni del RDC, garantendo la responsabilità democratica delle decisioni prese.

Il rafforzamento del RDC non deve limitarsi all'aspetto militare, ma deve includere anche componenti civili e di supporto logistico. Questo permetterà di affrontare una vasta gamma di operazioni, dai compiti umanitari alle missioni di combattimento e gestione delle crisi. In questo contesto, la collaborazione con altre agenzie europee e internazionali sarà fondamentale per garantire una risposta integrata ed efficace alle diverse tipologie di minacce.

Non da ultimo, si renderà necessario investire nella formazione e nell'addestramento delle forze del RDC. Questo non solo migliorerà le competenze tecniche e operative, ma favorirà anche una maggiore interoperabilità tra le diverse forze armate degli Stati membri: programmi di addestramento congiunti e scambi di personale contribuiranno a creare una cultura comune della difesa e a migliorare la coesione delle forze europee.

Proposta 4

Promuovere l'adozione di requisiti comuni e programmi industriali cooperativi tra gli Stati membri

Rafforzare gli strumenti europei per la cooperazione nella difesa, come il Capability Development Plan (CDP) e la Cooperazione Strutturata Permanente (PESCO), è fondamentale. Aumentare le risorse del Fondo Europeo per la Difesa (EDF) per progetti di ricerca e sviluppo capacitivo congiunto tra Stati membri e industrie europee contribuirà a migliorare l'interoperabilità e l'efficienza.

L'adozione di **requisiti comuni tra gli Stati membri** è cruciale per migliorare l'interoperabilità delle forze armate e ridurre i costi di sviluppo e produzione dei sistemi di difesa. Il CDP, attraverso una revisione annuale coordinata sulla difesa (Coordinated Annual Review on Defence, CARD), permette di identificare le capacità prioritarie e di definire requisiti comuni. Questo processo deve essere ulteriormente rafforzato e integrato con la Cooperazione Strutturata Permanente (PESCO), che promuove la cooperazione a lungo termine tra gli Stati membri.

Aumentare le risorse del Fondo Europeo per la Difesa (EDF) è essenziale per realizzare progetti di ricerca e sviluppo congiunti tra gli Stati membri e le industrie europee. Attualmente, il budget dell'EDF è di 8 miliardi di euro per il periodo 2021-2027, ma è necessario incrementarlo nel prossimo Multiannual Financial Framework europeo 2028-2034. Questo permetterà di finanziare progetti più ambiziosi e di lungo termine, garantendo l'autonomia strategica dell'Europa.

Inoltre, è fondamentale incentivare la cooperazione tra Stati Membri nell'acquisto di prodotti comuni. Attualmente, solo il 18% del valore degli acquisti di prodotti per la difesa è sviluppato congiuntamente. L'obiettivo è raggiungere il 40% entro il 2030, come indicato dal Programma europeo per l'industria della difesa (EDIP). Questo richiede un impegno congiunto da parte degli Stati membri e il supporto finanziario dell'UE.

Un'altra iniziativa importante è la creazione di un **budget comunitario per lo sviluppo di sistemi digitali interoperabili**. Questo garantirà che le diverse piattaforme di difesa utilizzino tecnologie compatibili, migliorando l'efficienza operativa e riducendo i costi di integrazione. Inoltre, l'adozione di standard comuni per le tecnologie digitali favorirà lo **sviluppo di un digital continuum** che permetterà alle forze armate europee di operare in modo coordinato e integrato.

Infine, è necessario **promuovere la cooperazione con l'Organizzazione Congiunta per la Cooperazione in Materia di Armamenti** (OCCAR). Nonostante non sia un organismo UE, l'OCCAR gestisce 20 programmi cooperativi e può essere incaricata dalla Commissione Europea di supervisionare e coordinare progetti europei. La collaborazione con l'OCCAR permetterà di sfruttare le sue competenze e la sua esperienza nella gestione di programmi complessi, migliorando l'efficienza e l'efficacia dei progetti di difesa europei.

Proposta 5

Favorire la creazione di sinergie tra aziende della difesa europee

Valutare la prontezza dell'industria della difesa europea, identificando le dipendenze lungo le catene del valore e colmando i gap industriali, è essenziale. L'aggregazione e la cooperazione industriale devono essere incentivate per lo sviluppo e la produzione congiunta di prodotti per la difesa comuni, migliorando così la capacità produttiva e l'innovazione.

