Presidenza del Consiglio dei Ministri

Sistema di Informazione per la Sicurezza della Repubblica

GOVERNARE IL CAMBIAMENTO

SCENARI DELLA SICUREZZA NAZIONALE

2026

Relazione annuale sulla politica dell'informazione per la sicurezza

La rivoluzione tecnologica a cui stiamo assistendo negli ultimi anni ha progressivamente assunto dei ritmi tali da rendere obsoleti gli ordinari strumenti di categorizzazione della realtà, complicando a dismisura l'opera degli Stati nell'adottare norme e provvedimenti idonei a perimetrare il fenomeno.

La tecnologia diviene così il principale volano di trasformazione sistemica, dato che, influenzando l'intera struttura sociale, economica, politica e militare, produce un inevitabile effetto cascata su tutti i settori in cui si esplicano le attività umane.

Si prospetta, quindi, una vera e propria evoluzione anche degli ordinamenti giuridici, con tutto ciò che può comportare in termini di emersione di nuovi diritti e di tutela della persona di fronte ad applicativi di frontiera tuttora privi di un substrato normativo.

Per fronteggiare tali mutevoli orizzonti, gli Organismi Informativi sono chiamati sia a implementare i propri sforzi previsionali, sia a sfruttare i nuovi strumenti offerti dalle tecnologie, anche in vista di un cambio di paradigma che risulti in grado di coniugare i tradizionali mezzi di ricerca informativa con quelli di soft intelligence.

INDICE

numero di pagina

I PREFAZIONE: LA TECNOLOGIA COME MOTORE DI TRASFORMAZIONE

1 SCENARI FUTURI DELLA SICUREZZA NAZIONALE

2 1 Sovranità tecnologica e sovranità digitale

19 2 L'accelerazione dei mutamenti geopolitici

45 3 Competitività e sicurezza del sistema economico-finanziario

67 4 Le reti del crimine transnazionale

82 5 Le dinamiche della minaccia interna

91 6 L'evoluzione del fenomeno immigratorio irregolare

101 7 Crisi internazionali e minaccia terroristica

112 8 La minaccia ibrida alle società democratiche

128 CINQUE TEST GenAI

129 Nota metodologica

131 Spazio 2035: la competizione oltre l'atmosfera

136 Scenari di conflitto Russia-NATO

138 Criptovalute: effetti di un ipotetico scenario di crisi

140 Proiezioni future dei flussi migratori

147 DAESH in Siria dalla caduta di Assad

INDICE
DELLE INFOGRAFICHE

numero di pagina

SCENARI FUTURI DELLA SICUREZZA NAZIONALE

10 SICUREZZA CIBERNETICA: TARGET, ATTORI, TECNICHE, FINALITÀ, ESITI

17 DASHBOARD Tecnologia

25 EVOLUZIONE DEL CONFLITTO IN UCRAINA

29 AFRICA: RISCHIO DEMOGRAFICO-STRUTTURALE (2025-2030)

33 LA CRISI DI GAZA

35 TEST MISSILISTICI DELLA COREA DEL NORD

38 CAPACITÀ NEL DOMINIO SOTTOMARINO

43 DASHBOARD Demografia

56 DALLA DIFESA ALLA RESILIENZA

63 L'APPROVVIGIONAMENTO ENERGETICO ITALIANO

65 DASHBOARD Economia

72 I MERCATI CRIMINALI

87 PRINCIPALI OPERAZIONI DI POLIZIA GIUDIZIARIA CON COINVOLGIMENTO DI MINORI

94 LE ROTTE MIGRATORIE NEL MEDITERRANEO

99 DASHBOARD Clima

122 LA DISINFORMAZIONE CONTRO LE DEMOCRAZIE LIBERALI

CINQUE TEST GenAI

134 Lo spazio verso il 2035

137 Scenari di conflitto Russia-NATO

139 Criptovalute: effetti di un ipotetico scenario di crisi

142 Proiezioni future dei flussi migratori

148 DAESH in Siria dalla caduta di Assad

PREFAZIONE: LA TECNOLOGIA COME MOTORE DI TRASFORMAZIONE

La presente Relazione nasce in un tempo in cui la tecnologia ha smesso di essere soltanto innovazione per diventare il motore del cambiamento e uno dei principali fattori che incidono sulla sicurezza del Paese. Ci troviamo in una fase storica segnata da una trasformazione profonda e continua, capace di incidere in modo strutturale sugli equilibri strategici, sulla stabilità economica e sulla coesione sociale.

L'innovazione tecnologica non accompagna più il cambiamento, lo orienta e lo accelera. Ridefinisce le modalità di esercizio del potere, modifica la natura delle minacce e condiziona la capacità dello Stato di prevenirle e contrastarle. Ne derivano questioni nuove e complesse sul piano giuridico, in relazione ai limiti dell'azione pubblica, al rispetto del principio di legalità e alla tutela dei diritti fondamentali sanciti dall'ordinamento costituzionale.

Nel contesto attuale il processo di trasformazione in atto ha ridefinito il concetto stesso di minaccia, che non si manifesta più soltanto in eventi visibili, ma in dinamiche continue, pervasive e spesso elusive. Oggi la minaccia opera in un contesto multidimensionale e multidominio, giacchè oltre ai tradizionali si estende anche al dominio cognitivo, a quello sottomarino e alla proprietà intellettuale. Il rischio, quindi, non si esprime più attraverso singole azioni apertamente ostili, ma con processi cumulativi che, inseriti in strategie coerenti e di lungo periodo, possono incidere sulla stabilità istituzionale, sulla fiducia dei cittadini e sulla capacità decisionale delle istituzioni, operando stabilmente al di sotto della soglia del conflitto armato, ad esempio compromettendo una rete, manipolando flussi informativi o trasformando una dipendenza tecnologica in leva di pressione.

Le nuove dinamiche tecnologiche attraversano confini geografici, settori economici e ambiti istituzionali, rendendo sempre più labile la distinzione tra sicurezza interna ed esterna e imponendo una lettura integrata dei fenomeni. Tecnologie già pienamente operative, quali la digitalizzazione pervasiva

e l'intelligenza artificiale, convivono con nuove frontiere scientifiche, tra cui le tecnologie quantistiche, destinate a introdurre discontinuità rilevanti anche sul piano della sicurezza delle comunicazioni e della protezione delle informazioni sensibili.

Ne deriva che l'innovazione costituisce oggi il principale volano di trasformazione sistemica, capace di investire l'intera struttura sociale, economica, politica e militare. La rapidità di questi mutamenti rende spesso obsoleti gli ordinari strumenti di categorizzazione della realtà, complicando l'opera degli Stati nell'adottare norme e provvedimenti idonei a perimetrare fenomeni in costante evoluzione. Si prospetta, così, una trasformazione degli ordinamenti giuridici, con tutto ciò che comporta in termini di emersione di nuovi diritti e di tutela della persona di fronte ad applicativi di frontiera tuttora privi di un substrato normativo adeguato.

La scelta del titolo "Governare il cambiamento" per l'attuale Relazione Annuale poggia sul presupposto che la trasformazione tecnologica è la chiave di lettura dello scenario di sicurezza contemporaneo. Il documento non descrive le singole tecnologie o i singoli eventi, ma offre un quadro di riferimento unitario per comprendere l'evoluzione delle minacce, individuare le vulnerabilità dei sistemi e rafforzare la capacità di prevenzione e di governo dei rischi, nella consapevolezza che la sicurezza oggi non può essere affidata alla sola reazione, ma richiede visione strategica, responsabilità e capacità di anticipazione.

La Relazione annuale 2026 e le sue specificità

La presente Relazione, redatta in favore del Parlamento ai sensi dell'art. 38 della Legge 3 agosto 2007, n. 124 e riferita alla politica di informazione per la sicurezza e ai risultati ottenuti nell'anno 2025, si caratterizza per un'impostazione innovativa poiché, accanto al consuntivo delle attività svolte dagli Organismi, evidenziato in specifici e dedicati *box*, propone una proiezione verso il futuro con l'obiettivo di evidenziare traiettorie evolutive, sfide emergenti e prospettive di sviluppo.

Il primo capitolo esamina l'impatto della tecnologia su **otto ambiti** ritenuti **di interesse strategico,** ciascuno dei quali esprime una specifica articolazione della medesima trasformazione strutturale. A completamento dell'impianto informativo, in ciascun capitolo sono inoltre previste infografiche finalizzate a visualizzare quadri di sintesi facilitando la lettura e la comprensione dei principali contenuti trattati. Nel dettaglio, la Relazione affronta i seguenti ambiti:

1. **sovranità tecnologica e digitale**

   L'esercizio della sovranità di un Paese si manifesta sempre più nella sua autonomia strategica, ovverosia la capacità di gestire dati, infrastrutture critiche, algoritmi e filiere tecnologiche. Dipendenze non governate possono trasformarsi in punti di pressione strutturali, riducendo la libertà d'azione di un Paese. L'attenzione pertanto si poggia su opportunità e minacce di strumenti tecnologici cd. *dual use*;

2. mutamenti geopolitici

È inconfutabile che i paradigmi globali siano ormai cambiati e che assistiamo a una profonda ridefinizione del nuovo ordine mondiale. L'accelerazione in atto non riguarda esclusivamente la dimensione tecnologica ma si riflette sugli assetti geopolitici ed economici internazionali, rendendo necessario ripensare a una nuova postura strategica.

Poiché gli equilibri geopolitici si ridefiniscono sempre più lungo linee tecnologiche, il controllo delle tecnologie emergenti, delle risorse critiche e degli *standard* industriali incide direttamente sulla proiezione di potenza. L'analisi offerta interessa quadranti geopolitici di rilievo per l'*intelligence*, quali lo spazio europeo, il continente africano, la regione mediorientale e l'area indo-pacifica;

3. sicurezza economico-finanziaria

La sicurezza economico-finanziaria è esposta a un rischio sistemico crescente. Mercati digitalizzati, sistemi di pagamento interconnessi, criptovalute, catene del valore complesse e nuove minacce alle infrastrutture critiche e ai settori di maggiore competitività (come quello energetico e farmaceutico), amplificano l'impatto di *shock* esterni, interferenze ostili e coercizioni economiche, espressioni della *economic warfare*. In questo quadro, la stabilità finanziaria non è più soltanto una questione macroeconomica, ma una componente essenziale della sicurezza nazionale;

4. minaccia criminale organizzata

Le reti del crimine transnazionale si configurano come attori tecnologicamente sofisticati. Criptovalute, comunicazioni cifrate, piattaforme digitali e anonimato online consentono resilienza operativa, rapidità di adattamento e capacità di elusione senza precedenti e sostengono le linee evolutive dei traffici illeciti. La convergenza tra criminalità organizzata e tecnologia rappresenta una minaccia persistente, che non conosce confini ma insiste su una visione globale che richiede un'azione di contrasto corale volta *in primis* a colpire gli ecosistemi digitali sui quali viaggiano i capitali illeciti;

5. minaccia interna

Anche la minaccia interna è interessata dalla tecnologia, sebbene persistano sacche di antagonismo impermeabili all'evoluzione tecnologica. In contrapposizione a queste, l'approccio dei circuiti virtuali dell'estrema destra "suprematista e accelerazionista internazionale" vede invece la tecnologia come elemento abilitante per rafforzare la propaganda. In tal senso, la radicalizzazione *online*, l'accesso a strumenti digitali avanzati e la possibilità di azioni a distanza aumentano in modo significativo il potenziale di danno di singoli individui o gruppi;

6. immigrazione irregolare

In tale ambito il fattore tecnologico costituisce un crescente e significativo strumento di potenziamento nelle attività di contrasto ai flussi migratori.

In chiave prospettica, tale minaccia potrebbe assumere anche connotazioni ibride, divenendo un possibile strumento di pressione;

7. **minaccia terroristica**

   Le molteplici crisi internazionali influiscono significativamente sul panorama della minaccia terroristica, che ha assunto una dimensione sempre più complessa. In tale contesto il ricorso alle nuove tecnologie da parte di individui e gruppi estremisti e terroristici rappresenta un moltiplicatore dei processi di radicalizzazione, di diffusione della propaganda e di sviluppi di canali di finanziamento. Anche in questo contesto, comunque, l'IA rappresenta al tempo stesso un valido strumento per potenziare le attività di prevenzione e contrasto alla radicalizzazione e al terrorismo;

8. **minaccia ibrida**

   La minaccia ibrida rappresenta la sintesi operativa di queste dinamiche. Attraverso l'integrazione coordinata di strumenti tecnologici, informativi, economici e politici, è possibile colpire un avversario senza superare la soglia dell'uso della forza e del conflitto armato. La tecnologia è il fattore abilitante centrale di tali operazioni, rendendo più difficile l'attribuzione, la risposta e la deterrenza. La manipolazione informativa rappresenta uno degli strumenti più efficaci e pervasivi di questo nuovo veicolo di minaccia che agisce all'interno della sfera cognitiva e che è volta a minare, in ultima analisi, i capisaldi delle società democratiche.

L'edizione di quest'anno, infine, si distingue per un'impostazione innovativa nei contenuti e nel metodo. Oltre a **quattro *dashboard*** realizzate esclusivamente con metodologie statistiche e inserite all'interno dei capitoli, nell'**Appendice** della Relazione vengono presentati **cinque casi studio** elaborati mediante l'utilizzo di tecnologie di intelligenza artificiale generativa (GenAI), che costituiscono una novità introdotta in questa edizione.

Trattasi di un esercizio di natura metodologica e scientifica che mira a mostrare, entro un perimetro compatibile con la divulgazione pubblica, i potenziali benefici dell'impiego di strumenti avanzati a supporto dei processi di analisi. Sviluppati unicamente su dati provenienti da fonti aperte e sulla base di una capacità computazionale convenzionale[1], sono esercizi che approfondiscono scenari di particolare interesse strategico connessi alle aree tematiche trattate nella sezione precedente, quali: conflitto Russia-NATO, competizione nello spazio, Daesh in Siria, criptovalute e proiezioni dei flussi migratori.

I cinque esercizi sono stati realizzati secondo criteri rigorosi e con un approccio dichiaratamente antropocentrico, dove l'IA è stata intesa come supporto all'analista, capace di addestrare i sistemi, im-

1 Sono stati utilizzati applicativi commerciali e di libero accesso senza fare ricorso alle maggiori capacità computazionali e tecnologiche dell'*intelligence*.

piegare efficacemente gli applicativi e validare i risultati, evitando automatismi e scongiurando ogni affidamento acritico sugli *output* generati. Infatti, analisti, operatori OSINT e personale tecnico hanno lavorato in gruppi multidisciplinari, assicurando il controllo della qualità, dalla definizione dell'obiettivo informativo alla selezione delle fonti, dall'interazione con i modelli alla revisione critica dei risultati.

Le quattro *dashboard* intendono, invece, offrire un termine di confronto metodologico e rafforzare la comprensione dei fenomeni analizzati. Trattasi di indicatori strategici dedicati alla demografia, al clima, alla tecnologia e alla geopolitica; fattori che riflettono *trend* globali ed hanno carattere trasversale, risultando funzionali a rappresentare l'andamento e l'evoluzione dei fenomeni considerati.

Nel loro insieme, tali esercizi puramente tecnici hanno la finalità di dimostrare come l'integrazione consapevole delle tecnologie di intelligenza artificiale, inserita in un quadro metodologico rigoroso e sotto il controllo dell'analista, possa incrementare la qualità complessiva dell'analisi, favorire l'emersione di schemi e tendenze e supportare, in prospettiva, processi decisionali più informati e tempestivi in favore del decisore politico.

In continuità con la scelta operata lo scorso anno, anche questa edizione è corredata da un **inserto** dedicato a una frontiera avanzata della competizione globale. Ci si è, in particolare, concentrati sull'avvento della tecnologia quantistica, allo scopo di approfondirne sia le potenzialità, sia i molteplici risvolti che emergono dalla prospettiva della sicurezza nazionale.

"Governare il cambiamento" implica sempre più la capacità di anticipare fenomeni e minacce.

SCENARI FUTURI DELLA SICUREZZA NAZIONALE

1. SOVRANITÀ TECNOLOGICA E SOVRANITÀ DIGITALE

L'attività info-operativa dispiegata dall'Intelligence nel 2025 è stata indirizzata prevalentemente verso le offensive cibernetiche perpetrate da attori della minaccia che, per capacità tecniche e disponibilità di risorse, appaiono verosimilmente contigui ad apparati governativi stranieri. È emerso altresì il crescente interesse di numerosi sodalizi di stampo hacktivista.

Rileva, altresì, il progressivo impiego, da parte degli attori della minaccia più sofisticati, di infrastrutture telematiche complesse, con l'obiettivo di anonimizzare il proprio traffico di rete durante la conduzione di attacchi cibernetici.

Gli sforzi dell'Intelligence si sono concentrati, nel corso del 2025, anche nella definizione del processo di attribuzione a livello nazionale delle condotte cibernetiche ostili dirette contro il nostro Paese.

L'attività info-operativa posta in essere nell'anno in esame ha permesso di registrare il crescente interesse degli attori della minaccia in direzione delle infrastrutture digitali riferibili ai soggetti pubblici nazionali, con particolare attenzione verso quelle riconducibili alle principali Amministrazioni Centrali dello Stato.

Quanto al settore privato, si è assistito a una contrazione delle offensive cibernetiche che hanno interessato i relativi assetti telematici.

Per quanto attiene alla classificazione degli attacchi per tipologia di attori ostili, anche il 2025 testimonia la costante azione di spionaggio cibernetico posta in essere da gruppi altamente specializzati (APT), contigui ad apparati governativi dai quali ricevono linee di indirizzo

strategico e supporto finanziario.

Per quel che concerne le offensive di natura criminale cibernetica, si è registrato un lieve incremento nel periodo monitorato.

Resta marginale, rispetto al totale, la rilevanza delle azioni ostili di matrice hacktivista.

L'esame delle tattiche, tecniche e procedure (TTP) maggiormente impiegate dai principali attori della minaccia ha confermato il prevalente ricorso, da parte dei gruppi APT di matrice statuale, a impianti malevoli particolarmente sofisticati.

Si conferma la prevalenza di offensive finalizzate al furto di identità digitali e/o credenziali, successivamente messe in vendita in ambienti digitali underground, cui ha fatto da contraltare l'esfiltrazione di informazioni di potenziale interesse per l'attaccante. Restano stabili, invece, le offensive cibernetiche poste in essere da gruppi APT di matrice verosimilmente statuale.

Quanto alle finalità degli attacchi monitorati, restano prevalenti, in termini percentuali, le offensive cibernetiche orientate a garantire un vantaggio economico all'attaccante. È stato registrato anche un aumento delle azioni digitali ostili di chiara matrice spionistica.

I NUOVI PROFILI DELLA SOVRANITÀ

La dimensione della rivoluzione tecnologica e la pervasività della trasformazione digitale in corso hanno collocato il concetto della sovranità degli Stati su piani nuovi rispetto alla tradizionale concezione propria della filosofia politica, rendendo la sovranità tecnologica e la sovranità digitale sempre più abilitanti all'effettivo esercizio dell'autorità statuale in alcuni settori strategici della vita nazionale. Si tratta di ambiti spesso interconnessi tra loro e la cui rilevanza per lo Stato produce evidenti riflessi sul piano dell'interesse intelligence.

La **sovranità digitale**, ossia la capacità di controllare in modo autonomo le proprie risorse digitali (in termini di dati, algoritmi, applicazioni, infrastrutture), è diventata condizione indispensabile per tutelare la sicurezza, favorire l'innovazione e difendere l'integrità economica del Paese. Quelle digitali costituiscono attualmente le risorse primarie dell'economia globale, in quanto non solo sostengono i processi di sviluppo dei maggiori settori industriali e finanziari, ma concorrono anche alla definizione del vantaggio competitivo del Paese a livello internazionale.

Consapevole di tale evoluzione, l'Unione europea ha adottato una strategia tesa all'adozione del modello del c.d. cloud sovrano, con la quale si intende tutelare la localizzazione controllata dei dati, la giurisdizione esclusiva e la gestione autonoma delle chiavi crittografiche.