L'Unione Europea deve adottare una **strategia per valutare la prontezza dell'industria della difesa europea**, considerando sia la capacità di sviluppo che quella produttiva. Questo processo deve tenere conto dei diversi scenari di evoluzione del quadro geopolitico e tecnologico, identificando le potenziali dipendenze lungo le catene del valore e i gap industriali da colmare. Utilizzare strumenti ad hoc come il **TEHA - Digital Technologies Security Index** permette di individuare i punti di debolezza a cui è esposta l'UE e di intraprendere azioni concrete per migliorarli.

Incentivare l'aggregazione e/o la cooperazione industriale a livello europeo è essenziale per sviluppare e produrre congiuntamente prodotti per la difesa comuni a più Stati Membri. Questo approccio è promosso dal nuovo framework SEAP (Structure for European Armament Programmes) nell'ambito del Programma europeo per l'industria della difesa (EDIP). La cooperazione industriale permetterà di sfruttare le economie di scala, riducendo i costi di sviluppo e produzione e migliorando l'efficienza complessiva.

È inoltre importante creare incentivi finanziari per promuovere la cooperazione tra le aziende della difesa europee. Questo può essere realizzato attraverso la condivisione dei costi di sviluppo e produzione, l'accesso a finanziamenti agevolati e la promozione di partenariati pubblico-privati. Il supporto della Commissione Europea e degli Stati membri sarà fondamentale per creare un ambiente favorevole alla cooperazione industriale.

Un altro aspetto cruciale è la promozione dell'innovazione nelle aziende della difesa. Questo può essere realizzato attraverso **programmi di ricerca e sviluppo congiunti, l'accesso a fondi europei per l'innovazione e la collaborazione con istituti di ricerca e università**. Promuovere l'innovazione permetterà alle aziende europee di sviluppare tecnologie all'avanguardia e di mantenere la loro competitività a livello globale.

Infine, è essenziale creare un **quadro normativo che favorisca la cooperazione industriale** e riduca le barriere burocratiche e regolamentari. Questo include l'armonizzazione delle normative nazionali, la semplificazione delle procedure di autorizzazione e l'eliminazione delle barriere protezionistiche. Un quadro normativo favorevole permetterà alle aziende di collaborare più facilmente e di sviluppare prodotti comuni in modo efficiente.

Proposta 6

Limitare l'utilizzo di misure protezionistiche nel mercato interno europeo

Limitare l'uso dell'articolo 346 del Trattato sul Funzionamento dell'Unione Europea (TFEU) per evitare il protezionismo che ostacola la cooperazione in progetti di sviluppo e produzione. Una corretta applicazione di questo articolo promuoverà l'efficienza della spesa militare e l'interoperabilità tra gli Stati membri, favorendo lo **sviluppo di un'industria europea della difesa competitiva a livello globale**.

L'articolo 346 del TFEU consente agli Stati membri di adottare misure necessarie per la protezione degli interessi essenziali della loro sicurezza. Tuttavia, questo articolo può essere utilizzato a scopi protezionistici, ostacolando la cooperazione in progetti congiunti di sviluppo e produzione. Ad esempio, gli Stati membri possono utilizzare l'articolo 346 per limitare l'acquisizione di strumenti di difesa, riducendo l'efficienza della spesa militare e compromettendo la capacità dell'UE di rispondere efficacemente alle minacce alla sicurezza.

Per limitare l'uso improprio dell'articolo 346, è necessario stabilire criteri chiari e trasparenti per la sua applicazione. Questo include la definizione di cosa costituisce un interesse essenziale di sicurezza e la creazione di meccanismi di supervisione per garantire che l'articolo sia utilizzato in modo appropriato. La Commissione Europea e gli Stati membri devono collaborare per sviluppare queste linee guida e monitorare l'applicazione dell'articolo 346.

Un altro aspetto importante è la promozione della trasparenza nelle decisioni relative all'uso dell'articolo 346. Gli Stati membri devono rendere pubbliche le motivazioni per l'applicazione dell'articolo e garantire che queste decisioni siano soggette a revisione e controllo. Questo non solo migliorerà la fiducia nel processo decisionale, ma ridurrà anche le possibilità di utilizzo protezionistico dell'articolo 346.

Limitare il protezionismo nel mercato interno europeo è cruciale per promuovere la cooperazione in progetti di sviluppo e produzione. Un mercato interno integrato e competitivo permetterà alle aziende europee di collaborare più facilmente e di sviluppare tecnologie all'avanguardia. Questo non solo migliorerà l'efficienza della spesa militare, ma favorirà anche lo sviluppo di un'industria europea della difesa competitiva a livello globale.