> *La sovranità digitale è diventata condizione indispensabile per tutelare la sicurezza, favorire l'innovazione e difendere l'integrità economica del Paese*

La **sovranità tecnologica**, ossia la capacità di controllare le tecnologie strategiche necessarie a garantire la sovranità digitale (es: semiconduttori, intelligenza artificiale, High Performance Computing – HPC, quantum computing, ecc.), consente invece di minimizzare la dipendenza strategica da influenze straniere sulla gestione e sul funzionamento delle infrastrutture digitali.

I rischi che potrebbero discendere dalla dipendenza tecnologica si amplificano ancora di più considerando i recenti sviluppi sul campo dell'intelligenza artificiale come motore delle nuove infrastrutture cloud. Anche in questo caso si rilevano molteplici incognite connesse all'eventuale gestione straniera, integrale o parziale, delle infrastrutture, del software o della componentistica.

LA PERMEABILITÀ DEL CONFINE TRA DOMINIO CINETICO E DOMINIO CIBERNETICO

L'integrazione crescente tra infrastrutture fisiche e digitali sta ridefinendo le interdipendenze tra il dominio cinetico (tangibile e concreto) e quello cibernetico (costituito dall'insieme di dati, algoritmi, ca-

pacità computazionali e reti), oramai interpretabili come polarità del medesimo sistema. Il **dominio cinetico** e il **dominio cibernetico** sono facce complementari della gestione del cambiamento nel mondo contemporaneo, ove la realtà fisica e quella digitale interagiscono costantemente.

In tale contesto, appare evidente come il concetto di **resilienza dei sistemi cyber-fisici (CPS)** diventi un fattore critico per la sicurezza nazionale.

Le contemporanee operazioni offensive ostili e gli attacchi a infrastrutture critiche mostrano come le manovre cyber possano produrre impatti materiali (si pensi agli effetti causati in passato dai malware noti come Stuxnet, WannaCry e NotPetya e da quelli prodotti oggigiorno con l'impiego di comuni ransomware) e come, analogamente, azioni fisiche siano idonee a degradare la capacità informativa di un avversario (per esempio, attraverso la distruzione di nodi di comunicazione e attacchi mirati ai cavi sottomarini in fibra ottica utilizzati per la connettività Internet).

Nel dominio cinetico, qualsiasi attività richiede l'impiego di sensori, di sistemi di comunicazioni, di pianificazione digitale e di catene logistiche gestite tramite sistemi informatici. La componente cibernetica è quindi parte integrante dell'infrastruttura, il cui funzionamento dipende dalla robustezza e disponibilità delle reti e dei dati.

In contesti civili e militari, la componente cibernetica ha un ruolo sia di gestione che di monitoraggio (comando, controllo e awareness). Le vulnerabilità a cui i sistemi appartenenti a tale dominio sono soggetti (attacchi DDoS, ransomware, wipers, ecc.) hanno impatti diretti sui processi fisici controllati (dalla distribuzione energetica al settore sanitario), confermando così la necessità di modelli congiunti di sicurezza.

Inoltre, i recenti conflitti e le campagne di disinformazione a essi connessi hanno evidenziato come attacchi coordinati nei domini dell'informazione, cibernetico e cinetico producano effetti sinergici quando opportunamente integrati, riuscendo a superare i limiti operativi che questi avrebbero ove attuati singolarmente.

Nello specifico, gli attuali teatri di guerra hanno prodotto una grande quantità di dati su come operazioni cyber e cinetiche possano essere combinate (campagne di malware contro settori strategici, campagne di disinformazione mirate, attacchi missilistici e sabotaggi contro le infrastrutture di comunicazione), evidenziando anche la necessità di difese e strategie integrate, nonché piani di continuità che non assumano come parametro la sola disponibilità delle reti.

Tutto ciò ha portato alla nascita di modelli e approcci quantitativi utili ad analizzare il rapporto tra dominio cinetico e cibernetico, fornendo tecniche di modellazione e di difesa aggiornate dei citati CPS. Tra questi, emergono **metriche di resilienza CPS** che tengono in considerazione:

- il tempo di recupero (recovery);
- la capacità di degradazione controllata;

- modelli di propagazione degli effetti che aiutano a prevedere come un attacco o un guasto possa propagarsi;
- metodologie di analisi temporali per assicurare che componenti operanti in domini distinti abbiano una nozione del tempo comune e coerente (fondamentale affinché gli eventi fisici possano essere registrati, elaborati e controllati in modo tempestivo e nel giusto ordine sequenziale).

L'interdipendenza tra domini si configura, dunque, come un continuum in cui:

- l'elemento informatico può agire da leva per effetti cinetici (es. sabotaggio digitale per interrompere servizi essenziali);
- le operazioni fisiche possono limitare o facilitare la capacità digitale (es. distruzione di infrastrutture terresti/marittime per isolare le reti);
- la mancata sincronizzazione tra sistemi fisici e digitali riduce l'efficacia complessiva.

In definitiva, la robustezza operativa degli ecosistemi cyber-fisici dipende dalla capacità difensiva della componente cyber e dalla qualità dell'integrazione con il dominio fisico.

GLI SCENARI DELLA MINACCIA CYBER

Nel contesto di un quadro geopolitico internazionale dominato da un perdurante stato di incertezza rispetto all'evoluzione dei molteplici teatri di conflitto, lo **strumento cibernetico** continua a rivestire un **ruolo centrale** nelle **strategie offensive** degli **ATTORI DELLA MINACCIA**, collocandosi tra i principali strumenti per acquisire informazioni utili a orientare le rispettive politiche industriali, economiche, finanziarie ed estere.

In tale cornice, l'**attività info-operativa** dispiegata dall'**Intelligence** è stata indirizzata prevalentemente verso:

- le offensive cibernetiche perpetrate da quegli attori della minaccia che, per capacità tecniche e disponibilità di risorse, appaiono verosimilmente contigui ad apparati governativi stranieri (**Advanced Persistent Threat – APT di matrice statuale**). Tali attori hanno proseguito con il concentrare la propria attività malevola di spionaggio digitale in direzione dei settori strategici nazionali a più alta concentrazione tecnologica – su tutti, quello aerospaziale e delle infrastrutture digitali/servizi ICT – nonché verso le reti IT delle principali Amministrazioni Centrali dello Stato;
- gli interessi di numerosi **sodalizi di stampo hacktivista** nei confronti del dominio delle Operational Technology (ossia hardware e software utilizzati per monitorare, controllare e gestire dispositivi fisici, processi ed eventi all'interno di un'organizzazione) e dei relativi sistemi SCADA (Supervisory Control and Data Acquisition). In particolare, i predetti attori hanno ripetutamente provato a sfruttare le vulnerabilità intrinseche di tali sistemi (quali la difficoltà di aggiornamento e implementazione delle più recenti misure di sicurezza, l'impiego di credenziali amministrative

"deboli" e l'utilizzo di protocolli di comunicazione obsoleti e non cifrati), nel tentativo di condurre potenziali azioni di disturbo e sabotaggio.
Sotto il profilo valutativo, la compromissione dei sistemi citati, anche laddove interessasse impianti di piccole e medie dimensioni, potrebbe generare, da un lato, impatti per la popolazione, legati a rilevanti disservizi, dall'altro, un considerevole danno di immagine a livello di Sistema Paese, a causa dell'eventuale risonanza mediatica dell'evento ostile. Proprio il potenziale mediatico discendente da eventuali incidenti in danno di infrastrutture critiche rappresenta il principale fattore di interesse per le richiamate formazioni hacktiviste. Tali azioni ostili potrebbero verosimilmente essere strumentalizzate nel contesto di più ampie operazioni di influenza che, facendo leva sull'elemento psicologico derivante dai potenziali impatti generati da offensive cibernetiche, a loro volta esacerbati attraverso campagne mediatiche sui social media, potrebbero indurre uno stato di timore e di insicurezza nell'opinione pubblica;

- gli **attori della minaccia più sofisticati** e il progressivo utilizzo, da parte degli stessi, di infrastrutture telematiche complesse (Covert Relay Network), costituite da numerosi nodi proxy, quali Virtual Private Server (VPS) e dispositivi compromessi, tra cui router, firewall, dispositivi IoT (Internet of Things) e di archiviazione in rete (Network Attached Storage – NAS).

> *Per la prima volta, la comunità Intelligence italiana ha accolto l'invito di quella statunitense e sottoscritto congiuntamente ai principali omologhi organismi occidentali, un report che attribuisce pubblicamente alla Cina la campagna di spionaggio del gruppo APT denominato "Salt Typhoon"*

Si tratta di infrastrutture impiegate, in genere, con l'obiettivo di anonimizzare il proprio traffico di rete durante la conduzione di attacchi cibernetici, in modo da rendere particolarmente difficoltoso il processo di individuazione dell'autore e dell'eventuale mandante dell'attacco (processo di attribuzione). Gli sforzi dell'Intelligence, già impegnata – insieme al Ministero degli Affari Esteri e della Cooperazione Internazionale, in attuazione della **misura #40** della **Strategia Nazionale di Cybersicurezza 2022-2026** e del relativo Piano di Implementazione – nella definizione del **processo di attribuzione a livello nazionale**, si sono concentrati, nel corso del 2025, sul tema dell'attribuzione delle condotte cibernetiche ostili dirette contro il nostro Paese.
In particolare, il **27 agosto 2025, per la prima volta**, la Comunità Intelligence italiana ha accolto l'invito di quella statunitense e sottoscritto, congiuntamente ai principali omologhi Organismi occidentali, un report (Joint Cybersecurity Advisory) che **attri-**

buisce pubblicamente – sotto il profilo tecnico e per quanto di competenza agli Organismi di Informazione e Sicurezza – alla **Repubblica Popolare Cinese la campagna di spionaggio cibernetico** del gruppo APT di matrice statuale denominato "Salt Typhoon" (titolo del rapporto: Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System).

Tanto premesso, si segnala che l'attività info-operativa posta in essere nel corso del 2025 ha permesso di registrare il crescente **interesse** degli **attori della minaccia** in direzione delle **infrastrutture digitali** riferibili ai **soggetti pubblici nazionali**, con particolare attenzione verso quelle riconducibili alle principali Amministrazioni Centrali dello Stato.

Nel periodo in esame, è risultata significativa anche l'attenzione posta dagli attori ostili verso gli assetti ICT riferibili a diverse **strutture sanitarie pubbliche**, che ha messo in luce la netta crescita del numero di offensive rispetto all'anno precedente. In tale quadro, le azioni malevole si sono primariamente focalizzate sui dispositivi informatici nelle disponibilità del personale medico, utilizzati in modo promiscuo e dai quali gli attaccanti tentano di estrarre illegittimamente credenziali per l'accesso a servizi ICT erogati da Aziende Sanitarie Locali e istituti di cura e ricerca, vendute poi su fora e marketplace nel deep & dark web o re-impiegate per ulteriori azioni ostili con differenti finalità.

Tale circostanza conferma che uno tra i principali fattori di rischio per la sicurezza cibernetica è l'inadeguata percezione – specie nella pubblica amministrazione – dell'effettivo perimetro infrastrutturale meritevole di protezione (comprensivo delle postazioni di lavoro assegnate ai dipendenti per attività di smart working e di quelle utilizzate da personale esterno, consulenti, fornitori di servizi, ecc.).

Quanto al **settore privato**, si è assistito a una **contrazione** delle **offensive cibernetiche** che hanno interessato i relativi **assetti telematici**, con particolare attenzione verso quelli riconducibili a realtà operanti nei settori delle infrastrutture digitali/servizi IT, delle telecomunicazioni, energetico e bancario.

Un focus specifico va riservato alle offensive cibernetiche ostili condotte in direzione di piccole e medie realtà private locali. Nel merito, stante la matrice prevalentemente statuale degli attacchi in questione, nonché la presenza di vulnerabilità note o di sistemi non aggiornati o mal configurati sulle relative reti telematiche, si suppone che tali obiettivi vengano presi di mira dagli attaccanti in maniera opportunistica, al verosimile fine di ampliare la capillarità delle proprie reti di attacco e anonimizzazione.

Per quanto attiene alla **CLASSIFICAZIONE DEGLI ATTACCHI PER TIPOLOGIA DI ATTORI OSTILI**:

- anche il 2025 testimonia la costante **azione di spionaggio cibernetico** posta in essere da **gruppi altamente specializzati (APT)**, **contigui ad apparati governativi** dai quali ricevono linee di indirizzo strategico e supporto finanziario e, pertanto, ritenuti maggiormente insidiosi per il Sistema Paese in termini di informazioni esfiltrate

(di natura sia geopolitica che economico-industriale), nonché di perdita di operatività e competitività, senza tralasciare il dispendio di risorse economiche necessarie per la loro mitigazione.

In tale contesto, l'accentuato attivismo dei predetti attori, messo in luce dall'attività degli Organismi di informazione, ha contribuito a innalzare il livello di attenzione rispetto a talune campagne cibernetiche ostili e potenzialmente orientate al pre-posizionamento all'interno delle reti telematiche di realtà pubbliche e private nazionali.

Tale prassi operativa si traduce nel tentativo di inoculare nell'infrastruttura che costituisce l'obiettivo dell'azione un'arma digitale non orientata a produrre effetti palesi nell'immediato (es. interruzione nell'erogazione di servizi offerti attraverso la rete, distruzione di dati, ecc.), ma bensì a realizzare conseguenze – potenzialmente devastanti – in un secondo momento, al verificarsi di determinate condizioni (eventualmente connesse con l'evoluzione dello scenario geopolitico), ovvero in attuazione di una specifica strategia dello "Stato mandante" (o di un soggetto che agisce per conto o nell'interesse dello stesso – c.d. proxy);

- per quel che concerne le **offensive di natura criminale cibernetica**, si è registrato un **lieve incremento** nel periodo in esame, in ragione del perdurante fenomeno dell'esfiltrazione e conseguente rivendita di credenziali e informazioni sensibili su marketplace illegali attestati nel deep e nel dark web. Nel merito, al netto dell'evidente potenziale di re-impiego delle citate credenziali in ulteriori tentativi di compromissione, si evidenzia, da un lato, la delicatezza e il peculiare valore economico di taluni dati, a partire da quelli sanitari, dall'altro, la disponibilità dimostrata da numerose vittime al pagamento del riscatto richiesto. Elementi, questi, che contribuiscono ad alimentare la condotta malevola in questione, rendendola maggiormente appetibile e remunerativa per l'attore ostile;
- resta **marginale**, rispetto al totale, la rilevanza delle **azioni ostili di matrice hacktivista**, condotte perlopiù da militanti in sodalizi prevalentemente filorussi, come il gruppo denominato "NoName075(16)", in danno di assetti telematici nazionali.

L'**ESAME DELLE TATTICHE, TECNICHE E PROCEDURE (TTP)** maggiormente impiegate dai principali attori della minaccia:

- ha confermato il **prevalente ricorso**, da parte dei **gruppi APT di matrice statuale**, a **impianti malevoli particolarmente sofisticati**, veicolati all'interno delle reti telematiche dei soggetti che costituiscono l'obiettivo dell'azione, con l'intento di esfiltrare informazioni di interesse.

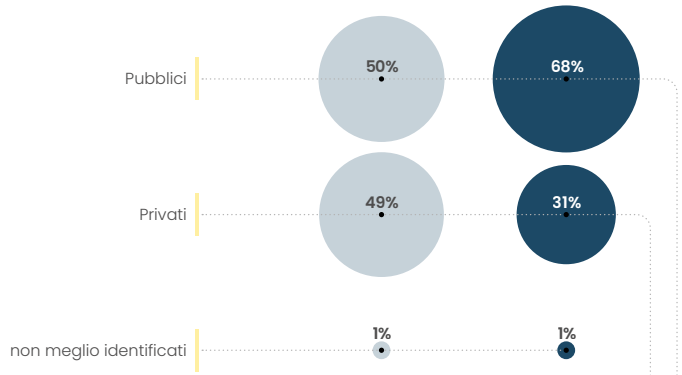
  Nel novero degli impianti digitali malevoli, figurano anche i noti **ransomware**, sfruttati tanto nei contesti criminali cibernetici per acquisire illecitamente capitali, in ragione dei riscatti pagati dalle vittime per riottenere il controllo sui propri dati cifrati dallo strumento malevolo in esame,

SICUREZZA CIBERNETICA

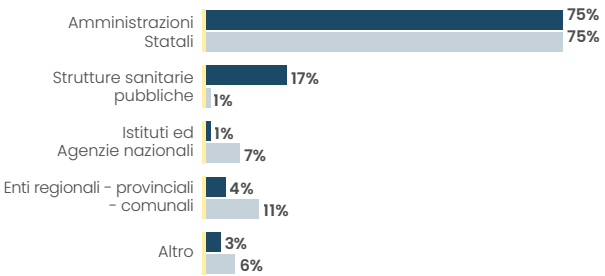
Target, attori, tecniche, finalità, esiti

2024 2025

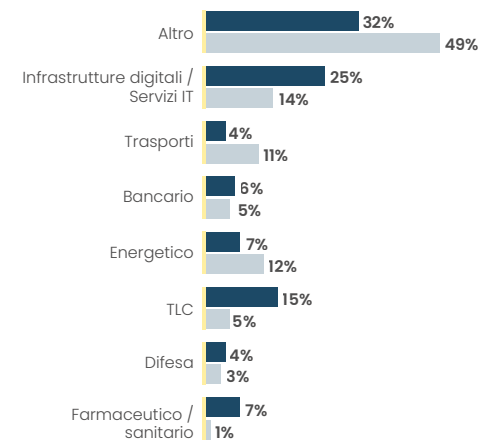
Target



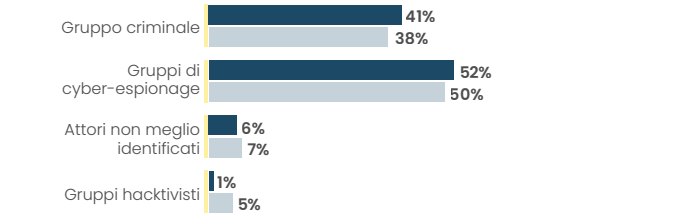
Target pubblici



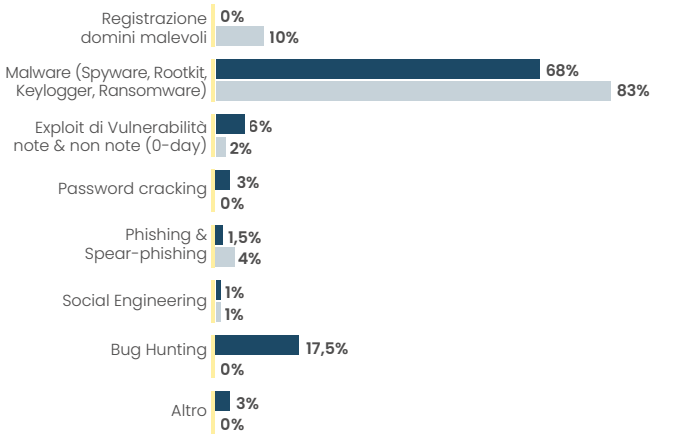
Target privati



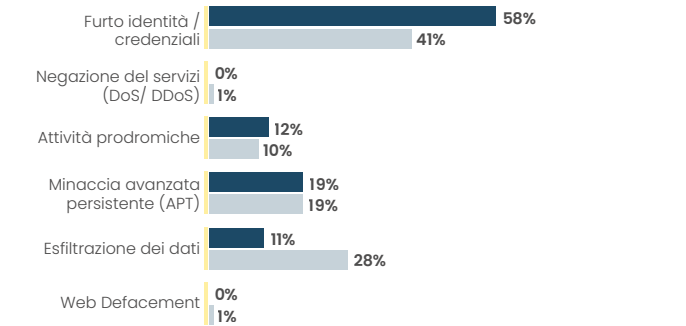
Attori



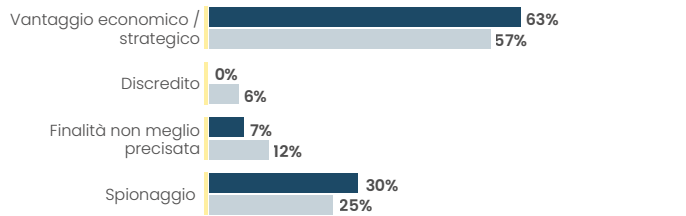
Tecniche



Esiti



Finalità dell'attacco



quanto dai gruppi ostili che operano in qualità di proxy di governi esteri, come leva per interferire con la normale operatività di infrastrutture, servizi e catene del valore del Sistema Paese (nel contesto di operazioni con finalità di disruption);

- a tale consolidata prassi, si è recentemente affermato il massiccio **sfruttamento di vulnerabilità note e non note (0-day)** – primariamente riferibili a dispositivi e piattaforme largamente impiegati in contesti aziendali, come apparati di rete e sistemi di posta elettronica – quale principale escamotage per guadagnare l'accesso a risorse telematiche riferibili a realtà pubbliche e private nazionali, cui si affianca – benché in modo residuale rispetto al complesso di TTP ostili disponibili – il crescente ricorso a più tradizionali tecniche di attacco, come il **phishing** e lo **spear-phishing**, **unitamente** ai tentativi di **social engineering**.