Proposta 7

Reinterpretare i parametri di sostenibilità degli investimenti in difesa per incentivare la partecipazione di investitori privati e istituzionali

Bilanciare i criteri ESG negli strumenti finanziari con le esigenze dell'industria della difesa è fondamentale. Formalizzare un quadro ESG specifico per il settore della difesa e incentivare il supporto di investitori istituzionali contribuirà a ridurre i rischi e a promuovere standard elevati di trasparenza e rendicontazione.

La sostenibilità degli investimenti nella difesa richiede un equilibrio tra gli obiettivi di sostenibilità ambientale, sociale e di governance (ESG) e le esigenze specifiche del settore della difesa. Un quadro ESG specifico per il settore della difesa deve distinguere tra i diversi tipi di attività di difesa, come armamenti difensivi e offensivi, e garantire il rispetto del diritto internazionale. Allo stesso tempo, deve **incentivare standard elevati di trasparenza e rendicontazione**, fornendo informazioni dettagliate sugli impatti sociali e ambientali delle operazioni e sugli sforzi per mitigare gli impatti negativi.

Incentivare il supporto di investitori istituzionali al finanziamento delle industrie della difesa è essenziale per ridurre il rischio sostenuto dagli investitori privati e aumentare ulteriormente i loro investimenti. Questo può essere realizzato attraverso la creazione di strumenti finanziari specifici per il settore della difesa, come fondi di investimento tematici e obbligazioni green legate a **progetti di difesa sostenibile**.

Un primo passo importante è stato l'aggiornamento, a maggio 2024, dei beni dual use ammissibili ai finanziamenti della Banca Europea per gli Investimenti (BEI) e l'abolizione della soglia minima di ricavi attesi da applicazioni civili o della quota di utenti civili all'interno di investimenti legati alla difesa. Il prossimo passo dovrà essere l'**eliminazione del concetto di dual-use nei finanziamenti per la difesa ammissibili dalla BEI**, a favore di una valutazione del valore strategico degli investimenti nella difesa.

Per promuovere la sostenibilità degli investimenti nella difesa, è essenziale anche adottare misure per migliorare la trasparenza e la rendicontazione delle pratiche ESG da parte delle aziende del settore. Questo può includere l'adozione di standard internazionali di rendicontazione ESG, la pubblicazione di rapporti annuali sulle performance ESG e la creazione di meccanismi di supervisione indipendenti per monitorare il rispetto degli standard ESG.

Infine, è necessario promuovere la cooperazione internazionale per affrontare le sfide globali della sostenibilità nel settore della difesa. Questo può includere la collaborazione con organizzazioni internazionali, la partecipazione a iniziative globali di sostenibilità e la condivisione di best practice con altri paesi. La cooperazione internazionale permetterà di affrontare le sfide globali della sostenibilità in modo più efficace e di promuovere un approccio coordinato e integrato.

Proposta 8

Dotare l'Europa di una strategia a lungo termine per garantire autonomia strategica e sovranità tecnologica digitale per la difesa

Adottare una strategia a lungo termine per la base tecnologica e industriale della difesa europea è essenziale. Un piano europeo per lo sviluppo delle tecnologie digitali per la difesa, supportato da risorse comunitarie e governance centralizzata, garantirà l'autonomia strategica e l'innovazione tecnologica.

L'adozione di una strategia a lungo termine per l'autonomia strategica e la sovranità tecnologica digitale richiede un approccio integrato e coordinato a livello europeo. Questo include la definizione di un piano europeo per lo sviluppo e la produzione delle tecnologie digitali per la difesa, comune a tutti i Paesi Membri e dotato di risorse comunitarie. Un esempio è l'**ampliamento del Fondo Europeo della Difesa**, che attualmente dispone di un budget di 8 miliardi di euro per il periodo 2021-2027, con l'obiettivo di aumentare significativamente il budget nel prossimo Multiannual Financial Framework europeo 2028-2034.

L'**utilizzo di strumenti finanziari innovativi, come gli Eurobond**, può essere una soluzione per finanziare un budget della difesa europea a supporto di progetti di ricerca e sviluppo in tecnologie digitali per la difesa. Questo approccio permetterà di raccogliere capitali sul mercato a costi competitivi e di creare un ritorno economico superiore al costo del capitale raccolto. Gli **Eurobond potrebbero essere utilizzati per finanziare progetti strategici**, come lo sviluppo di **sistemi di intelligenza artificiale avanzata**, **tecnologie di cybersecurity** e **piattaforme di comunicazione sicura**.

Incentivare gli investimenti di venture capital nelle startup del settore della difesa è un'altra componente chiave della strategia. Un esempio di successo è il «NATO Innovation Fund», il primo fondo multi-sovrano di venture capital al mondo, partecipato da 24 Paesi dell'Alleanza Atlantica, con 1 miliardo di euro in dotazione. A giugno 2024, il fondo ha investito in quattro startup (ARX Robotics, Fractile AI, iCOMAT e Space Forge), dimostrando il potenziale di questo approccio per promuovere l'innovazione nel settore della difesa.

Per garantire l'autonomia strategica e la sovranità tecnologica digitale, è essenziale anche promuovere la collaborazione tra gli Stati membri e le istituzioni europee. Questo include la creazione di **partenariati pubblico-privati**, la promozione di programmi di ricerca e sviluppo congiunti e la condivisione delle migliori pratiche e delle tecnologie all'avanguardia.

Un altro aspetto importante è la formazione e lo sviluppo delle competenze nel settore delle tecnologie digitali per la difesa. Questo richiede programmi di formazione specializzati, la promozione di percorsi di carriera nel settore della difesa e l'integrazione di competenze tecnologiche avanzate nelle forze armate europee.

Infine, è fondamentale adottare misure per proteggere la proprietà intellettuale e garantire la sicurezza delle tecnologie sviluppate, attraverso un quadro normativo robusto per la protezione dei diritti di proprietà intellettuale, la promozione di pratiche di cybersecurity avanzate e la collaborazione con partner internazionali per prevenire il furto di tecnologie sensibili.

Proposta 9

Rafforzare l'integrazione e la cooperazione in ambito spaziale

Il settore spaziale rappresenta un quadrante geopolitico cruciale per il futuro. È necessario integrare il piano europeo per le tecnologie digitali della difesa con iniziative relative alle tecnologie spaziali, potenziando il Fondo Europeo della Difesa e il Programma Spaziale dell'UE.

Il settore spaziale è destinato a diventare un elemento chiave della geopolitica globale, con implicazioni significative per la sicurezza, l'economia e la politica. In quest'ottica, l'Europa non può permettersi di restare indietro ed essere dipendente da tecnologie extra-europee. L'integrazione delle iniziative relative alle tecnologie spaziali con il piano europeo per le tecnologie digitali della difesa è essenziale per garantire l'autonomia strategica e la sovranità tecnologica dell'Europa.

Attualmente, il Fondo Europeo della Difesa dispone di un budget di 8 miliardi di euro per il periodo 2021-2027, ma solo una piccola parte di questi fondi è destinata a progetti spaziali. È necessario **potenziare il Fondo Europeo della Difesa e aumentare il numero di progetti spaziali finanziati**, garantendo risorse adeguate allo sviluppo delle tecnologie spaziali. Allo stesso tempo, il Programma Spaziale dell'UE, con un budget di circa 14,8 miliardi di euro per il periodo 2021-2027, deve essere ampliato per sostenere una maggiore cooperazione e integrazione delle tecnologie spaziali.

Promuovere e intensificare le partnership tra paesi europei è fondamentale per rafforzare la cooperazione spaziale. Questo include la promozione della Cooperazione Strutturata Permanente (PESCO) e garantire un ruolo guida per l'Agenzia Spaziale Europea (ESA). L'ESA ha accumulato un'esperienza e un know-how significativi nel campo delle tecnologie spaziali e può svolgere un ruolo chiave nel coordinare e promuovere la cooperazione spaziale europea.

Un'iniziativa importante è l'**istituzione di un European Space Force Command**, che offra un **coordinamento e una governance efficiente ed efficace per le operazioni spaziali europee in tema di difesa**. Questo comando spaziale sarà responsabile della pianificazione, del coordinamento e dell'esecuzione delle operazioni spaziali, garantendo una risposta rapida ed efficace alle minacce spaziali. Inoltre, il comando spaziale potrà collaborare strettamente con il RDC e altre forze armate europee, integrando le capacità spaziali nelle operazioni di difesa.