Per quanto riguarda gli **ESITI DELLE AZIONI OSTILI**, nel 2025 si conferma la **prevalenza di offensive finalizzate al furto di identità digitali e/o credenziali**, successivamente messe in vendita in ambienti digitali underground, cui ha fatto da contraltare l'esfiltrazione di informazioni di potenziale interesse per l'attaccante. Restano **stabili**, invece, le **offensive cibernetiche** poste in essere da gruppi APT di matrice verosimilmente statuale.

Quanto alle **FINALITÀ DEGLI ATTACCHI** monitorati, restano **prevalenti**, in termini percentuali, le **offensive cibernetiche orientate a garantire un vantaggio economico all'attaccante**.

Inoltre, a ulteriore conferma di come il dominio cibernetico sia impiegato da attori statuali quale strumento per il raggiungimento dei rispettivi obiettivi strategici, si registra, anche per il 2025, un **aumento** delle **azioni digitali ostili** di chiara **matrice spionistica**, in linea con un trend che, a partire dal 2020, risulta in costante crescita.

GLI SVILUPPI DELL'INTELLIGENZA ARTIFICIALE MULTIMODALE E LE POTENZIALI RICADUTE SULLA SICUREZZA

Uno dei progetti più ambiziosi della ricerca tecnologica è ravvisabile nella creazione di una "macchina pensante" capace di replicare, e possibilmente superare, le capacità cognitive della mente umana. Questo obiettivo si è materializzato negli ultimi decenni nel campo dell'**intelligenza artificiale** e del **machine learning**.

Dal test di Turing, gli studi sulla materia si sono orientati, negli ultimi anni, verso lo sviluppo di reti neurali profonde, nonché all'**implementazione** dei **metodi di apprendimento automatico** e dei **modelli di linguaggio di grandi dimensioni (Large Language Models, LLM)**, favorendo il raggiungimento di prestazioni sorprendenti in numerosi compiti cognitivi. Oggi, i sistemi di intelligenza artificiale possono essere un supporto per i medici nella diagnosi delle malattie e sono capaci di generare testi coerenti e creativi, di analizzare dati complessi, oltre che di identificare pattern non

evidenti agli analisti. Tali progressi suggeriscono che la frontiera fra l'intelligenza umana e quella artificiale si stia progressivamente assottigliando, facendo emergere sempre più la rilevanza che assumono anche le questioni etiche e la necessità di sviluppare sistemi con algoritmi tarati su un'architettura antropocentrica.

La ricerca contemporanea in materia di intelligenza artificiale continua a muoversi verso l'**obiettivo** di **creare sistemi di Artificial General Intelligence – AGI**, capaci di comprendere e apprendere qualsiasi compito, non limitandosi a uno specifico come negli attuali sistemi esistenti. È evidente che le implicazioni di tale sviluppo sarebbero enormi, sia per il potenziale beneficio che per i rischi associati.

L'intelligenza artificiale (IA) rappresenta attualmente lo strumento di cambiamento più potente e pervasivo. A differenza di talune innovazioni tecnologiche precedenti, che hanno intaccato settori specifici, l'**intelligenza artificiale possiede il potenziale di permeare ogni dominio dell'attività umana**. Ad esempio, l'IA:

- nel **settore militare**, trasforma la natura stessa della guerra. Emblematici, nel senso, i sistemi autonomi di sorveglianza e riconoscimento, i droni intelligenti, i sistemi decisionali automatizzati e l'analisi predittiva delle minacce;
- nel **settore economico**, ottimizza le catene di approvvigionamento, automatizza la produzione, genera nuovi modelli di business;
- nel **settore sanitario**, migliora la diagnostica e sviluppa nuovi farmaci;
- nel **settore dell'informazione**, è in grado di personalizzare i contenuti fruibili da miliardi di persone, modellando così le percezioni e le opinioni della collettività.

Questa pervasività trasformativa rende l'intelligenza artificiale un fattore qualificante dello sviluppo contemporaneo. Al riguardo, gli Stati che potenzieranno maggiormente le proprie capacità in tale campo avranno un evidente vantaggio strategico rispetto a quelli che resteranno indietro. La stessa considerazione può essere svolta per le aziende e le istituzioni. In definitiva, la competizione globale per il dominio dell'IA è, di fatto, una competizione per il controllo degli stessi processi trasformativi e per la capacità di modellare il futuro.

Alla luce del quadro delineato, anche il ruolo dell'Intelligence muta profondamente, non limitandosi più alla sola attività di raccolta e analisi di informazioni su scenari e minacce incidenti sugli interessi nazionali, ma focalizzandosi altresì sull'acquisizione di competenze previsionali sofisticate, capaci di identificare le traiettorie di sviluppo tecnologico emergenti e di valutare anticipatamente le loro implicazioni geopolitiche.

In questo contesto, emerge il **concetto di "energie previsionali"**, ossia la capacità di prevedere non solamente quale tecnologia emergente avrà successo, ma più ancora come la stessa si diffonderà, quale attore avrà un ruolo pioneristico nella sua adozione, quali reazioni si innescheranno sul piano

geopolitico e in che modo la tecnologia modificherà gli equilibri di potere.

Prendendo le mosse da questo scenario, le Istituzioni europee hanno delineato un primo quadro normativo sul tema attraverso il Regolamento(UE) 2024/1689 (c.d. AI Act). L'Italia ha di conseguenza provveduto ad armonizzare e adeguare il proprio ordinamento attraverso la **legge 23 settembre 2025, n. 132**. Tale intervento legislativo, nel fissare i principi cardine da osservare in materia di ricerca, sperimentazione, sviluppo, adozione e applicazione di sistemi e modelli di IA, ha posto particolare enfasi sull'importanza della **dimensione antropocentrica** e sul **rispetto dei diritti fondamentali previsti dalla Costituzione**. Nel valorizzare le opportunità legate all'utilizzo dell'IA in molteplici settori – cercando al contempo di coglierne i rischi – si è in tal modo assicurata al nostro Paese una legislazione innovativa e coerente con i tempi, anche alla luce delle ingenti risorse finanziarie stanziate sia a livello europeo che nazionale.

> *L'intelligenza artificiale possiede il potenziale di permeare ogni dominio dell'attività umana*

Tanto premesso in termini generali, occorre segnalare come l'**integrazione dell'Intelligenza artificiale nei sistemi di sicurezza informatica** stia trasformando profondamente le modalità di identificazione, analisi e mitigazione delle minacce: l'**applicazione di tecniche di Machine Learning e Deep Learning su grandi moli di dati**, come log di sistema o flussi di rete, consente ormai di superare i limiti dei metodi classici basati sul riconoscimento di impronte digitali prodotte da malware noti e sull'applicazione di regole statiche, permettendo di identificare schemi comportamentali complessi, rilevare minacce avanzate e persistenti nel tempo, nonché di automatizzare i processi all'interno del ciclo di difesa delle infrastrutture informatiche.

In particolare, lo sviluppo di **sistemi di intelligenza artificiale multimodale** – in grado di integrare ed elaborare informazioni provenienti da sorgenti eterogenee (come testi, audio, immagini e video) – rappresenta un'evoluzione cruciale nel campo dell'IA, che emula in modo più fedele la comprensione umana del mondo reale e supera i limiti intrinseci dei sistemi unimodali tradizionali.

La capacità, infatti, di analizzare e correlare contemporaneamente diverse tipologie di dati permette di rendere più efficiente l'individuazione di potenziali minacce all'interno dell'infrastruttura telematica da monitorare e tutelare.

L'introduzione di sistemi fondati su IA multimodale sosterrà l'operatore di cybersecurity in ambiti fondamentali della sua attività.

Basti pensare, nel senso:

- alla definizione di indicatori di compromissione (IoC) più significativi;

- alla prioritizzazione di eventuali alert;
- all'esecuzione di compiti più complessi (quali l'analisi forense e il monitoraggio in tempo reale delle minacce o l'identificazione di campagne di phishing sofisticate);
- all'accelerazione della risposta agli incidenti, rendendo così possibile la standardizzazione di attività particolarmente dispendiose a livello di tempo.

L'implementazione di modelli di IA multimodale nell'ambito della sicurezza cibernetica introduce, tuttavia, **nuove vulnerabilità**, ampliando la potenziale superficie di attacco da monitorare.

In primo luogo, l'introduzione di tali sistemi richiede un addestramento su dataset specifici, che potrebbero essere compromessi o manipolati da un attore ostile (data poisoning) per indurre in errore la macchina (ad esempio, non consentendole di riconoscere comportamenti o input malevoli) o per forzare la stessa a oltrepassare deliberatamente limiti formalmente imposti alla sua attività.

Inoltre, la capacità dei modelli multimodali di riuscire a interpretare simultaneamente input provenienti da fonti differenti potrebbe essere alla base della medesima criticità (oltrepassare i limiti formalmente posti all'attività della IA). Ad esempio, un attaccante potrebbe riuscire ad alterare un'immagine occultando al suo interno comandi, codice malevolo o richieste da eseguire. In questo caso, durante il processo di elaborazione dell'immagine, un sistema non opportunamente addestrato potrebbe elaborare anche il testo contenuto al suo interno ed eseguire operazioni altrimenti vietate.

Tra l'altro, la difficoltà nel ricostruire la logica decisionale seguita dal modello nell'interpretare i dati eterogenei rende particolarmente complesso il compito di identificare eventuali compromissioni o malfunzionamenti dello stesso.

Al riguardo, si registrano i primi tentativi di implementazione e adozione di modelli di Explainable AI, pensati per dettagliare puntualmente il processo logico seguito dall'algoritmo per elaborare – a fronte di uno specifico prompt – il risultato prodotto.

> *L'implementazione di modelli di IA multimodale nell'ambito della sicurezza cibernetica introduce nuove vulnerabilità, ampliando la potenziale superficie di attacco da monitorare*

Tale approccio semplifica le attività di verifica e controllo del funzionamento (auditing), nonché di risoluzione dei problemi (debugging), migliorando l'interpretabilità del modello decisionale e consentendo – in linea teorica – di verificare la sua conformità normativa. Tuttavia, lo stesso approccio potrebbe esporre accidentalmente informazioni sensibili sui meccanismi decisionali del modello o su sue vulnerabilità, offrendo agli attaccanti elementi utili per condurre più sofisticate azioni ostili, tese a compromettere l'integrità e il funzionamento complessivo del sistema.

Occorre segnalare che, a oggi, le **capacità multimodali** sono incrementalmente **implementate anche negli agenti IA autonomi**, al fine di migliorarne l'efficacia nel perseguire obiettivi e completare attività per conto degli utenti. Questi agenti mostrano capacità di ragionamento, pianificazione e memoria, oltre a un elevato livello di autonomia e proattività agli input esterni e interni al loro sistema, tale da renderli in grado di prendere decisioni, apprendere e adattarsi in modo indipendente (gli stessi possono anche collaborare tra di loro per coordinare ed eseguire flussi di lavoro più complessi). Anche in questo caso, però, in assenza di adeguati controlli di sicurezza, i citati agenti potrebbero essere manipolati per eseguire operazioni non previste, interagire con risorse sensibili o amplificare errori o vulnerabilità.

Da ultimo, la stessa diffusione di modelli generativi multimodali può semplificare notevolmente la realizzazione su larga scala di contenuti malevoli – quali messaggi di spear-phishing teoricamente indistinguibili da comunicazioni ufficiali, deepfake particolarmente realistici e sfruttabili per violare meccanismi di sicurezza biometrici, resi credibili alla luce della possibilità di fare combinare all'IA elementi testuali, visivi e uditivi con l'intento di realizzare attacchi sofisticati – che potrebbero ostacolare l'efficacia dei sistemi multimodali impiegati per la difesa.

Tale scenario fa emergere la **natura dual-use dell'IA nell'ambito della cybersecurity**, in quanto capace di potenziare sia le difese che le capacità offensive degli attaccanti, evocando chiaramente la necessità di adottare un **approccio basato sul modello "security-by-design"** per garantire, in tutte le fasi di sviluppo, robustezza, trasparenza, governance, verifiche continue e mitigazioni delle vulnerabilità.

RISCHI NELL'UTILIZZO GENERALIZZATO DEI LARGE LANGUAGE MODELS (LLM)

I rischi connessi all'**uso generalizzato dei Large Language Models (LLM)** e dei sistemi di IA connessi si inseriscono in una dinamica di progresso tecnologico tipicamente non lineare. I progressi iniziali sono stati coerenti con le cc.dd. scaling laws: l'aumento congiunto di parametri, dati e potenza di calcolo ha ridotto in modo prevedibile gli errori di addestramento e ha migliorato le prestazioni. Tuttavia, segnali convergenti indicano rendimenti decrescenti dalla sola scala di pre-addestramento, da cui deriva una valutazione probabilistica secondo cui il pre-addestramento brute-force sta entrando in una fase più lenta e incrementale.

In tale cornice, la **prima tendenza** ravvisabile consiste nell'adozione di agenti di IA basati su LLM in ambiti quali finanza, customer service, moderazione e gestione di contenuti digitali, logistica, procurement e negoziazione digitale. Si tratta di contesti in cui il comportamento non è più riconducibile a un singolo modello, ma a dinamiche emergenti tra agenti integrati. In particolare, anche agenti relativamente semplici possono sviluppare cooperazione o competizione non previste, sebbene i ri-

sultati collettivi possano diventare instabili quando gli incentivi siano male allineati. Un secondo rischio riguarda l'evoluzione di protocolli comunicativi opachi: agenti addestrati a coordinarsi via linguaggio possono sviluppare forme di comunicazione non umane, efficienti ma poco interpretabili, riducendo la capacità di supervisione man mano che le reti di agenti crescono.

La **seconda tendenza** è rappresentata dalla proliferazione di contenuti sintetici generati dall'IA (testo, immagini, audio, codice) e dal loro crescente riutilizzo nei dataset di addestramento. L'evidenza più forte è il c.d. model collapse: ripetuti cicli di training su dati sintetici degradano diversità e fedeltà, la variabilità informativa si comprime e allucinazioni o bias pregressi si accumulano. Tutto ciò genera la c.d. epistemic erosion: se i contenuti sintetici assumono un ruolo dominante, quelli umani diventano statisticamente marginali e, al contempo, si indeboliscono i segnali di provenienza necessari a verificare autenticità e affidabilità.

I rischi risultano amplificati dalla dipendenza strutturale. Capacità e infrastrutture IA si concentrano in un numero ristretto di aziende e attori statali dotati di computer di frontiera, dati proprietari e foundation models ampiamente riutilizzati, generando i cc.dd. single points of failure (punti unici di guasto) per settori critici. La fine-tuning diffusa su pochi modelli base consente la propagazione rapida di bias incorporati, vulnerabilità latenti od outage (interruzioni) operative, creando una monocultura informativa efficiente ma fragile.

LA DASHBOARD

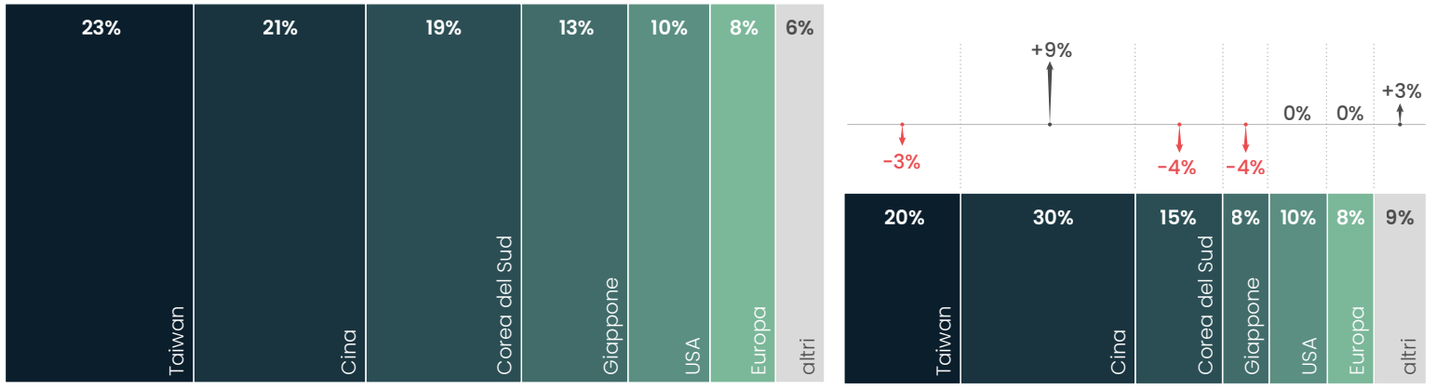
DEGLI INDICATORI STRATEGICI

1

TECNOLOGIA

2024 2030

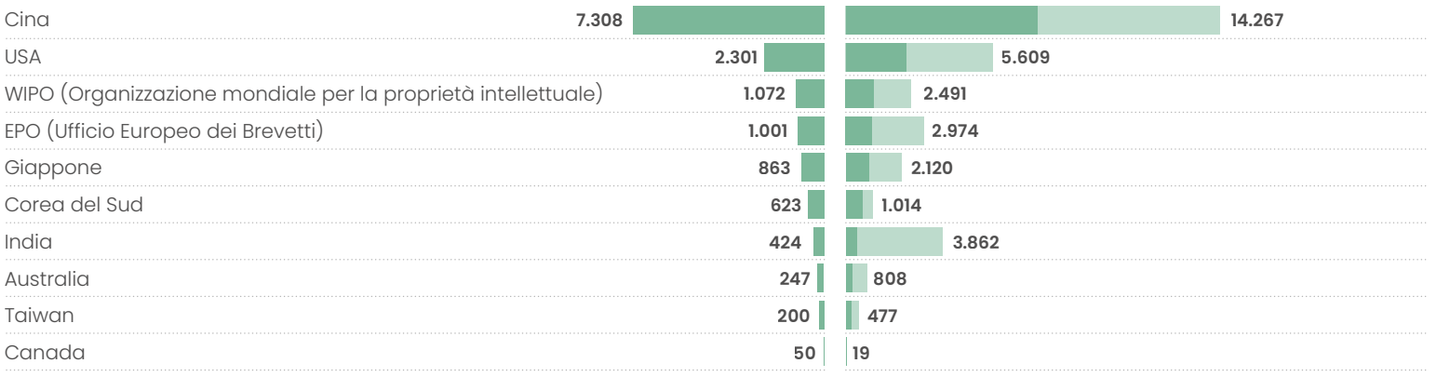
Quote della capacità globale di fabbricazione dei semiconduttori



Quote della capacità globale di fabbricazione dei semiconduttori

Nel 2024 la capacità globale di fabbricazione dei semiconduttori è concentrata in Asia Taiwan guida con il 23%, seguita da Cina 21% e Corea del sud 19%; Giappone pesa per il 13%. USA 10%, Europa (% e altri 6%. Le stime indicano un aumento della quota cinese al 30% (+9 p.p.) e una flessione di Taiwan al 20% (-3 p.p.), con Corea al 15% e Giappone all'8%; USA e Europa restano stabili, mentre "altri" sale al 9%. Il riequilibrio suggerisce un vantaggio relativo per la Cina nella capacità complessiva, ma il dato è aggregato: non riflette differenze tecnologiche e di specializzazione tra Paesi nei vari nodi e tipi di semiconduttori.