Per promuovere l'innovazione nel settore spaziale è, infine, essenziale incentivare gli investimenti in ricerca e sviluppo. Questo include la promozione di programmi di ricerca congiunti, il sostegno alle startup e alle PMI che sviluppano tecnologie spaziali e la creazione di partenariati pubblico-privati. Inoltre, è necessario adottare politiche di supporto per facilitare l'accesso ai finanziamenti e ridurre le barriere burocratiche e regolamentari.

Proposta 10

Creare dialogo tra mondo dell'innovazione e della difesa

Promuovere un **dialogo tra il settore della ricerca e dell'innovazione e la difesa è essenziale per accelerare l'innovazione tecnologica**. Modelli di collaborazione tra università e Istituzioni della Difesa, percorsi per integrare talenti e mappatura delle aziende europee contribuiranno a rafforzare la capacità difensiva.

Il dialogo tra il settore della ricerca e dell'innovazione e la difesa è fondamentale per garantire che i progressi scientifici siano applicati in modo strategico per rafforzare la capacità difensiva. Promuovere **modelli di collaborazione più stretti tra università e Istituzioni della Difesa** permetterà di accelerare l'innovazione tecnologica, ottimizzare le risorse e garantire che i progressi scientifici siano applicati in modo efficace. Questi modelli di collaborazione devono prevedere adeguati livelli di tutela per i temi di natura militare, ma allo stesso tempo favorire dinamiche tipiche del mondo dell'innovazione.

Un esempio di iniziativa è la promozione di programmi di ricerca congiunti tra università e Istituzioni della Difesa, che permettano di sviluppare nuove tecnologie e soluzioni innovative. Questi programmi possono includere **progetti di ricerca su tecnologie emergenti**, come l'intelligenza artificiale, la cybersecurity, i sistemi autonomi e le tecnologie quantistiche. La collaborazione tra ricercatori e esperti militari garantirà che le tecnologie sviluppate rispondano alle esigenze specifiche del settore della difesa.

Favorire **percorsi per integrare talenti nel settore della difesa** è un'altra componente chiave. Questo può includere programmi di formazione specializzati, borse di studio per studenti e ricercatori e programmi di scambio tra università e Istituzioni della Difesa. L'obiettivo è attrarre i migliori talenti nel settore della difesa e garantire che abbiano le competenze necessarie per affrontare le sfide dell'innovazione in ambito militare. Le iniziative strategiche europee per lo sviluppo delle competenze, come il **Pact for Skills**, possono contribuire a creare opportunità di miglioramento delle competenze e riqualificazione per la forza lavoro in UE in ambito aerospazio e difesa.

Effettuare una **mappatura delle aziende europee che possono contribuire all'innovazione della difesa** è essenziale per identificare le capacità esistenti e stimolare l'innovazione. Questo processo permetterà di identificare le aziende più promettenti e di supportarle nello sviluppo di tecnologie avanzate per la difesa. Inoltre, la mappatura permetterà di creare reti di collaborazione tra aziende, università e Istituzioni della Difesa, favorendo lo scambio di conoscenze e competenze.

Un'altra iniziativa importante è l'**istituzione di un Chief Technology Officer** (CTO) della difesa, che guidi l'innovazione tecnologica nel settore e coordini le attività di ricerca, sviluppo e prototipazione. Seguendo l'esempio degli Stati Uniti e del Regno Unito, un CTO della difesa in UE potrebbe svolgere un ruolo chiave come ponte tra le forze armate e le industrie tecnologiche e accademiche, facilitando collaborazioni che possono **accelerare l'innovazione e lo sviluppo di nuove tecnologie**. Il CTO della difesa avrà il compito di definire le priorità tecnologiche, sviluppare strategie di innovazione e garantire il coordinamento tra i vari attori coinvolti.

Per promuovere il dialogo tra innovazione e difesa, è anche importante creare eventi e piattaforme di incontro tra ricercatori, aziende e rappresentanti delle forze armate. Questi eventi possono includere conferenze, workshop, hackathon e competizioni di innovazione, che favoriranno lo scambio di idee e la collaborazione tra i diversi attori.