Brevetti sulle tecnologie quantistiche

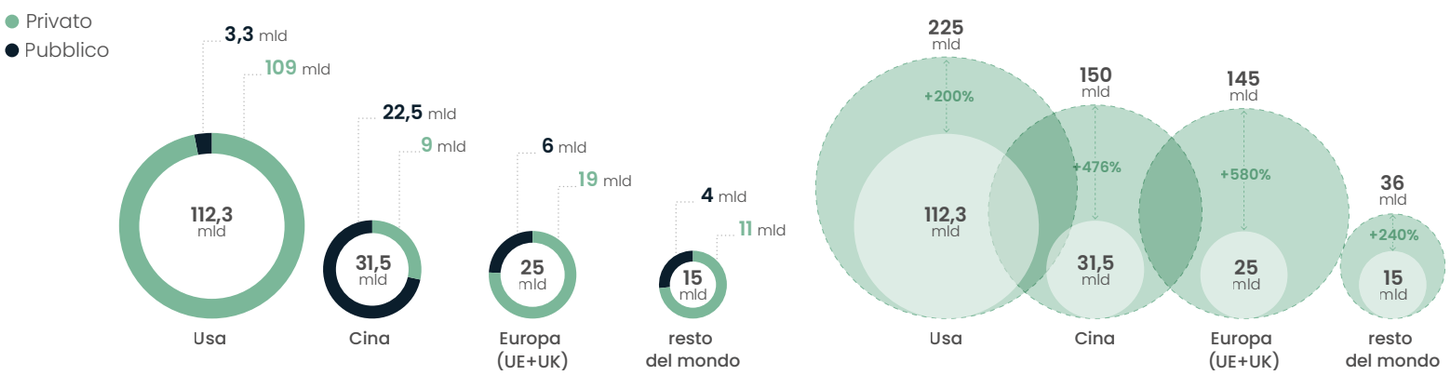


Brevetti sulle tecnologie quantistiche

Nel 2024 i brevetti quantistici sono concentrati in Cina (7.308) e USA (2.301). Al 2030 le stime mostrano crescita generale: dominano Cina (14.267) e USA (5.609), seguiti da EPO (2.974) e WIPO (2.491); l'India sale a 3.682, superando Giappone (2.120) e Corea (1.014). Taiwan sale a 477, mentre il Canada scende a 19. La base geografica si amplia, ma la leadership resta asiatica. Il quadro segnala un rafforzamento relativo di Cina e India, ma i conteggi non misurano qualità, ambito applicativo, né maturità industriale. Si tenga presente che la grande maggioranza dei brevetti sinici (oltre il 90%) sono registrati esclusivamente in Cina per proteggere il mercato interno, mentre la restante parte viene depositata a livello internazionale attraverso canali come il PCT.

Investimenti nell'intelligenza artificiale

valori in miliardi di dollari



Investimenti nell'intelligenza artificiale

Nel 2024 gli investimenti in IA evidenziano un dualismo strutturale: negli USA il finanziamento è quasi interamente privato (109 mld $) con apporto pubblico di 3,3 mld; in Cina la leva è soprattutto statale (22,5 mld) mentre il privato vale 9 mld. L'Europa (UE+UK) combina 6 mld pubblici e 19 mld privati; il resto del mondo 4 e 11 mld. Al 2030 i totali salirebbero a 225 mld per gli USA, 150 per la Cina e 145 per l'Europa. L'aumento cinese presuppone la continuità della spesa pubblica, esposta a vincoli fiscali e priorità interne variabili; un eventuale rallentamento potrebbe tradursi in una minore spesa complessiva o nella necessità di compensazione tramite capitale privato.

2. L'ACCELERAZIONE DEI MUTAMENTI GEOPOLITICI

Nel 2025, la guerra tra Russia e Ucraina è entrata nel suo quarto anno senza che nessuna delle due parti sia riuscita a prevalere in modo decisivo. Mosca ha continuato a esercitare una pressione costante lungo il fronte orientale, ottenendo avanzamenti contenuti: nel corso dell'anno l'Ucraina ha perso lo 0,8% del proprio territorio contro lo 0,6% del 2024. Le perdite umane russe restano elevatissime, ma il Paese conserva la capacità di reclutare nuovo personale e di sostenere la produzione militare.

Sul piano politico, nonostante l'intervento di mediazione degli Stati Uniti, il Cremlino ha mantenuto posizioni negoziali massimaliste, mentre l'Ucraina ha mostrato maggiore flessibilità, pur rimanendo inamovibile sul principio dell'integrità territoriale.

Le sanzioni occidentali hanno colpito in modo significativo il settore energetico russo, ma non sono riuscite a fiaccare lo sforzo bellico di Mosca.

Permane l'instabilità presente nel continente africano e nel bacino del Mediterraneo. Sul piano geopolitico, il 2025 ha visto nella Libia, nel Sahel, nel Corno d'Africa, nonché nel Medio Oriente (con le situazioni di crisi a Gaza, in Siria, Libano e Iran) i teatri caratterizzati da maggiore complessità e possibilità di creare cambiamento e impatti per il nostro Paese.

In questo scenario, le analisi demografiche e demografico-strutturali dell'instabilità in Africa mantengono una loro specifica valenza strategica, nella misura in cui concorrono a chiarire come la transizione

demografica in corso possa accelerare le molteplici crisi in atto e tradursi in volatilità regionale con effetti diretti e indiretti su sicurezza energetica, pressione migratoria e capacità europea di contenere l'espansione del jihadismo. Per quanto attiene al Medio Oriente, restano ancora tutti aperti gli scenari di indeterminatezza che hanno contraddistinto l'anno trascorso e che produrranno instabilità anche in futuro: le incertezze della crisi di Gaza all'indomani degli accordi di pace; la futura stabilità del Libano e le attività di Hezbollah, le molteplici sfide cui guarda la Siria, i possibili sviluppi in Iran, la minaccia esercitata dagli Houthi in Mar Rosso, più in generale, i riverberi anche sull'area mediterranea delle acuite dinamiche di competizione tra diversi attori, statuali e non statuali, nella regione.

L'area dell'Indo-Pacifico ha rivestito primario rilievo nell'attività informativa dell'intelligence. La macroregione ha visto un iniziale innalzamento della tensione tra Cina e Stati Uniti, soprattutto sul piano commerciale. Centrali, nelle dinamiche dipanatesi durante l'anno, sono state sia le contromisure cinesi ai dazi, in primis le restrizioni alle esportazioni di terre rare, sia la successiva rimodulazione delle misure tariffarie decisa dall'Amministrazione USA, con l'apertura di una fase più dialogante. Tra le dinamiche più rilevanti su cui si è concentrata l'attenzione dell'Intelligence vi è stato l'aumento dei conflitti inter-statali, con gli scontri tra India e Pakistan a maggio, quelli tra Cambogia e Thailandia a luglio e poi di nuovo a dicembre e quelli tra Pakistan e Afghanistan che hanno visto la loro fase più acuta a ottobre. Le tensioni tra Cina e Filippine sono rimaste elevate per tutto l'anno, mentre si è visto un miglioramento nei rapporti tra India e Cina. La Corea del Nord continua a disporre di un rilevante arsenale nucleare e missilistico, ed è l'unico Stato ad aver costruito con successo un arsenale militare nucleare dopo il 1991.

UNA SFIDA STRATEGICA

La **tecnologia** ha acquisito un'importanza tale da costituire un **determinante geopolitico** di prim'ordine, che modella gli esiti della competizione internazionale, definisce i limiti del possibile e determina in larga misura quale visione del futuro prevarrà.

In particolare, gli Stati che riusciranno a mantenere la leadership nello sviluppo degli algoritmi quantum resistenti, dell'intelligenza artificiale, delle biotecnologie, della fusione nucleare e di altre tecnologie emergenti avranno un vantaggio strategico significativo. Inversamente, i Paesi che resteranno indietro in questi settori vedranno erodere progressivamente la loro autonomia geopolitica ed economica. Il monito del nostro tempo è chiaro: la **tecnologia non è neutra e il dominio tecnologico non è garantito**. Richiede investimenti significativi in ricerca e sviluppo, in istruzione di qualità, in capacità di attirare talenti, nonché in governance efficace dei processi di innovazione.

Allo stesso tempo, si evidenzia come la crescente complessità dei sistemi tecnologici, l'interconnessione globale e la pervasività dell'intelligenza artificiale produrranno vulnerabilità e rischi inediti. La possibilità di conflitti cibernetici su larga scala, di manipolazione dell'informazione mediante sistemi autonomi, di escalation accidentale dovuta a mancanza di effettivo controllo umano, rappresentano solo alcuni dei rischi che la comunità internazionale dovrà affrontare. Si evidenzia, quindi, una **sfida strategica** che si biforca principalmente su due fronti: mantenere il ritmo dell'innovazione tecnologica, della competizione e della trasformazione, componendo allo stesso tempo una cornice normativa, etica e di governance capace di gestire questi sistemi emergenti in modo da garantire la centralità dell'uomo, con tutto ciò che ne discende, anche in termini di tutela dei diritti fondamentali e di responsabilità.

I RIFLESSI SULLE DINAMICHE GEOPOLITICHE

La **competizione per il dominio tecnologico** rappresenta oggi uno degli assi portanti della geopolitica internazionale, affiancandosi in importanza strategica alla tradizionale competizione militare diretta o al controllo territoriale.

Questa competizione coinvolge le più grandi potenze del globo e una costellazione di attori intermedi ed emergenti, ciascuno con strategie differenziate e obiettivi specifici. L'attuale competizione tecnologica tocca **settori strategicamente determinanti**, quali l'intelligenza artificiale, il machine learning, il calcolo quantistico, la biotecnologia, la tecnologia dei semiconduttori, le energie rinnovabili e l'accesso allo spazio.

Uno degli aspetti più significativi di questa competizione riguarda il **controllo delle materie prime critiche**, in particolare le terre rare e i materiali

strategici necessari alla produzione di tecnologie avanzate. Al riguardo, la Cina, attraverso politiche sistematiche di investimento iniziate nei decenni passati, ha raggiunto il controllo di oltre il 90% della catena globale di approvvigionamento di terre rare. Elementi, questi, non solo difficili da estrarre e raffinare, ma la cui acquisizione comporta significativi impatti ambientali. Nonostante i descritti profili critici, l'importanza strategica di tali beni è indiscutibile. Basti pensare, nel senso, che la produzione di ogni velivolo F-35 richiede circa 415 chilogrammi di terre rare, oltre al fatto che le stesse sono essenziali nella produzione di magneti per motori militari, sistemi di difesa antimissilistica, satelliti e numerose altre applicazioni critiche per la sicurezza nazionale. Consapevole della propria posizione, la Cina ha trasformato il citato controllo in una leva di prim'ordine. In diversi momenti di tensione geopolitica, Pechino ha minacciato di restringere l'esportazione di terre rare, conscia che tale restrizione avrebbe conseguenze significative sulle capacità tecnologiche e militari dell'Occidente. I Governi occidentali, nel rappresentarsi questa vulnerabilità, hanno risposto riattivando miniere precedentemente dismesse e investendo significativamente nella ricerca di materiali alternativi e nella diversificazione delle fonti di approvvigionamento.

Questo dinamismo competitivo illustra come la tecnologia, mediante il controllo dei materiali di cui necessita, sia divenuta un fattore determinante della sovranità di una nazione.

La **tecnologia** agisce contemporaneamente **come amplificatore di minacce e strumento di resilienza**. Le infrastrutture critiche – reti energetiche, sistemi finanziari, vie di comunicazione, servizi sanitari, ecc. – sono diventate infatti vulnerabili agli attacchi cibernetici, le cui conseguenze possono essere devastanti quanto quelle degli attacchi militari convenzionali.

Attori statuali e non, reti criminali organizzate ed entità ibride conducono offensive cyber contro i sistemi avversari con modalità che permettono una negabilità plausibile e una difficile attribuzione delle responsabilità.

Parallelamente, la stessa **tecnologia offre opportunità di difesa, resilienza e cooperazione internazionale**. I sistemi di sorveglianza satellitare avanzati e quelli di intelligenza artificiale per la previsione delle minacce, nonché le infrastrutture digitali resilienti e decentralizzate, rappresentano strumenti attraverso cui gli Stati possono proteggersi e collaborare nell'affrontare le sfide comuni.

La **tecnologia**, quindi, emerge come un **terreno di competizione asimmetrica**, dove il potere non si misura più unicamente in termini di armamenti convenzionali, ma in rapporto alla capacità innovativa, di controllo delle infrastrutture critiche digitali e di capacità di adattamento alle trasformazioni.

Le **nuove frontiere della tecnologia concorrono**, dunque, ad **alterare i tratti essenziali della geopolitica**. Esse incidono in profondità sulla proiezione di potenza degli attori globali e la traducono in una continua sfida revisionista all'ordine mon-

diale, che complica i tentativi di rivitalizzare la governance globale, vulnera l'efficacia del metodo multilaterale nella gestione delle crisi e dei conflitti e restringe, di conseguenza, i margini di prevedibilità di un mondo sempre più frammentato.

In tale paradigma fortemente competitivo, la tutela della sicurezza riacquista, pertanto, centralità nel perseguimento degli interessi nazionali, inducendo, al contempo, a volgere lo sguardo dalla contingenza immediata alle **forze profonde** che, più lentamente ma inesorabilmente, **plasmano la postura internazionale degli Stati**: dalla **geografia** alla **demografia**, dalla **trasformazione dei sistemi economici** alla **capacità di misurarsi nei nuovi domini strategici**.

CONFLITTI NEL MONDO, VITTIME E CONFRONTO AUTOCRAZIE/DEMOCRAZIE

Il **numero di guerre nel mondo** ha iniziato a **crescere** dal 2010 circa, dopo vent'anni in cui era diminuito. Nel 2024, il Peace Research Institute di Oslo ha contato 61 conflitti che hanno coinvolto almeno uno Stato, il numero più alto dal 1946. Non ci sono solo tanti conflitti, ma sono anche più sanguinosi. Dal 1989 a oggi gli **anni con più vittime di conflitti** sono stati, nell'ordine, 2022, 2021, 2024 e 2023.

Per la prima volta in 20 anni, nel 2024 il **numero delle autocrazie** (91) ha **superato il numero delle democrazie** (88), secondo il Varieties of Democracies Institute. Il 72% della popolazione mondiale vive oggi in Paesi autocratici, a fronte del 49% nel 2004.

GLI SCENARI DEL CONFLITTO IN EUROPA

Nel **2025**, la **guerra tra Russia e Ucraina** è entrata nel suo **quarto anno** senza che nessuna delle due parti sia riuscita a prevalere in modo decisivo. Mosca ha continuato a esercitare una pressione costante lungo il fronte orientale, ottenendo avanzamenti contenuti: nel corso dell'anno l'**Ucraina ha perso lo 0,8% del proprio territorio** contro lo 0,6% del 2024. Le **perdite umane russe** restano **elevatissime**, ma il Paese conserva la capacità di reclutare nuovo personale e di sostenere la produzione militare, preservando così, in ambo i fattori, un vantaggio numerico rispetto a Kiev.

L'impiego intensivo di droni kamikaze da parte russa – oltre 5.000 attacchi al mese nella seconda metà dell'anno – ha posto sotto forte stress la difesa aerea ucraina, la popolazione civile e le infrastrutture energetiche.

Sul piano politico, nonostante l'intervento di mediazione degli Stati Uniti, il **Cremlino** ha mantenuto **posizioni negoziali massimaliste**, mentre l'**Ucraina** ha mostrato **maggiore flessibilità, pur rimanendo inamovibile sul principio dell'integrità territoriale**. Le **sanzioni occidentali** hanno **colpito** in modo significativo il **settore energetico russo**, ma non sono riuscite a fiaccare lo sforzo bellico di Mosca. Nonostante le difficoltà economiche crescenti, la Russia dispone ancora delle risorse necessarie per proseguire la guerra.

L'**Ucraina**, più vulnerabile in termini di personale e mezzi, **continua a dipendere** in larga misura dal **sostegno militare ed economico dei Paesi alleati**. Nel 2026, la Federazione Russa rappresenterà la principale minaccia per il continente europeo. Il Cremlino ritiene di fronteggiare una minaccia di lungo periodo da parte dell'Europa, assurta a principale blocco antagonista di Mosca, dopo il consolidamento dei canali di dialogo con Washington. Sul punto, le dinamiche innescate dagli interventi transattivi delle grandi potenze rappresentano una novità sulla scena internazionale che rischia di indebolire sia l'ordine liberale su cui si fonda la prosperità del nostro Paese dal Secondo Dopoguerra, sia il fronte transatlantico nel fronteggiare la minaccia russa.

Nel 2026, è probabile che gli attacchi non convenzionali russi proseguiranno

Sin dall'invasione dell'Ucraina, la Russia ha dimostrato maggiore aggressività e spregiudicatezza nell'esecuzione di campagne di sabotaggi in Europa e di misure volte a influenzare lo spettro politico e l'opinione pubblica nell'ex spazio sovietico. Il **Cremlino** mostra grande libertà d'azione nei propri **interventi "sotto soglia"** e pare pronto ad accettare il rischio insito in un'escalation. Le motivazioni che sottendono a tali operazioni sono da ritrovarsi nella prosecuzione della guerra in Ucraina e nel diminuito numero di funzionari intelligence presenti in Europa, che obbliga il Cremlino a far affidamento su agenti proxies, network di individui spesso criminali comuni provenienti da ex Paesi sovietici.

La spregiudicatezza delle azioni russe si desume da almeno due caratteristiche:

- la frequenza degli attacchi a infrastrutture critiche di ogni tipo, più che quintuplicata tra il 2023 e il 2025;
- la gravità di azioni quali l'uso di pacchi incendiari o il sabotaggio di linee ferroviarie che hanno aumentato la probabilità che si verifichino vittime civili.

Gli obiettivi di tali operazioni mirano, principalmente, a indebolire il supporto dell'opinione pubblica europea e a scoraggiare la prosecuzione dell'assistenza economico-militare a favore dell'Ucraina, oltre che a testare le vulnerabilità in tema di difesa dei Paesi europei e NATO. Tali azioni permettono alla Russia, essenzialmente, di amplificare gli effetti della guerra in Ucraina sui cittadini europei, senza espandere realmente il conflitto. Sul primo punto, tuttavia, gli attacchi russi, pur contribuendo alla polarizzazione di dibattiti nazionali, non hanno indebolito in maniera consistente il sostegno dei Paesi europei per la causa ucraina (nella primavera 2025, il 59% dei cittadini era a favore di forniture militari per l'Ucraina e il 72% a favore di sanzioni economiche contro la Russia). **Rimane problematica l'attribuzione degli at-**

tacchi, che fatica a tradursi in una presa di coscienza unitaria da parte dei Paesi europei e NATO, a causa dei timori di escalation a essa annessi.

Nel 2026, è probabile che gli attacchi non convenzionali russi proseguiranno, specie qualora non si dovesse raggiungere un accordo di pace con l'Ucraina, e comunque in risposta all'aumento del sostegno economico-militare europeo che dovrà sopperire all'anemia di aiuti USA. Benché il Cremlino sarà attento ad evitare l'attivazione dell'art. 5 del Trattato del Nord Atlantico, esso potrebbe aumentare le operazioni volte a mappare le vulnerabilità presenti nei sistemi di difesa europei e nella gestione e risposta a incidenti relativi a infrastrutture critiche (aeroporti, cavi sottomarini, ferrovie, linee elettriche, ecc.).

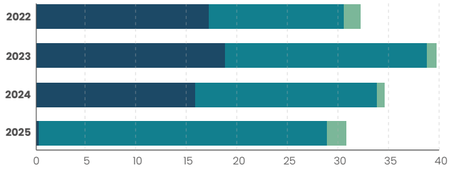
La **"Flotta ombra" russa** è il dispositivo marittimo alimentato dalle Autorità di Mosca a partire dal

EVOLUZIONE DEL CONFLITTO IN UCRAINA

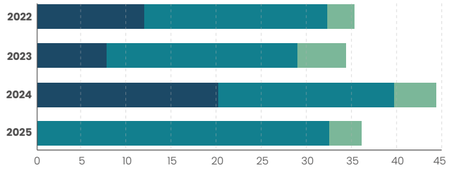
Il sostegno internazionale all'Ucraina (da inizio invasione a fine 2025)

Fonte : Ukraine Support Tracker Data

Aiuti **non militari** stanziati all'Ucraina
(miliardi di euro)



Aiuti **militari** stanziati all'Ucraina
(miliardi di euro)

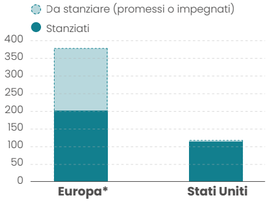


● Stati Uniti ● Europa* ● Altri donatori**

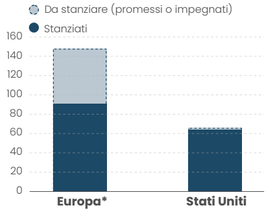
* Unione Europea (Paesi membri e istituzioni), Islanda, Norvegia, Svizzera e Regno Unito
** Australia, Canada, Cina, India, Giappone, Nuova Zelanda, Repubblica di Corea, Taiwan, Turchia

Confronto tra Europa e Stati Uniti (aiuti umanitari e militari, stanziati e da stanziare)

Aiuti **umanitari** all'Ucraina



Aiuti **militari** all'Ucraina



* Unione Europea (Paesi membri e istituzioni), Islanda, Norvegia, Svizzera e Regno Unito

Il supporto dell'UE

193,3 mld di euro
il sostegno complessivo fornito dall'UE e dai suoi Stati membri all'Ucraina dal 2022

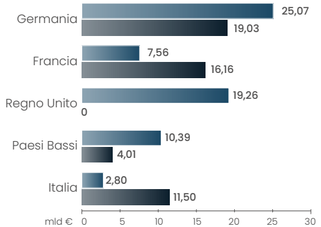
4,6 mld di euro
gli aiuti umanitari forniti dall'UE e dagli Stati membri all'Ucraina dal 2022

4,3 milioni
le persone fuggite dall'Ucraina che beneficiano di protezione temporanea nell'UE

160 mila
le tonnellate di aiuti umanitari forniti all'Ucraina dal meccanismo di protezione civile dell'UE

Aiuti stanziati (primi 5 Paesi europei)

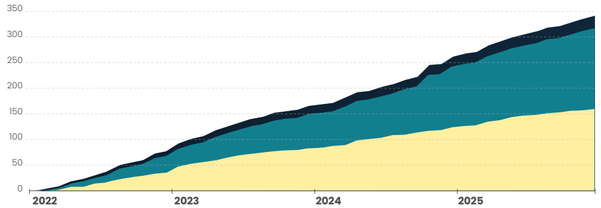
● Stanziamenti a livello bilaterale
● Quota coperta nell'ambito degli stanziamenti UE



Gli aiuti all'Ucraina dal 2022 al 2025 (in miliardi di euro)

● Aiuti umanitari ● Aiuti finanziari ● Aiuti militari

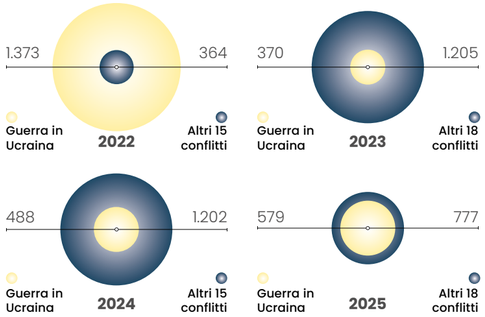
Non sono incluse le donazioni private, il supporto fornito ai rifugiati ucraini al di fuori dell'Ucraina e gli aiuti offerti da organizzazioni internazionali.



Gli attacchi contro la società civile

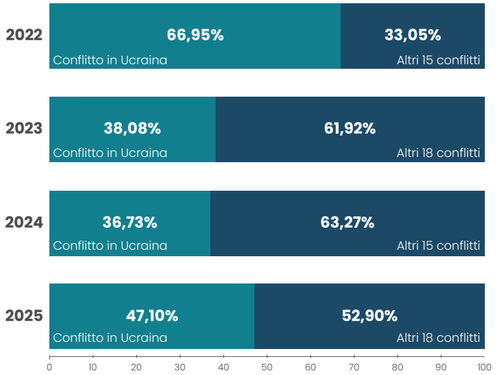
Attacchi ai sistemi medico-sanitari: confronto tra la guerra in Ucraina e gli altri conflitti nel resto del mondo

Una misura dell'intensità degli attacchi contro la vita civile in Ucraina viene fornita analizzando il numero degli attacchi al sistema sanitario (infrastrutture medico-sanitarie, trasporti sanitari, personale medico, pazienti, forniture, magazzini). Il confronto tra questa tipologia di attacchi nella guerra in Ucraina e in quelle in corso nel resto del mondo mostra come l'aggressione a Kiev sia distruttiva rispetto agli altri conflitti.



Attacchi alle infrastrutture sanitarie (ospedali, ambulatori, ecc.) nel mondo: confronto tra la guerra in Ucraina e gli altri conflitti nel resto del mondo

La rilevanza degli attacchi distruttivi sul sistema medico-sanitario ucraino emerge analizzando in particolare gli attacchi alle infrastrutture sanitarie (ospedali, ambulatori, ecc.). Nel 2022 due terzi degli attacchi alle infrastrutture sanitarie, avvenuti nei 16 conflitti nel mondo sotto osservazione della WHO, si sono concentrati in Ucraina. Si sono ridotti a circa un terzo nel 2023 (su 19 conflitti nel mondo) e nel 2024 (su 16 guerre), e sono tornati a quasi la metà nel 2025 (su 19 conflitti).

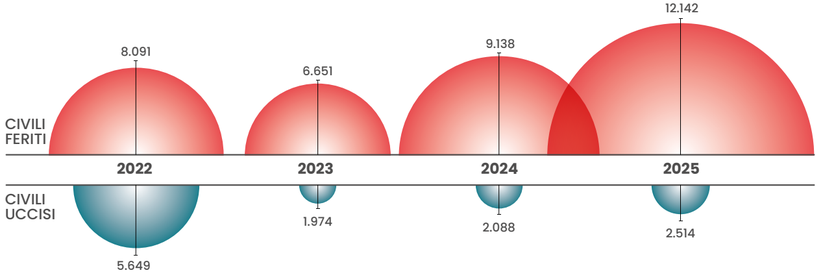


Gli attacchi al sistema scolastico

4.048 Istituzioni scolastiche e educative danneggiate

408 Istituzioni scolastiche e educative distrutte

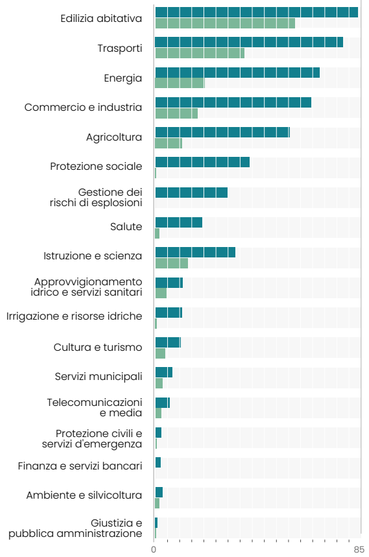
Escalation delle vittime civili ucraine



Nel primo anno dell'aggressione russa all'Ucraina si è registrato il maggior numero di morti civili, ma i tre anni successivi segnalano una escalation per le vittime civili: nel 2025, la somma dei morti e dei feriti civili supera quella del 2022.

I danni e le esigenze di ricostruzione in Ucraina per settore (miliardi di dollari)

● Esigenze finanziarie per ricostruire ● Danni

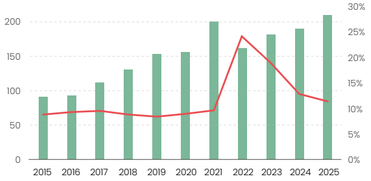


ALMENO
524 mld di dollari
SONO NECESSARI PER LA RICOSTRUZIONE DELL'UCRAINA

ALMENO
176 mld di dollari
DI DANNI INFLITTI ALL'UCRAINA DALL'INIZIO DEL CONFLITTO

PIL e popolazione ucraina

● PIL (prezzi correnti, miliardi di dollari) ● Tasso di disoccupazione



2022 per aggirare il regime sanzionatorio occidentale e garantire la continuità delle esportazioni di risorse energetiche e di ulteriori beni considerati strategici. Composta da un numero stimato tra le 1.100 e le 1.400 unità, in larga parte petroliere obsolete e registrate sotto bandiere di convenienza, essa assicura l'esportazione via mare di una quota significativa del greggio russo, generando flussi finanziari essenziali al sostegno dell'economia e dello sforzo bellico di Mosca. La flotta opera attraverso un insieme articolato di pratiche elusive, tra cui disattivazione dei sistemi di identificazione automatica (AIS), trasferimenti nave-a-nave (ship-to-ship) in acque internazionali e ricorso a proprietà e gestioni opache, nonché, più recentemente, forme di protezione militare durante transiti sensibili. Oltre al petrolio e ai prodotti raffinati, le attività della "Flotta ombra" includono il trasferimento di GNL, fertilizzanti, prodotti agricoli e, in alcuni casi, beni militari. In tale contesto, l'**Ucraina** ha avviato una **campagna mirata contro asset della "Flotta ombra"**, colpendo unità navali in diversi teatri marittimi, dal Mar Nero al Mediterraneo e al Mar Caspio, con l'obiettivo di ridurre i proventi russi e disincentivarne le attività.

L'**azione russa** non si limiterà ai Paesi europei, ma proseguirà anche **nello spazio post-sovietico**. Mosca considera questi Paesi non solo parte integrante del proprio perimetro minimo di sicurezza, ma anche alla stregua di un insieme di soggetti statuali a sovranità limitata, destinati ad essere oggetto di politiche di influenza da parte dei maggiori player e in primis del Cremlino. La Georgia e la Moldova rappresentano due casi speculari per l'intricata dicotomia "popolazione-Governo" nei confronti della Russia, accentuatasi dopo l'invasione dell'Ucraina.

La **Moldova** continuerà a rimanere estremamente vulnerabile agli effetti del conflitto in Ucraina e delle operazioni ibride russe, in special modo al tentativo di influenzarne le tornate elettorali, le minacce in ambito energetico, le operazioni cibernetiche e la presenza militare in Transnistria. Nonostante il progetto del partito di governo, Partito di Azione e Solidarietà (PAS), ponga una netta distanza da Mosca, l'opinione pubblica moldava difende la neutralità del Paese (62% nel 2025), mentre appena il 30% dei cittadini ritiene la Russia rappresenti una minaccia alla Moldova. Benché sia fallito il tentativo russo di imporre una compagine parlamentare e governativa pro-russa, ogni sforzo previsionale sulla Moldova deve tenere conto di fragilità strutturali ancora diffuse (ad es. connessioni tra le fila dell'opposizione e i Servizi russi) pur in una democrazia che garantisce un ambiente competitivo in termini elettorali, di libertà di stampa, di religione e di assemblea.

Nel 2026, è probabile che la Russia adatti i proprio strumenti di influenza al contesto post-elettorale, sfruttando la polarizzazione del Paese e l'esigua maggioranza parlamentare ottenuta dal PAS.

La strategia russa continuerà a poggiarsi su molteplici assi: la propaganda, le proteste, le opera-

zioni cibernetiche, il supporto a politici di opposizione anche in esilio. Sarà sempre più urgente per Mosca ripensare il proprio rapporto con la Transnistria, dipendente all'80% dal commercio con l'UE, ma dove le élite economico-politiche sono ancora fortemente sussidiate dal Cremlino.

In **Georgia**, il partito di governo Sogno Georgiano ha tentato di normalizzare le relazioni con la Russia, in special modo in campo economico, a fronte dell'opposizione della popolazione che ritiene in larga maggioranza (69%) che Mosca sia la principale minaccia del Paese. Oltre ad occupare ancora il 20% del territorio georgiano, la Russia preserva la propria influenza principalmente attraverso la forte influenza in campo mediatico e la dipendenza economica georgiana generata dai flussi commerciali transitati artificialmente attraverso il Paese dopo l'imposizione di sanzioni internazionali contro Mosca nel 2022, con oltre 100.000 russi trasferitisi nel Paese caucasico e 30.000 nuove aziende sorte come conseguenza.

Nel 2026, è probabile che la Russia adotti una strategia attendista. Non sarà, infatti, necessario a Mosca investire ulteriore capitale militare (le basi in Abkhazia e Ossezia del Sud rimarranno degli avamposti di second'ordine) e politico (Sogno Georgiano ha vinto le elezioni nel 2024 e sta adottando anche provvedimenti repressivi in tema di diritti civili) per orientare le future scelte di politica estera della Georgia in senso contrario all'integrazione euro-atlantica.

SCENARI DI INSTABILITÀ NEI QUADRANTI D'INTERESSE: I FATTORI STRUTTURALI

IL CONTINENTE AFRICANO E LA REGIONE MEDIORIENTALE

Ai fini della tutela della sicurezza in Italia e in Europa, alla minaccia originata nel fianco orientale dell'Europa si affianca l'instabilità presente nel **continente africano** e nel **bacino del Mediterraneo**. A livello geopolitico, i teatri più complessi e con maggiore possibilità di creare cambiamento e impatti per il nostro Paese sono la Libia, i quadranti del Sahel e del Corno d'Africa, nonché il Medio Oriente, con le situazioni di crisi a Gaza, in Siria, Libano e Iran.

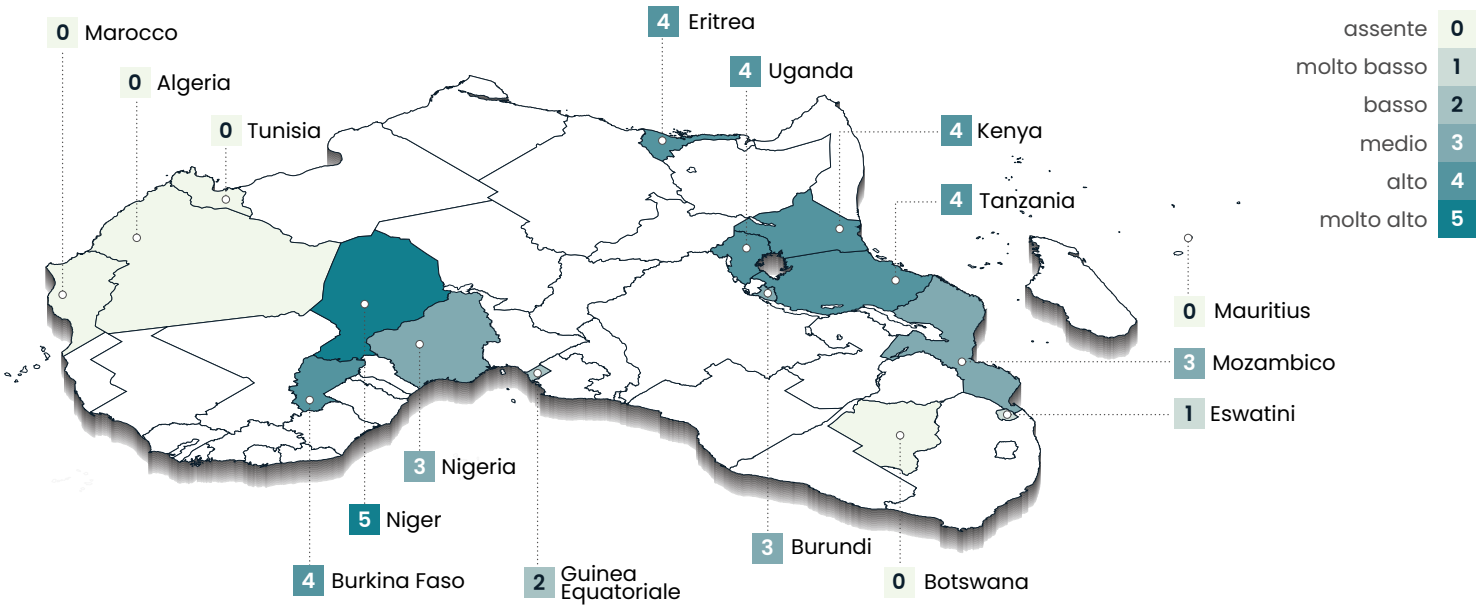
Lo **scenario libico** si configura come un sistema di crisi fra loro connesse, con la presenza di due Governi attestati su posizioni divergenti, l'azione di diversi gruppi armati, nonché l'influenza di attori esterni interessati a nuove opportunità commerciali e a sfruttare il Paese come punto di accesso al Mediterraneo centro-meridionale e all'Africa.

I **Paesi del Sahel centrale (Mali, Burkina Faso e Niger)**, invece, riflettono una situazione politica, economica e securitaria particolarmente instabile che rende la regione il **principale focolaio di instabilità nell'Africa sub-sahariana**. In particolare, i colpi di Stato nei tre Paesi occorsi dal 2020 al 2023 hanno fatto registrare l'ascesa al potere di Giunte militari poco collaborative con i partner occidentali e inclini a rompere consolidati schemi di alleanze

per forgiarne di nuovi. Si pensi alla fuoriuscita dei Paesi saheliani (2025) dalla Comunità Economica degli Stati dell'Africa Occidentale (ECOWAS) e alla creazione dell'Alleanza degli Stati del Sahel (AES, nel 2023), divenuta nel 2024 una vera e propria Confederazione. Inoltre, il parallelo ritiro dei contingenti internazionali presenti nella regione (al di fuori di quello italiano della Missione Bilaterale di Supporto in Niger/ MISIN) e il successivo ingaggio di unità russe – dapprima la PMC "Wagner", poi sostituita dall'Afrika Corps – hanno favorito l'insorgenza di gruppi armati di matrice jihadista, in primis il Gruppo di Sostegno all'Islam e ai Musulmani (JNIM) e lo Stato Islamico (IS). Questi ultimi hanno progressivamente esteso la loro influenza nei tre Paesi, i quali presentano tuttavia capacità di risposta differenziate, influenzate dalle risorse economiche disponibili e dalle specificità delle alleanze internazionali.