Bibliografia

- Checkpoint, “2024 Cyber Security Report”, 2024, *https://pages.checkpoint.com/2024-cyber-security-report*.
- Commissione Europea, “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions on Defence of Democracy”, 2023, *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=COM:2023:630:FIN*.
- *Commissione Europea, “*Comunicazione congiunta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Una nuova strategia industriale europea per il settore della difesa: conseguire la prontezza dell’UE attraverso un’industria europea della difesa reattiva e resiliente”, 2024, *https://defence-industry-space.ec.europa.eu/document/download/ad46efd3-9a4a-4d85-b040-4cf7f7c92b6e_en?filename=JOIN_2024_10_1_IT_ACT_part1_v2.pdf*.
- Commissione Europea, “European Defence Fund: Indicative multiannual perspective 2024-2027”, 15 marzo 2024, *https://defence-industry-space.ec.europa.eu/document/download/fe017e8c-1c58-4d39-a8a6-e158542e8a95_en?filename=Indicative%20Multiannual%20Perspective%202024-2027.pdf*.
- Commissione Europea, Joint Research Centre, “The landscape of hybrid threats – A conceptual model – Public version”, 2021, *https://op.europa.eu/en/publication-detail/-/publication/b534e5b3-7268-11eb-9ac9-01aa75ed71a1/language-en.*
- Commissione Europea, “Strategic dependencies and capacities”, 2021, *https://commission.europa.eu/document/download/0a5bdf82-400d-4c9c-ad54-51766e508969_en?filename=swd-strategic-dependencies-capacities_en.pdf&prefLang=it*.
- *Commissione Europea, “Supply chain analysis and material demand forecast in strategic technologies and sectors in the EU – A foresight study”, 2023, https://op.europa.eu/en/publication-detail/-/publication/9e17a3c2-c48f-11ed-a05c-01aa75ed71a1/language-en/format-PDF.*
- Commssione Europea, “EU strategic dependencies and capacities: second stage of in-depth reviews”, 2022, *https://ec.europa.eu/newsroom/cipr/items/738844/en*.
- Commissione Europea, Directorate-General for Defence Industry and Space, “Access to equity financing for European defence SMEs”, 2024, *https://data.europa.eu/doi/10.2889/698738*.
- Congressional Research Service, “Defense Primer: Ballistic Missile Defense”, 30 gennaio 2023, *https://crsreports.congress.gov/product/pdf/IF/IF10541*.

- Congressional Research Service, “Hypersonic Weapons: Background and Issues for Congress”, Agosto 2024, *https://crsreports.congress.gov/product/pdf/R/R45811*.
- Dragos, “OT Cybersecurity: The 2023 Year in review”, febbraio 2024, *https://www.dragos.com/resources/reports/2023-ot-cybersecurity-year-in-review-report/*.
- *Energy Transition Commission, “Material and Resource Requirements for the Energy Transition”, luglio 2023, https://www.energy-transitions.org/wp-content/uploads/2023/08/ETC-Materials-Report_highres-1.pdf.*
- *ENISA,* “ENISA Threat Landscape for DoS Attacks”, 2023, *https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-dos-attacks*.
- ESA, “ESA’s annual space environment report”, 2024, *https://www.sdo.esoc.esa.int/environment_report/Space_Environment_Report_latest.pdf*.
- European Defence Agency, “Annual Report 2023”, 2024, *https://eda.europa.eu/docs/default-source/brochures/qu-aa-24-001-en-n.pdf*.
- European Defence Agency, “2022 Coordinated annual review on defence report”, 2022, *https://eda.europa.eu/docs/default-source/eda-publications/2022-card-report.pdf*.
- European Defence Agency, “Defence data 2022 – Key findings and analysis”, 2023, *https://data.europa.eu/doi/10.2836/50078*.
- European Defence Agency, “The 2023 EU Capability Development Priorities”, 2023, *https://eda.europa.eu/docs/default-source/brochures/qu-03-23-421-en-n-web.pdf*.
- European Parliamentary Research Service, “Improving the quality of public spending in Europe”, 2020, *https://www.dgdi.me/data/publications/eu_ets/cifrel-Improving_the_quality_of_public_spending_in_Europe.pdf*.
- Fortinet, “2024 State of Operational Technology and Cybersecurity Report”, 2024, *https://www.fortinet.com/content/dam/fortinet/assets/reports/report-state-ot-cybersecurity.pdf*.
- Gazzetta Ufficiale della Repubblica Italiana n.159 del 09-07-2024), “DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 20 giugno 2024, n. 99”, pag. 6, *https://www.gazzettaufficiale.it/eli/gu/2024/07/09/159/sg/pdf*.
- IPCC, “Synthesis report of the IPCC sixth assessment report (AR6)”, 2023, *https://report.ipcc.ch/ar6syr/pdf/IPCC_AR6_SYR_LongerReport.pdf*.
- IRIS, “The impact of the war in Ukraine on the European defence market”, Settembre 2023, *https://www.iris-france.org/wp-content/uploads/2023/09/19_ProgEuropeIndusDef_JPMaulny.pdf*.
- Leonardo, “Industrial Plan 2024-2028”, 2024, *https://www.leonardo.com/documents/15646808/28263189/CMD_Final.pdf?t=1710945422583&_gl=1*380vu5*_up*MQ..*_ga*OTgzNDExMDU5LjE3MjQzMjg5Njc.*_ga_WRC29ZGWWH*MTcyNDMyODk2Ni4xLjAuMTcyNDMyODk2Ni4wLjAuMA..*_ga_EX831B1KRH*MTcyNDMyODk2Ni4xLjAuMTcyNDMyODk2Ni4wLjAuMA*.
- NATO, “Defence Expenditure of NATO Countries (2014-2024)”, 2024, *https://www.nato.int/nato_static_fl2014/assets/pdf/2024/6/pdf/240617-def-exp-2024-en.pdf*