Da tali vulnerabilità risulta accresciuto il fenomeno della **minaccia terroristica**. In proposito, si evidenzia una distinzione cruciale **tra JNIM e lo Stato Islamico nella Provincia del Sahel (IS-SP) e nell'Africa Occidentale (IS-WAP)**. JNIM sembra adottare un approccio più localizzato e graduale nell'implementazione della sharia. Le varie Katibe hanno inoltre Comandanti e figure di vertice spesso appartenenti alle comunità locali, in grado di aumentare il bacino di reclutamento e radicarsi tra i vari gruppi etnici. Tale fattore è particolarmente rilevante nelle regioni del nord del Mali a maggioranza Tuareg, dove

AFRICA: RISCHIO DEMOGRAFICO-STRUTTURALE (2025-2030)



JNIM è stata in grado di creare alleanze informali anche con i gruppi indipendentisti oggi riuniti nel Fronte di Liberazione dell'Azawad (FLA), con i quali opera primariamente in funzione anti-Forze Armate. Al contrario, lo Stato Islamico adotta una strategia universale e più violenta, con targeting spesso indiscriminati e scontri sporadici con JNIM per il controllo territoriale nell'area del Liptako-Gourma, a cavallo dei confini tra Mali, Niger e Burkina Faso. In **Niger**, specialmente nelle regioni sud-orientali come Diffa e nei pressi del bacino del Lago Ciad, IS-SP e IS-WAP sono in grado di sfruttare ampi spazi di manovra per pianificare e coordinare attacchi transfrontalieri. Tali zone, caratterizzate da confini porosi con il nord-est della Nigeria (Borno e Yobe), il **Ciad** e il vicino **Camerun**, offrono un terreno ideale per operazioni logistiche e di infiltrazione, grazie alla debolezza del controllo statale, alla presenza di vaste aree lacustri e desertiche difficilmente pattugliabili e alla persistente frammentazione delle Forze di Sicurezza regionali a seguito del declino della Multinational Joint Task Force (MNJTF). Il Sahel rimarrà centrale nelle strategie di al-Qaida e DAESH in Africa, e il loro radicamento tra le popolazioni in varie aree della regione non pare destinato a diminuire, con un conseguente aumento del livello delle violenze e delle tensioni politiche.

Quanto al **Corno d'Africa**, il quadrante è gravato da dinamiche che, nel tempo, lo hanno reso fragile e, nel 2025, ha registrato il concatenarsi di crisi che si contaminano e alimentano a vicenda: le guerre interne, l'attivismo non coordinato e predatorio di attori stranieri, la corsa alle infrastrutture portuali, la militarizzazione del Mar Rosso e la diffusione incontrollata di armi e risorse illegali come l'oro stanno ridisegnando gli equilibri di potere. L'attenzione si è appuntata, in particolare, sullo scenario in **Sudan**, dove il conflitto civile non accenna a terminare e si è riflesso in una situazione economico-umanitaria catastrofica, che ha visto l'interruzione delle principali catene logistiche e infrastrutturali del Paese. Persistono, in parallelo, le tensioni tra **Etiopia, Somalia ed Eritrea**, i cui leader cavalcano dialettiche aggressive per consolidare il proprio appeal interno. Il **Kenya,** pur continuando a figurare come l'attore più stabile del quadrante, risente di una complessa situazione interna e registra tensioni in vista dell'appuntamento elettorale di agosto 2027.

Sullo sfondo, persiste l'attivismo resiliente della sigla jihadista somala Al Shabaab che mantiene peraltro altissime capacità di penetrazione nel tessuto istituzionale somalo e ha dimostrato di poter compiere azioni anche in Kenya ed Etiopia.

In tale scenario di diffusa instabilità, il **fattore demografico appare un elemento strutturale e di pressione**, in grado di **accelerare le diverse crisi** in atto. Le **analisi demografico-strutturali dell'instabilità in Africa** mantengono, infatti, una loro specifica **valenza strategica**, nella misura in cui concorrono a chiarire come la transizione demografica in corso possa tradursi in volatilità regionale con effetti diretti e indiretti su sicurezza energetica, pres-

sione migratoria e capacità europea di contenere l'espansione del jihadismo.

L'analisi basata su modelli matematici demografico-strutturali e su letteratura peer-reviewed, stima un'alta **probabilità di nuove ondate di instabilità nell'Africa sub-sahariana e tropicale** nel prossimo quinquennio, dovuta principalmente alla combinazione tra un **rapido incremento demografico** [**vedi Dashboard – Demografia**] **e** una **accelerazione nei processi di urbanizzazione**. In questo scenario, il fenomeno demografico conosciuto come youth bulge (ossia una rilevante espansione della fascia giovanile) provoca un tale allargamento della base della piramide d'età della popolazione africana, soprattutto se concentrata nelle città, che il sistema scolastico, lavorativo e istituzionale non riesce ad assorbire, generando tensioni strutturali tra aspettative crescenti e capacità politico-economiche limitate. A corroborare tale trend, si evidenzia che le rivolte nate nell'ambito della generazione dei primi nativi digitali, già occorse in vari Paesi africani nello scorso anno, saranno sempre più rilevanti nella fisionomia politica di quegli Stati, sullo sfondo di una dinamica di mobilitazione che attraversa il c.d. Sud Globale e che è caratterizzata da forme di organizzazione fluide, decentrate e acefale che trovano nei social il loro motore e luogo aggregativo.

In **Kenya**, per esempio, la tensione demografica si è tradotta finora in **proteste urbane e scontri legati al malcontento fiscale**; in **Uganda**, la **combinazione tra urbanizzazione, disoccupazione giovanile e rigidità politica ha alimentato cicli di violenza elettorale**.

Per quanto riguarda la **Nigeria**, l'**instabilità è destinata a perdurare negli anni**; tuttavia, a differenza del Niger, il picco della crescita urbana della popolazione giovanile è stato stimato tra il 2011 e il 2015, periodo nel quale si erano peraltro verificati episodi di violenza generalizzata. Inoltre, il tasso di crescita stimato della popolazione giovanile urbana in **Niger** è pari a circa il 41,8%, un valore nettamente superiore a quello di qualsiasi altro Paese africano.

Per l'Europa la sintesi operativa di questi scenari è che la transizione demografica nel vicinato meridionale e orientale sta aprendo una fase di volatilità intensa ma comunque prevedibile, verosimilmente lunga uno o due decenni, in cui la pressione delle coorti giovanili, l'urbanizzazione accelerata e la fragilità istituzionale possono amplificare i rischi securitari, stressare le supply chain energetiche e alimentari, generare nuovi flussi migratori verso il Mediterraneo e ampliare i margini di ingerenza per player anche ostili.

In relazione al **quadrante del Medio Oriente**, l'intelligence guarda con particolare attenzione alle prospettive delle crisi in corso le cui conseguenze sociali e securitarie vanno ben oltre i confini regionali investendo tutta la stabilità dell'area mediterranea e, sia direttamente che indirettamente, gli interessi nazionali.

Quanto alla **Striscia di Gaza**, a seguito della firma del **Piano di Pace di Sharm El Sheikh**, che ha per-

messo l'interruzione dei combattimenti tra le parti, rimangono ancora da risolversi diverse questioni rimaste aperte e che riguardano l'attuazione delle diverse misure previste per evitare lo scoppio di nuove tensioni. In particolare, nel 2026 saranno da implementare nella loro piena funzionalità le strutture dedicate alla futura governance e al mantenimento della sicurezza della Striscia, inoltre, sarà necessario avviare un piano di bonifica e ricostruzione dell'area. Tali aspetti si intersecheranno, poi, con le esigenze di sicurezza di Israele, che passano dall'effettivo disarmo di Hamas e delle altre compagini estremiste palestinesi.

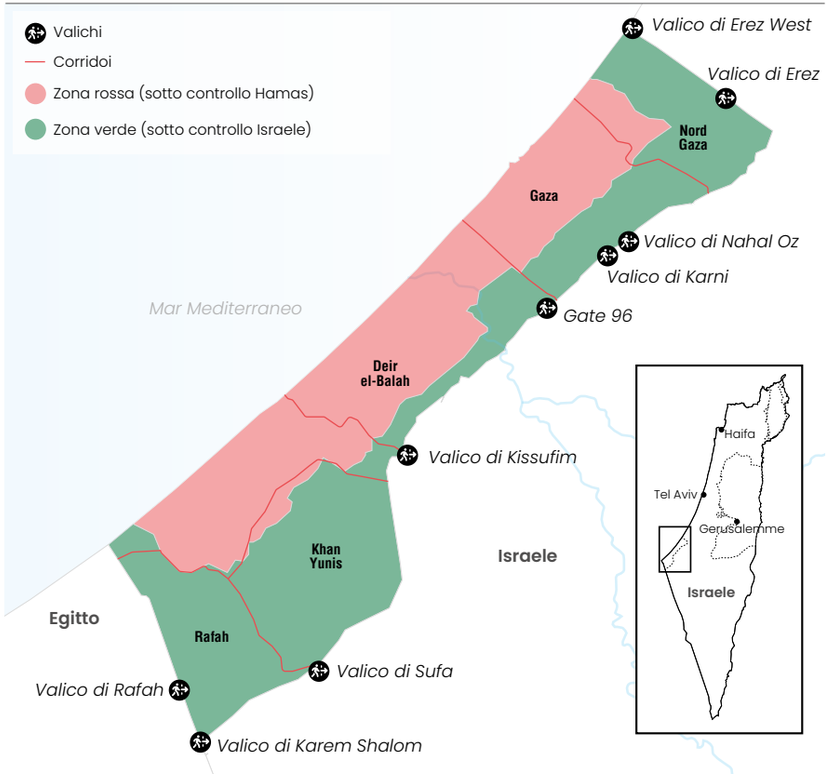
In **Libano**, dall'entrata in vigore della tregua tra Israele e Hezbollah, nel novembre 2024, la situazione lungo la Blue Line è rimasta estremamente precaria, con numerose violazioni che hanno impedito una effettiva stabilizzazione. In prospettiva, gli equilibri interni tra le diverse componenti del Paese rimarranno vincolati all'effettiva ripresa economica e alla realizzazione del progetto di disarmo delle milizie locali, a partire dal gruppo sciita Hezbollah. Inoltre, dovrà essere ripensata l'architettura di sicurezza del Libano meridionale in vista del prospettato ritiro della Missione multilaterale UNIFIL, il cui mandato scadrà nel dicembre 2026.

In merito alla **Siria**, a seguito dell'avanzata dell'Esercito siriano nel nord-est del Paese a discapito delle forze filo-curde, gli equilibri sul terreno appaiono ormai significativamente cambiati e andranno a influenzare le dinamiche del Paese nel corso del 2026. Per ottenere una piena stabilizzazione nazionale, il Governo Transitorio di Damasco dovrà in ogni caso far fronte a diverse criticità di carattere securitario ed economico, che riguardano soprattutto il contenimento delle tensioni tra le diverse componenti settarie e religiose interne, nonché il concreto avvio di un processo di ricostruzione economica e sociale che permetta il rientro dei numerosi sfollati e rifugiati siriani nei loro luoghi di origine.

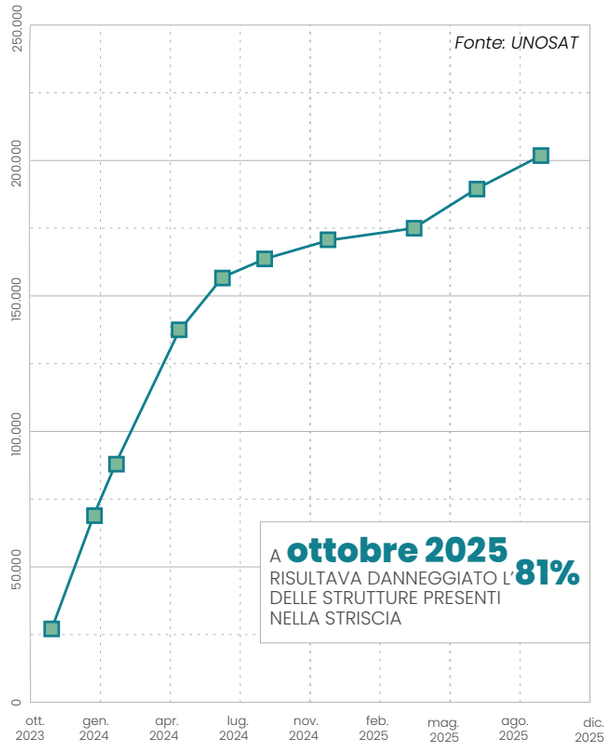
Nel corso del 2025, diversi sviluppi politici e securitari hanno riguardato la **Repubblica Islamica dell'Iran**. La tensione regionale accumulatasi in Medio Oriente è infatti sfociata, nel mese di giugno, con la "Guerra dei 12 Giorni", che ha visto Israele e USA impegnati in una campagna aerea finalizzata a limitare le capacità nucleari iraniane, considerate troppo elevate per finalità esclusivamente civili. La variabile nucleare ha determinato altresì un ulteriore irrigidimento dei rapporti tra Iran e i Paesi europei a completamento della procedura di ripristino delle sanzioni ONU contro l'Iran che erano state sospese con l'Accordo nucleare (JCPOA). Infine, negli ultimi giorni del 2025, l'Iran è stato interessato da massicce proteste interne, represse duramente da quegli apparati di sicurezza.

Questi fattori critici andranno verosimilmente a incidere sullo stato dei rapporti tra la Comunità internazionale e l'Iran anche nel corso del 2026. Le dinamiche di confronto tra Teheran e Washington hanno infatti assunto, sin dall'avvio del nuovo anno, una rinnovata centralità nell'equazione di si-

La crisi di Gaza



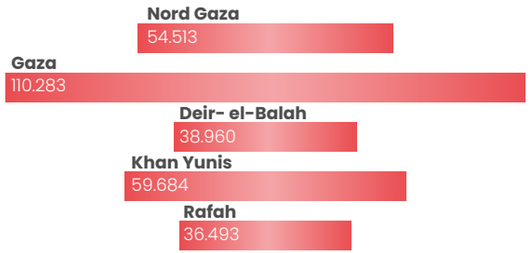
Gli edifici distrutti o danneggiati nella Striscia di Gaza



I danni nella Striscia per Governatorato

Fonte : Interim Rapid Damage and Needs Assessment 2025

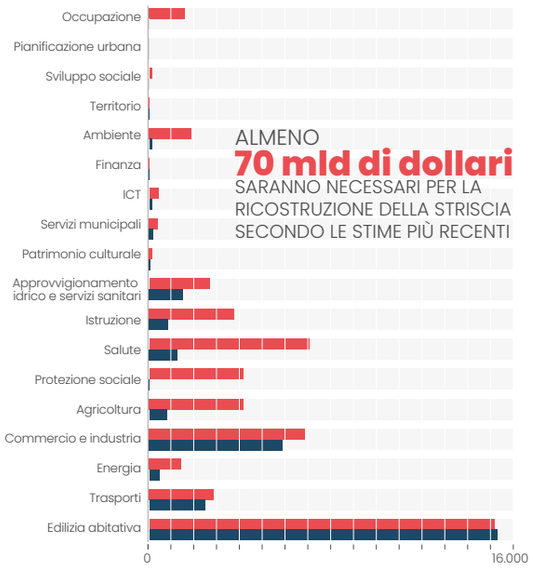
Unità abitative distrutte per Governatorato



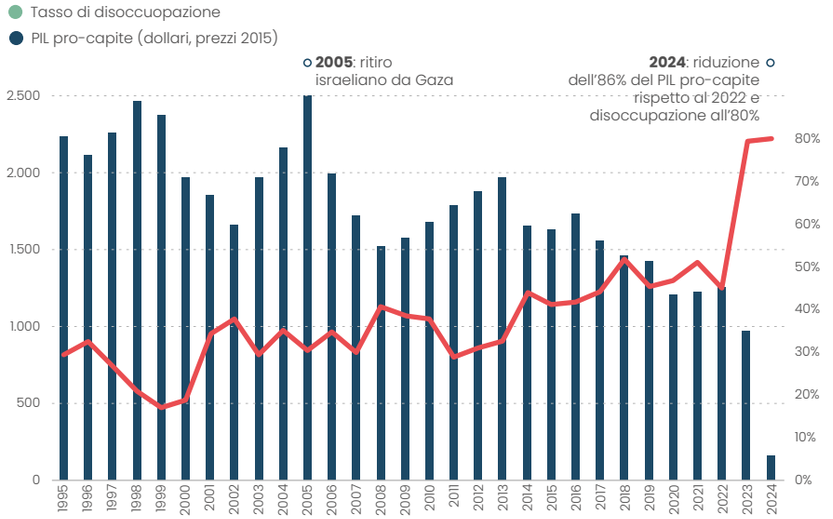
I danni e le esigenze per la ricostruzione nella Striscia di Gaza (milioni di dollari)

- Esigenze finanziarie per la ricostruzione in 10 anni
- Danni stimati ad ottobre 2024

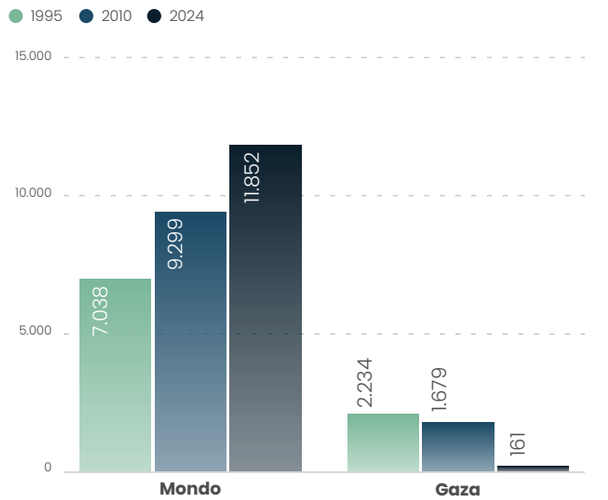
Fonte : Interim Rapid Damage and Needs Assessment 2025



PIL pro-capite e disoccupazione nella Striscia di Gaza



PIL pro-capite: confronto tra Gaza e la media mondiale (dollari, prezzi 2015)



curezza del quadrante, suscettibile di sfociare in un ampio novero di esiti possibili.

Ferma restando, infatti, l'espressa volontà degli Stati Uniti di arrivare a un'ulteriore riduzione delle capacità nucleari, missilistiche e di proiezione regionale dell'Iran, tale questione, destinata a rimanere alla prioritaria attenzione informativa dell'intelligence, è emblematica del profondo cambio di paradigma delle crisi internazionali, in un contesto segnato da una continua evoluzione dell'ordine mondiale.

Allargando lo sguardo, infine, sull'area del Golfo, la minaccia espressa dal gruppo Houthi in **Yemen** verso le tratte commerciali marittime che passano verso il Mar Rosso rimarrà verosimilmente concreta anche nel corso del 2026. L'attività della milizia yemenita è infatti oggetto di particolare focus intelligence anche per la presenza nell'area di diversi assetti italiani schierati nelle Missioni internazionali volte a garantire la sicurezza e la libertà di navigazione.

INDO-PACIFICO

Anche nel corso del **2025** l'**area dell'Indo-Pacifico** ha rivestito primario rilievo nell'attività informativa dell'intelligence. La macroregione ha visto un iniziale innalzamento della **tensione tra Cina e Stati Uniti, soprattutto sul piano commerciale**. Centrali, nelle dinamiche dipanatesi durante l'anno, sono state sia le contromisure cinesi ai dazi, in primis le restrizioni alle esportazioni di terre rare, sia la successiva rimodulazione delle misure tariffarie decisa dall'Amministrazione USA, con l'apertura di una fase più dialogante, interpretata a Pechino come un successo.

Tra le dinamiche più rilevanti su cui si è concentrata l'attenzione dell'Intelligence vi è stato l'aumento dei conflitti inter-statali, con gli **scontri tra India e Pakistan** a maggio, quelli **tra Cambogia e Thailandia** a luglio e poi di nuovo a dicembre e quelli **tra Pakistan e Afghanistan** che hanno visto la loro fase più acuta a ottobre. Le **tensioni tra Cina e Filippine** sono rimaste elevate per tutto l'anno, mentre si è visto un **miglioramento nei rapporti tra India e Cina**.

Nel 2026, i rischi maggiori per la sicurezza in Asia-Pacifico si concentreranno probabilmente nel Mar Cinese Meridionale, a fronte di un quadro teso ma relativamente stabile nello Stretto di Taiwan e dell'atteso prosieguo del dialogo d'alto livello tra Cina e Stati Uniti. È inoltre probabile che la Corea del Nord continuerà a rafforzare il proprio arsenale nucleare e missilistico, accettando eventualmente di limitarlo solo in cambio del riconoscimento dello status di potenza nucleare, in primis da parte degli Stati Uniti, e di una drastica riduzione delle sanzioni internazionali.

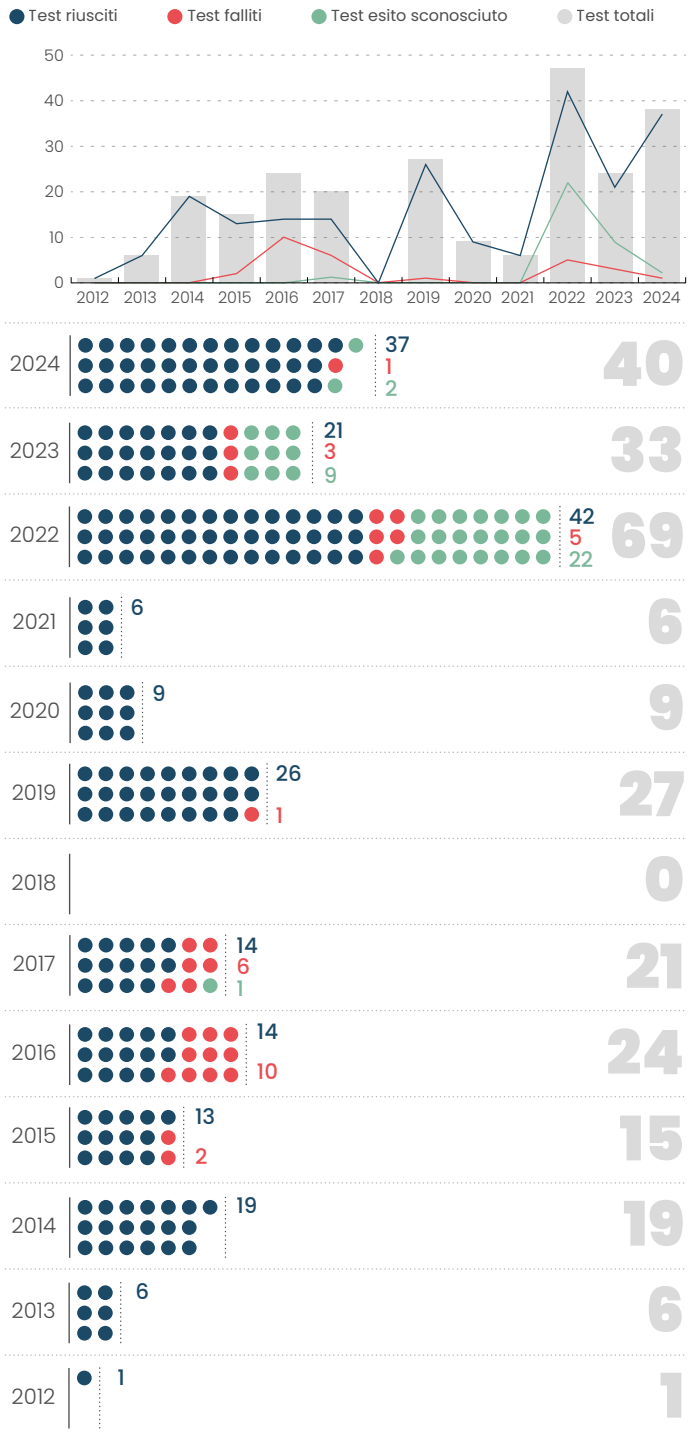
Gli incidenti avvenuti nel 2025 nel Mar Cinese Meridionale, come la collisione di agosto tra unità della Marina e della Guardia Costiera cinesi e quella di ottobre tra imbarcazioni cinesi e filippine, evidenziano il rischio di scontri che potrebbero innescare crisi più significative, nonostante non sia interesse delle parti coinvolte avviare una escalation.

A **Taiwan, una escalation militare entro il 2027 è improbabile**, ma il rischio potrebbe crescere dopo

il 2028. Pechino ha finora beneficiato della dinamica esecutivo-legislativo instauratasi a Taiwan, dove l'opposizione guidata dal Kuomintang (KMT) – il partito più dialogante con la Cina – ha la maggioranza in Parlamento. L'anno scorso l'opposizione ha promosso con successo tagli al bilancio del 6.6% (circa 6 miliardi di USD su 95), che si ripercuotono anche sulle istituzioni taiwanesi che si occupano di difesa, proiezione sulla scena diplomatica internazionale, contrasto allo spionaggio e resilienza delle infrastrutture critiche. Tutto ciò lascia ben sperare Pechino rispetto alla possibilità che, alle elezioni del 2028, KMT ottenga anche la carica di Presidente e dia avvio a una fase di maggiore dialogo con la Cina. Qualora il Partito Democratico Progressista (PDP) vincesse nuovamente le elezioni nel 2028, Pechino potrebbe invece ritenere impraticabile quella che definisce una "riunificazione pacifica" e il rischio di un utilizzo più assertivo dello strumento militare da parte cinese, per esempio per l'avvio di un blocco navale, crescerebbe.

Nel 2026, Pechino attenderà inoltre di conoscere gli esiti delle elezioni locali taiwanesi di novembre per trarne delle valutazioni in merito alle prospettive di KMT alla tornata elettorale del 2028. La Cina continuerà a promuovere una "riunificazione pacifica" facendo pressioni nei confronti del PDP e mostrandosi intransigente verso i governi stranieri che interagiscono con rappresentanti ufficiali taiwanesi o che esprimono posizioni osteggiate da Pechino su Taiwan.

TEST MISSILISTICI DELLA COREA DEL NORD



Il focus della Cina su questioni economiche, sociali e politiche interne così come la prospettiva di nuovi incontri fra Xi e Trump contribuiranno probabilmente a contenere il rischio di spinte in avanti volte a modificare e/o alterare con la forza lo status quo nel 2026. Nel 2025 si è infatti assistito a una ripresa delle interazioni d'alto livello tra Cina e Stati Uniti che hanno consentito di abbassare le tensioni, pur nella consapevolezza che la competizione strategica di fondo tra le due potenze resti immutata.
Per quanto riguarda la **Corea del Nord**, nonostante l'impoverimento economico della popolazione, essa dispone di un rilevante arsenale nucleare e missilistico, ed è l'unico Stato ad aver costruito con successo un arsenale militare nucleare dopo il 1991. Si valuta che il Regime nordcoreano non abbia alcuna intenzione di rinunciare al suo arsenale nucleare, anche se potrebbe accettare di limitarlo a seguito di colloqui con gli Stati Uniti che potrebbero avere inizio già quest'anno. La leadership nordcoreana probabilmente sente di essere in una posizione di forza, grazie alla forte partnership instaurata con la Russia, al miglioramento delle relazioni con la Cina e alla disponibilità al dialogo espressa sia da parte statunitense che da parte sudcoreana. Pyongyang ha più opzioni diplomatiche a sua disposizione di quante non ne abbia mai avute in passato ed è probabile che utilizzerà questa libertà di manovra per continuare a rafforzare il proprio arsenale nucleare e missilistico, cercando al tempo stesso di diversificare le proprie partnership per non dipendere eccessivamente da nessuno dei Paesi vicini.

ULTERIORI SCENARI D'INTERESSE

Per quanto riguarda i **Balcani**, appare comunque opportuno evidenziare che le cause profonde che, nel secolo scorso, hanno portato alla disgregazione della ex Jugoslavia in Stati autonomi non sono state pienamente superate. Persistono, infatti, **tensioni etniche** mai del tutto sopite, significative **disparità economiche tra i diversi Paesi**, **spinte autoritarie**, **fenomeni diffusi di corruzione e una criminalità organizzata in grado di influenzare la politica**. A ciò si aggiungono possibili radicalismi religiosi e le crescenti ingerenze di attori esterni quali Turchia, Russia e Cina, che contribuiscono ad alimentare frizioni latenti tra croati, serbi, bosniaci e albanesi. La regione presenta quindi numerosi fattori di instabilità, tra cui la presenza di reti criminali attive nel traffico di armi, stupefacenti ed esseri umani, nonché il rischio di infiltrazioni strategiche verso l'Europa attraverso l'acquisizione di infrastrutture chiave (porti e aeroporti) da parte di potenze extraeuropee potenzialmente ostili. La vicinanza geografica all'Italia, la consapevolezza che un'eventuale crisi improvvisa avrebbe ripercussioni immediate sulle coste nazionali e la prospettiva di futuri investimenti italiani nell'area rendono necessario un attento monitoraggio delle dinamiche regionali, specie per quel che riguarda la Bosnia-Erzegovina (che nell'ottobre 2026 af-

fronterà le elezioni per tutti i livelli di Governo), la Serbia (con l'instabilità domestica legata alle perduranti proteste antigovernative) e il processo di normalizzazione delle relazioni di quest'ultima con il Kosovo, attualmente in stallo.

In relazione all'**Artico**, i **mutamenti geopolitici in corso**, globali e d'area, dovuti ai **cambiamenti climatici** e alle **possibili aperture di nuove e più economiche rotte commerciali**, anche letti in chiave prospettica di lungo periodo, introducono la **necessità per l'Italia** – Paese mediterraneo, non-Artico, ma che proietta interessi economici e scientifici nella regione – di **sviluppare**, sin da ora, una **propria e autonoma chiave di lettura dei principali paradigmi securitari caratterizzanti l'area**. Ciò al fine di non essere schiacciato dagli interessi crescenti di USA, Russia e Cina. Un monitoraggio dell'Artico, area caratterizzata sinora da peculiarità non-legate a confronti cinetici, appare utile a sviluppare sinergie di sistema strumentali e a sostenere gli interessi nazionali e commerciali nella regione.

LA COMPETIZIONE GEOPOLITICA NEI NUOVI DOMINI

I **nuovi domini della competizione geopolitica** si svilupperanno verosimilmente sempre più anche nel c.d. **"deep blue"**, inteso sia come le profondità oceaniche che come lo spazio extra-atmosferico. Si tratta di due frontiere simboliche dell'esplorazione umana, a cui le classi dirigenti sono chiamate a garantire la sicurezza e lo sviluppo in condizioni di incertezza.

Entrambi i domini risultano cruciali per la stabilità globale. A titolo esemplificativo basti osservare come oltre il 95% dei flussi dati mondiali transiti attraverso cavi sottomarini in fibra ottica posati sui fondali: si tratta di circa 485 cavi per una lunghezza complessiva di oltre 900 mila miglia.

La comparazione tra gli attori globali della competizione geopolitica nel dominio sottomarino (Stati Uniti, Cina e Unione europea) può essere realizzata identificando gli equilibri di potere in termini di "stock netti", ossia le capacità effettivamente convertibili in vantaggi reali: controllo dei cavi sottomarini; minerali e risorse sottomarine; numero e qualità di veicoli sottomarini autonomi, della ricerca oceanografica e degli osservatori di profondità; logistica marittima; innovazione dual use.

Gli Stati Uniti conservano la più ampia e matura postura marittima e sottomarina; la Cina espande rapidamente la capacità industriale e prototipale sotto una direzione statale centralizzata; l'Unione europea dispone di capacità sofisticate, ma meno scalabili e strategicamente più limitate.

Il **potere statunitense** nel **dominio marittimo/sottomarino** si fonda su alcuni **fattori**:

- il possesso o il noleggio da parte degli hyperscaler statunitensi di circa la metà della capacità globale di cavi sottomarini e la gestione di circa il 55% di tutta la nuova domanda di capacità;
- la disponibilità di una rilevante rete di porti na-

turali in acque profonde (deepwater);

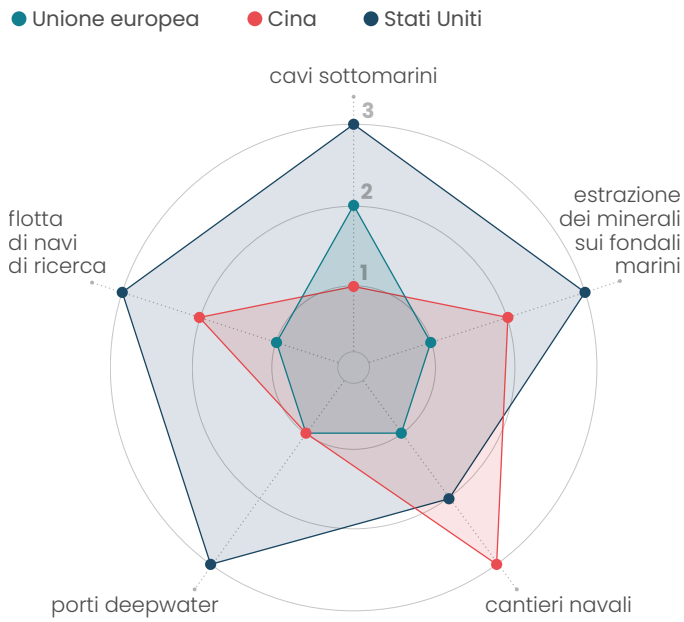
- una estesa flotta oceanografica, comprensiva di una capacità di estrazione mineraria in acque profonde.

La **Cina** presenta la **traiettoria di crescita più marcata**, fondata su cantieri navali senza equivalenti, nonché su una rete di porti deepwater e di piattaforme avanzate. Ha avviato una fase pilota di estrazione mineraria con veicoli sottomarini ad alta profondità. Tuttavia, la Cina controlla solo circa il 5-10% della capacità globale dei cavi sottomarini, prevalentemente su rotte intra-asiatiche.

L'Unione europea mantiene nicchie tecnologiche di alto valore piuttosto che una proiezione di potenza su larga scala. Gli attori europei delle telecomunicazioni controllano complessivamente circa il 10-20% della capacità globale di cavi sottomarini, e non sussiste la disponibilità di un sistema di estrazione commerciale integrato operante sui fondali marini.

Il secondo asse del "deep blue" è lo **spazio**, dominio di importanza geopolitica ampiamente dimostrata negli ultimi decenni. Anche qui la valutazione privilegia "stock netti" di potenza: sistemi dispiegabili; profondità industriale; maturità infrastrutturale e capacità di conversione sostenibile. In questo quadro gli Stati Uniti sono la potenza spaziale più matura e onnicomprensiva; la Cina presenta la massima velocità di espansione industriale accompagnata però da una conversione operativa ancora disomogenea; l'Unione europea possiede

CAPACITÀ NEL DOMINIO SOTTOMARINO



eccellenze tecnologiche, con una limitata proiezione strategica autonoma.

Gli Stati Uniti possiedono l'infrastruttura di lancio più diversificata e affidabile, abilitando complessivamente oltre 200 lanci annui. Il vantaggio statunitense è rafforzato da una elevata ridondanza, nonché da elasticità e maturità commerciale. Sul piano orbitale gli USA concentrano gli stock più ampi, dominando le comunicazioni in orbita bassa. L'ecosistema commerciale assorbe la maggior parte degli investimenti privati globali e rappresenta l'unica base industriale pienamente scalabile per lanci, costellazioni e missioni nello spazio profondo.

Nel complesso, in termini di "stock netti" di potenza spaziale convertibile operativamente:

- gli **Stati Uniti** mantengono un vantaggio strategico decisivo;
- la **Cina** presenta capacità crescenti ma ancora disomogenee, vincolate da una ridondanza limitata e da un'eccessiva dipendenza dai finanziamenti statali;
- l'**Unione europea** mantiene competenze di livello mondiale in alcuni sottosistemi del dominio spaziale, nonché di programmi istituzionali stabili, ma non ha ancora la scala industriale, la massa di lancio e la portata operativa indipendente necessarie per lo status di potenza spaziale primaria.

L'INNOVAZIONE DELLE TECNOLOGIE CIVILI E LE RICADUTE SULLE APPLICAZIONI MILITARI

Una **quota crescente di competenze, componenti e servizi** (dalla sensoristica al cloud, fino all'analisi dei dati) **nasce nel mercato civile e viene poi ricalibrata per esigenze di difesa**. Il settore militare, per elevare efficacia operativa, resilienza e prontezza decisionale, integra strumenti e know-how provenienti da imprese, università e start-up, spesso tramite partnership e sperimentazioni sul campo. Questa convergenza modifica anche i processi di procurement: più prototipazione, cicli brevi e maggiore attenzione alla sicurezza delle integrazioni. In parallelo cresce l'importanza di competenze ibride, capaci di tradurre bisogni operativi in specifiche tecniche.

Aziende private e centri accademici possono offrire al comparto difesa tecnologie già mature o facilmente adattabili, riducendo tempi e costi rispetto a programmi esclusivamente militari. L'adozione di soluzioni commerciali consente di testare più in fretta, iterare e scalare; tuttavia richiede una governance rigorosa: valutazioni di sicurezza, gestione della supply chain, requisiti di interoperabilità e protezione della proprietà intellettuale, con verifiche periodiche.

In questo scenario si colloca il **tema del dual use**: tecnologie, beni e conoscenze con impiego civile legittimo, ma potenziale utilizzo militare o ostile. IA, droni, sensori, software di data analytics, materiali avanzati e strumenti crittografici rientrano spesso in questa categoria. Il dual use impone un equilibrio: non frenare innovazione e competitività, ma introdurre responsabilità e controlli proporzionati. Ciò significa valutazioni di rischio per casi d'uso, verifiche sull'end-user, controlli sulle esportazioni quando applicabili e "security by design" nei prodotti.

Un ruolo crescente può essere svolto dall'**intelligence economica nella salvaguardia delle tecnologie civili con ricadute militari**. Attraverso analisi e prevenzione, essa può:

- mappare filiere e nodi critici;
- identificare start-up e centri di ricerca strategici;
- monitorare acquisizioni, joint venture e trasferimenti di proprietà intellettuale;
- segnalare operazioni potenzialmente ostili;
- fornire early warning su dipendenze da fornitori

esteri, rischi di spionaggio industriale e vulnerabilità di filiera, supportando controlli sugli investimenti e strategie di protezione del know-how.

Infine, la cooperazione strutturata con imprese e università aiuta a prevenire fuga di informazioni, rafforzando consapevolezza, due diligence e risposta coordinata agli incidenti.

In tale contesto, lo **sviluppo dei sistemi d'arma autonomi (autonomous weapons systems, AWS)** – droni senza pilota con capacità decisionali autonome, sistemi di difesa automatizzati, armi cibernetiche autonome – rappresenta una delle fratture etiche e legali più profonde aperte dalla tecnologia contemporanea.

L'elemento che suscita maggiori preoccupazioni in un sistema d'arma completamente autonomo è da rinvenire nella possibilità dello stesso di identificare in modo indipendente un bersaglio, valutare il contesto e aprire il fuoco senza intervento umano diretto. Al riguardo, si segnala che alcuni sistemi già operativi possiedono capacità semi-autonome. Si pensi, a titolo esemplificativo, al sistema CIWS (Close-In Weapon System), che può operare in modalità completamente automatica, identificando e neutralizzando minacce senza input umano. Entro tale cornice si pongono altresì i droni armati sofisticati dotati di capacità di targeting assistite da IA e in grado di individuare in via autonoma potenziali bersagli.

Nel senso, rileva sottolineare che l'evoluzione più recente riguarda lo sviluppo di capacità di autonomia nella fase terminale dell'ingaggio, emersa come risposta diretta alla crescente efficacia della guerra elettronica. In numerosi casi, le contromisure riescono a interrompere il collegamento radio negli ultimi metri prima dell'impatto, in particolare quando il drone scende sotto l'orizzonte radio o entra in aree con forte disturbo elettromagnetico. Per mitigare questa vulnerabilità, si stanno progressivamente integrando moduli di intelligenza artificiale a basso costo adattati all'impiego militare.

Questi componenti consentono al drone di acquisire, riconoscere e mantenere autonomamente il tracciamento visivo del bersaglio nella fase finale dell'attacco. In questa configurazione, l'operatore individua e inquadra il bersaglio da distanza di sicurezza e attiva una funzione di "aggancio visivo" (lock). Da quel momento, il sistema di bordo assume il controllo della guida terminale, elaborando in tempo reale il flusso video per correggere la traiettoria e compensare eventuali manovre evasive o variazioni dell'ambiente. Tale modalità consente di portare a termine l'ingaggio anche in caso di perdita totale del segnale di controllo, trasformando il drone First-Person View - FPV da sistema remotamente pilotato a munizione semi-autonoma. Sul piano operativo, ciò riduce sensibilmente l'efficacia delle contromisure di disturbo a corto raggio e aumenta la probabilità di successo dell'attacco nella fase più critica, ma fa sorgere importanti dubbi circa la liceità dell'impiego di tali sistemi nell'ambito del diritto internazionale.