- NATO, "Defence expenditure as percentage of GDP NATO total and NATO Europe", 2024, *https://www.nato.int/nato_static_fl2014/assets/pdf/2024/2/pdf/FACTSHEET-NATO-defence-spending-en.pdf.*
- NATO, "NATO Advisory Group on Emerging and disruptive Technologies", 2021, *https://www.nato.int/nato_static_fl2014/assets/pdf/2022/7/pdf/220715-EDT-adv-grp-annual-report-2021.pdf*.
- Oxford Poverty & Human Development Initiative, UNDP, "Global Multidimensional Poverty Index 2023", 2023, *https://hdr.undp.org/system/files/documents/hdp-document/2023mpireporten.pdf*.
- *Presidenza del Consiglio dei Ministri, "Relazione annuale sulla politica dell'informazione e della sicurezza", 2023, https://www.sicurezzanazionale.gov.it/data/cms/posts/933/attachments/711cf87b-1a38-4864-975a-e253a67cbdba/download?view=true.*
- SIPRI, "Trends in World Military Expenditure", 2022, *https://www.sipri.org/sites/default/files/2023-04/2304_fs_milex_2022.pdf.*
- SIPRI, "Trends in World Military Expenditure", 2023, *https://www.sipri.org/sites/default/files/2024-04/2404_fs_milex_2023.pdf.*
- Stato Maggiore della Difesa, "L'impatto delle Emerging & Disruptive Technologies (EDTs) sulla Difesa", 2022, *https://www.difesa.it/assets/allegati/31787/3.concetto_impatto_delle_edt_sulla_difesa_ed._2022.pdf*.
- The European House – Ambrosetti, "La filiera italiana dell'Aerospazio, della Difesa e della Sicurezza", 2018, *https://www.ambrosetti.eu/lo-scenario-di-oggi-e-di-domani-per-le-strategie-competitive-2018/*.
- The European House – Ambrosetti, "Politica estera e difesa comune per l'Europa: sfide e opportunità per l'Italia e l'Unione Europea", 2022, *https://www.ambrosetti.eu/news/perche-politica-estera-e-difesa-comune-europea-sono-unopportunita-per-litalia-e-lue/*.
- Unione Europea, "Decisione (PESC) 2021/698 del Consiglio, del 30 aprile 2021, sulla sicurezza dei sistemi e dei servizi dispiegati, gestiti e utilizzati nell'ambito del programma spaziale dell'Unione che possono incidere sulla sicurezza dell'Unione e che abroga la decisione 2014/496/PESC", 2021, *http://data.europa.eu/eli/dec/2021/698/oj*.
- Unione Europea, "Regolamento (UE) 2021/696 del Parlamento europeo e del Consiglio del 28 aprile 2021 che istituisce il programma spaziale dell'Unione e l'Agenzia dell'Unione europea per il programma spaziale e che abroga i regolamenti (UE) n. 912/2010, (UE) n. 1285/2013 e (UE) n. 377/2014 e la decisione n. 541/2014/UE", 2021, *http://data.europa.eu/eli/reg/2021/696/oj*.
- United Nations Environment Programme, "Bracing for Superbugs: Strengthening environmental action in the One Health response to antimicrobial resistance", 2023, *https://www.unep.org/resources/superbugs/environmental-action*.
- U.S Department of Defence, "Summary of the Joint All-Domain Command & Control (JADC2) strategy", marzo 2022, *https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF*.
- U.S. Geological Survey, "Mineral Commodity Summaries 2024", 2024, *https://pubs.usgs.gov/periodicals/mcs2024/mcs2024.pdf.*

Italia

MILANO
Via F. Albani, 21
20149 Milano
Tel. +39 02 46753.1

BOLOGNA
Via Persicetana Vecchia, 26
40132 Bologna
Tel. +39 051 268078

ROMA
Via Po, 22
00198 Roma
Tel. +39 06 8550951

Europa

AMBURGO
GLC Glücksburg Consulting
AGBülowstraße 922763 Hamburg
Tel. +49 40 8540 060
Mr. Martin Weigel
amburgo@ambrosetti.eu

BERLINO
GLC Glücksburg Consulting AG
Albrechtstraße 14 b 10117 Berlin
Tel. +49 30 8803 320
Mr. Martin Weigel
berlino@ambrosetti.eu

BRUXELLES
Ambrosetti Brussels Office
Tel. +32 476 79 10 89
Laura Basagni
laura.basagni@ambrosetti.eu

ISTANBUL
Consulta
Kore Şehitleri Caddesi Üsteğmen
Mehmet Gönenç Sorak No. 3
34394 Zincirlikuyu-ŞiŞli-Istanbul
Tel. +90 212 3473400
Mr. Tolga Acarli
istanbul@ambrosetti.eu

LONDRA
Ambrosetti Group Ltd.
5 Merchant Square, Paddington
London W2 1AY
london@ambrosetti.eu

MADRID
Ambrosetti Consultores
Castelló n° 19
Madrid, 28001
Tel. +34 91 575 1954
Ms. Marta Ortiz
madrid@ambrosetti.eu

Asia

BANGKOK
Mahanakorn Partners Group Co., Ltd.
Kian Gwan House III, 9th Floor, 152
Wireless Rd., Lumpini,
Pathumwan, Bangkok, 10330, Thailand
Tel. +66 (0) 2651 5107
Mr. Luca Bernardinetti
bangkok@ambrosetti.eu

PECHINO
Ambrosetti (Beijing) Consulting Ltd.
No.762, 6th Floor, Block 15
Xinzhaojiayuan, Chaoyang District
Beijing, 100024
Tel. +86 10 5757 2521
Mr. Mattia Marino
beijing@ambrosetti.eu

SEOUL
HebronStar Strategy Consultants
4F, ilsin bldg., 27,Teheranlro37-gil,
Gangnam-gu, Seoul
Tel. +82 2 417 9322
Mr. Hyungjin Kim
seoul@ambrosetti.eu

SHANGHAI
Ambrosetti (Beijing) Consulting Ltd.
Room 20L, Liduxingui Building,
No.831Xinzha Road, Jing'an District,
Shanghai
Tel:+86 21 52861891
Tel. +86 21 5237 7151
Mr. Mattia Marino
shanghai@ambrosetti.eu

SHANGHAI
Bai Shi Barbatelli & Partners Commercial Consulting Shanghai Company Ltd. (Shanghai)
Room 210, No.555 Wuding Road Jing'an
District, Shanghai, P.R. China
Tel. +86 21 5299 8905
Ms. Cristiana Barbatelli
shanghai-partner@ambrosetti.eu

SINGAPORE
The European House - Ambrosetti (Singapore) Consulting Pte. Ltd.
2 Woodlands Square
#05-70, Woods Square
Singapore 737715
Tel. +65 90998391
Mr. Marco Bardelli
singapore@ambrosetti.eu

TOKYO
Corporate Directions, Inc. (CDI)
Tennoz First Tower 23F
2-2-4 Higashi Shinagawa, Shinagawa-ku
Tokyo, 140-0002
Tel. +81 3 5783 4640
Mr. Nobuo Takubo
tokyo@ambrosetti.eu

Medio Oriente

DUBAI
The European House – Ambrosetti Middle East
Business Center Dubai World Central
P.O. Box: 390667 - Dubai - UAE
Mob. (UAE) +971.54.55.10003
Mob. (IT) +39.340.592.1349
Mr. Luca Miraglia
luca.miraglia@ambrosetti.eu

Africa

ROSEBANK - JOHANNESBURG
TEHA Africa Ltd
116 Oxford Road, Oxford & Glenhove,
Building 1
Rosebank
2196, Johannesburg
Tel. +27 76 487 8195
Mr. Nico De Kock
info@ambrosetti.za

The European House Ambrosetti

www.ambrosetti.eu