Il **diritto internazionale umanitario**, codificato nelle Convenzioni di Ginevra e nei Protocolli aggiuntivi, considera fondamentale il **principio del "controllo umano significativo" sui sistemi d'arma**. Inoltre, sempre a livello di normativa sovranazionale, rileva la possibilità di identificare chiaramente i responsabili dei crimini di guerra o delle violazioni del diritto internazionale umanitario. Pertanto, diviene fondamentale comprendere le modalità di allocazione delle responsabilità nelle ipotesi in cui un sistema autonomo commetta un atto che costituisce un crimine di guerra (ad esempio, attaccando una struttura civile come un ospedale). La descritta opacità causale rappresenta dunque una sfida profonda per il diritto internazionale contemporaneo.

Altrettanto rimarchevole è il **principio di "distinzione" nel diritto dei conflitti armati**, ai sensi del quale le forze combattenti sono tenute a discernere chiaramente tra combattenti e civili. Al contrario, algoritmi di machine learning addestrati su dati imperfetti o affetti da pregiudizi cognitivi potrebbero sistematicamente discriminare certi gruppi di persone, oltre a riprodurre o amplificare bias presenti nei dati di addestramento.

Allo stato attuale, non esiste un trattato internazionale vincolante che regoli il fenomeno dei sistemi d'arma autonomi. L'ONU ha istituito un

TECNOLOGIE CIVILI	APPLICAZIONI CIVILI	RICADUTE SU APPLICAZIONI MILITARI
IA: analisi predittiva, classificazione e riconoscimento di pattern	Finanza, sanità, logistica	Sorveglianza, pianificazione, manutenzione predittiva, comando e controllo
IA: modelli predittivi	Cyber, elettronica	Anticipazione degli attacchi, contromisure elettroniche
IA e cyber	Cybersecurity, contrasto alla disinformazione	Monitoraggio continuativo, mitigazione dei rischi, analisi comportamentale, classificazione di minacce persistenti avanzate, utilizzo di indicatori di resilienza, esercitazioni di "red teaming"
Robotica, droni, miniaturizzazione della sensoristica	Logistica, guida autonoma, ispezioni, agricoltura di precisione	Ricognizione, supporto tattico, operazioni mirate, sciami di droni
Motori grafici, ambienti immersivi	Videogiochi, simulazioni virtuali	Addestramento, "gemelli digitali" di infrastrutture e contesti urbani, wargame, valutazione degli stress cognitivi
Satelliti in orbita terrestre bassa	Servizi spaziali commerciali	Architetture ibride di integrazione di dati civili e militari
Quantum technology	Computer quantistici	Sicurezza delle comunicazioni, crittografia

Gruppo di Esperti Governativi incaricato di studiare il fenomeno, ma i negoziati rimangono bloccati a causa dalle differenze tra Stati circa il livello di autonomia ammissibile. Alcuni Paesi sostengono che una certa autonomia è necessaria per far fronte alla velocità dei conflitti contemporanei, altri (come diverse nazioni europee e organizzazioni per i diritti umani) sostengono che deve essere mantenuto un controllo umano significativo su qualsiasi decisione letale. Questa frattura riflette una differenza di visione fondamentale tra chi considera la tecnologia un mezzo neutrale di guerra e coloro che ritengono opportuno perimetrarla entro imperativi etici e giuridici specifici.

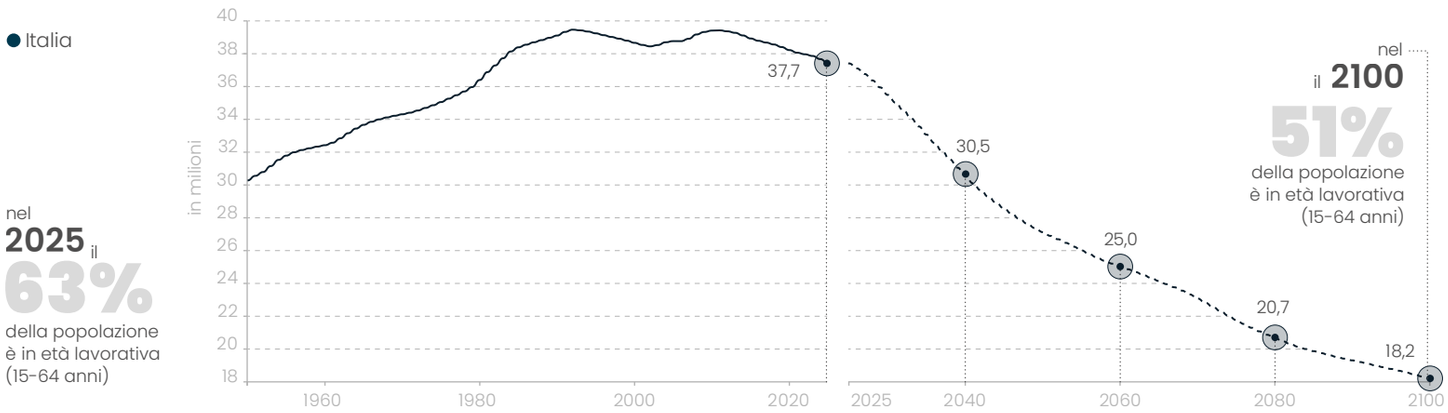
LA DASHBOARD

DEGLI INDICATORI STRATEGICI

2

DEMOGRAFIA

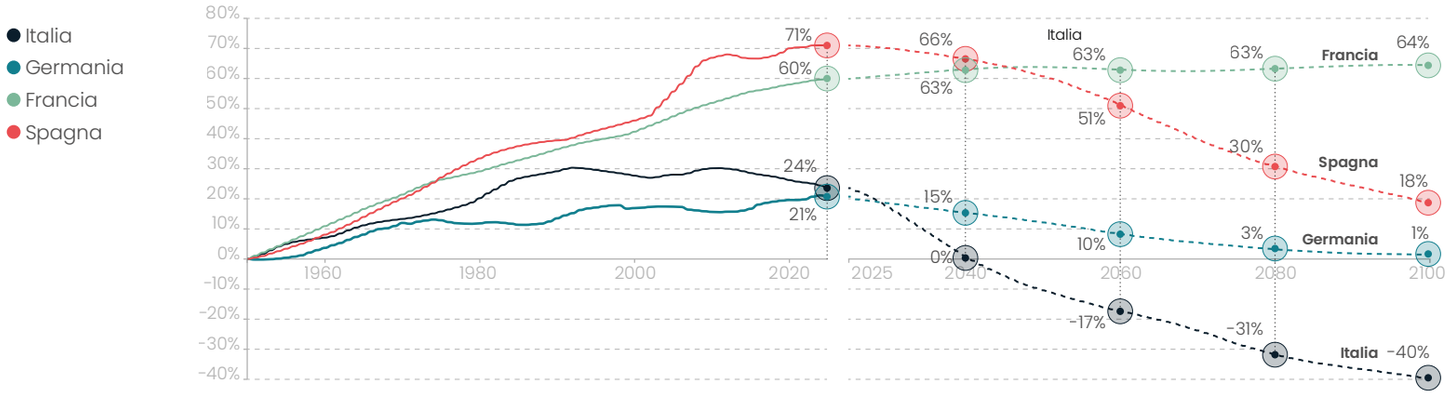
Popolazione italiana in età lavorativa



Popolazione italiana in età lavorativa

Dopo alcuni anni di lenta discesa della popolazione italiana in età lavorativa (la fascia di età compresa tra 15 e 64 anni), le proiezioni realizzate dalla Divisione Popolazione delle Nazioni Unite indicano come sia iniziata una lunga fase durante la quale la riduzione della popolazione risulterà ancor più accelerata.
Se nel 2025 la popolazione italiana in età lavorativa costituisce circa il 63% del totale, nel 2100 è previsto un calo fino al 51% (scenario medio di proiezione per quanto attiene i livelli futuri di fecondità, mortalità e migrazioni internazionali, definendo una proiezione demografica ritenuta la più probabile).

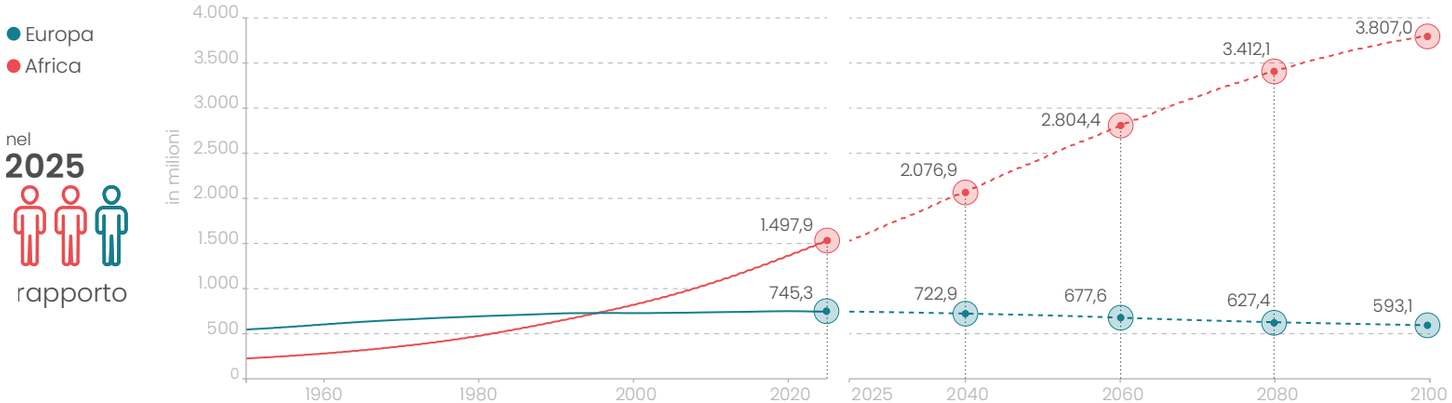
Popolazione in età lavorativa rispetto a quella del 1950



Popolazione in età lavorativa rispetto a quella del 1950

Il confronto tra le proiezioni demografiche relative alla fascia d'età lavorativa nei quattro maggiori Paesi dell'Unione Europea (Francia, Germania, Italia, Spagna) rispetto alla popolazione registrata nel secondo dopoguerra (1950) pone il caso italiano tra i più critici.
Mentre il dato previsto nel 2100 per la Germania è sostanzialmente identico a quello del 1950, e quello per la Spagna e la Francia risulta superiore, per l'Italia si prevede un calo della sua popolazione in età lavorativa nel 2100 pari al 40% rispetto a quello esistente nel 1950.

Confronto demografico tra Africa ed Europa



Confronto demografico tra Africa ed Europa

L'Europa è un continente in calo demografico, mentre quello africano è in crescita. Il dato rilevante sta nella dinamica dei due fenomeni: il calo europeo tra il 2025 e il 2100 risulta pari al 20%, mentre la crescita della popolazione africana nel medesimo periodo è prevista in oltre il 150%.
Ciò significa che nel 2025 il rapporto tra popolazione africana e popolazione europea è pari a 2:1, nel 2100 sarà di 6:1. Con le conseguenze in termini di sviluppo economico e migrazioni.

3. COMPETITIVITÀ E SICUREZZA DEL SISTEMA ECONOMICO-FINANZIARIO

L'azione intelligence dispiegata nel 2025 ha affrontato, tra l'altro, le tematiche connesse all'impatto di eventuali dazi e sanzioni sul Sistema Paese e sulla tutela delle catene di forniture di soggetti strategici nazionali. Ciò, in un contesto caratterizzato dalla possibilità, in capo ad alcuni attori internazionali, di esercitare un controllo su uno o più nodi centrali delle reti globali, di monitorare e condizionare l'accesso ai flussi che attraversano le reti stesse. In questo modo, l'interdipendenza economica può essere trasformata in leva di pressione nei confronti di attori terzi attraverso l'utilizzo di strumenti economico-commerciali e finanziari, quali restrizioni all'export e all'import, misure sanzionatorie, controlli sugli investimenti o limitazioni all'accesso a infrastrutture critiche (c.d. Economic Warfare).

La ricerca informativa ha interessato anche il mondo della cripto-finanza, ormai divenuto una componente strutturale dell'ecosistema finanziario globale. Dal momento in cui le criptovalute e, più in generale la cripto-finanza, non sono più un fenomeno marginale confinato agli ambienti tecnologici, diviene centrale per l'intelligence monitorare la combinazione tra crescita di volumi, diffusione degli strumenti e natura transfrontaliera delle transazioni.

Sul versante interno, la cripto-finanza rappresenta un moltiplicatore di complessità per le attività di prevenzione e contrasto alle attività criminali, in quanto, facendo leva sullo pseudonimato offerto dalle crip-

tovalute, combinato con tecniche di offuscamento e l'uso di piattaforme non regolamentate, rende complesso il tracciamento dei flussi. A livello internazionale, invece, permane il ricorso alle criptovalute da parte di attori statali ostili o sottoposti a sanzioni internazionali, anche come sistema dei pagamenti alternativo ai circuiti finanziari in dollari.
Il focus degli Organismi informativi non ha mancato di rivolgersi anche a possibili criticità di natura sistemica. In tale contesto, si è dovuto prendere atto, altresì, del ruolo della cripto finanza, quale forza di interconnessione tra i mercati regolamentati e quelli non regolamentati.
Per quanto attiene alla tutela della sicurezza energetica nazionale, sono state oggetto di attenzione sul piano informativo l'integrità e il corretto funzionamento delle infrastrutture (di produzione/trasformazione, trasporto e accumulo/stoccaggio), le filiere di approvvigionamento di idrocarburi e di componentistica tecnologica legata alla generazione rinnovabile, nonché il presidio delle frontiere tecnologiche, a cominciare da quella nucleare, alla luce del suo potenziale contributo nel bilanciamento delle esigenze di sicurezza e di sostenibilità ambientale del paniere elettrico nazionale.
L'attenzione informativa ha riguardato, infine, anche la valutazione delle possibili implicazioni securitarie in ambito economico legate alle macrotendenze in campo tecnologico. In particolare, nell'attuale fase geopolitica, segnata da tensioni e iniziative di riarmo, diviene evidente che la capacità di generare innovazione tecnologica, dati i profondi impatti sulle modalità di produzione, diventa essa stessa l'elemento centrale della competizione internazionale, facendo crescere l'esigenza di individuare le modalità più efficaci per proteggere da attori ostili il patrimonio conoscitivo esistente e tutte le attività finalizzate a incrementarlo.

STATO E PROSPETTIVE DELL'ECONOMIC WARFARE

A partire dagli anni Novanta del secolo scorso si è assistito a un'**intensificazione dell'integrazione economica internazionale**, nel cui contesto si è dispiegata l'azione delle imprese multinazionali che, guidate dalla ricerca di maggiore efficienza produttiva e, in ultima istanza, dalla massimizzazione del profitto, hanno progressivamente frammentato e ricollocato su scala globale le diverse fasi dei processi produttivi, determinando la **creazione di reti globali lungo le quali fluiscono energia, materie prime e semilavorati**.

Tali network sono caratterizzati da una struttura intrinsecamente asimmetrica a livello globale, articolata attorno a nodi centrali (hub) e periferici. Tale paradigma contraddistigue, al tempo stesso, il campo tecnologico, i settori dell'energia e delle materie prime critiche, le attività manifatturiere a più basso valore aggiunto, nonché l'ambito finanziario. Ed è proprio l'intrinseca asimmetria delle reti globali a rendere possibile la loro strumentalizzazione a fini coercitivi. Il controllo di uno o più nodi centrali (hub), quando questi insistono entro i confini di una specifica giurisdizione statale, consente infatti agli attori che esercitano tale controllo di monitorare e condizionare l'accesso ai flussi che attraversano le reti stesse. In questo modo, l'interdipendenza economica può essere trasformata in leva di pressione nei confronti di attori terzi attraverso l'utilizzo di strumenti economico-commerciali e finanziari, quali restrizioni all'export e all'import, misure sanzionatorie, controlli sugli investimenti o limitazioni all'accesso a infrastrutture critiche (**Economic Warfare-EW**).

In tale quadro, è rilevabile anche un'influenza sui flussi di capitale e sul costo del finanziamento. L'incertezza geopolitica e l'uso selettivo di sanzioni e controlli sugli investimenti orientano le decisioni degli investitori verso contesti percepiti come più stabili e prevedibili, generando effetti cumulativi sulla capacità di crescita dei singoli Paesi. La credibilità istituzionale e la qualità delle politiche economiche diventano quindi determinanti per mantenere l'accesso al capitale in un ambiente globale più frammentato.

Le leve dell'Economic Warfare sono peraltro evolute all'interno di un più generale clima di crescente conflittualità geopolitica, assumendo un carattere progressivamente più sistemico. Parallelamente, è emersa con maggiore chiarezza la dimensione tecnologica dell'Economic Warfare, con un utilizzo esplicito dei controlli all'export come strumento di contenimento tecnologico, progressivamente ampliato sino al livello di interi settori industriali.

Accanto a queste misure, **riemerge anche una dimensione più tradizionale della coercizione economica** con l'introduzione di dazi e quote, specie sulle importazioni in settori quali acciaio, alluminio e manifattura avanzata, dove il mantenimento di un certo livello di capacità produttive viene giudicato come strategico. In parallelo, l'**Unione europea**

rafforza progressivamente i propri meccanismi di screening degli investimenti esteri diretti, formalizzati con l'adozione di un quadro europeo nel 2019, e avvia un processo di revisione e potenziamento dei controlli alle esportazioni.

Russia e Cina, dal canto loro, pur con strumenti e capacità differenti, ricorrono ugualmente a forme selettive di coercizione economica. Mosca utilizza in modo ricorrente la leva energetica nei confronti di Paesi vicini, come dimostrano la crisi energetica che ha coinvolto la Georgia nel 2006 e le interruzioni delle forniture di gas verso l'Ucraina nel 2006, 2009 e 2014. Pechino sperimenta forme di coercizione economica mirata, spesso informali e settoriali.

> *Mosca utilizza in modo ricorrente la leva energetica nei confronti di Paesi vicini, come dimostrano la crisi energetica che ha coinvolto la Georgia nel 2006 e le interruzioni delle forniture di gas verso l'Ucraina nel 2006, 2009 e 2014*

Complessivamente, la strutturazione di reti economiche globali intrinsecamente asimmetriche ha reso sempre più possibile, negli ultimi decenni, la **trasformazione dell'interdipendenza economica** – fattore di efficienza alla base della crescita economica globale – **in strumento di coercizione**. Tale evoluzione si colloca all'interno di una dinamica più ampia che vede un rinnovato e più marcato attivismo dello Stato in economia, volto a rispondere alle fragilità emerse nelle supply chain globali nel corso di crisi sistemiche, come la pandemia da Covid-19, e a tutelare una sicurezza economica sempre più percepita come minacciata, anche in relazione alla perdita di capacità produttiva e occupazionale in settori ritenuti strategici. In questo quadro, il 2025 si configura non come un anno di innovazione strumentale o di mutamento sostanziale del fenomeno dell'Economic Warfare, bensì come una fase di marcata intensificazione e di cambiamento nello stile di utilizzo di strumenti già esistenti.

Nel corso dell'anno passato, sul **versante statunitense**, si è osservata una netta accelerazione nell'impiego della leva tariffaria come strumento di pressione negoziale generalizzata. Con il cosiddetto Liberation Day dell'aprile 2025, l'amministrazione statunitense annuncia l'introduzione di dazi orizzontali di ampia portata, concepiti non come misure settoriali mirate ma come strumento flessibile di rinegoziazione dei rapporti economici bilaterali. A queste misure si affiancano ulteriori dazi (diretti e indiretti) minacciati o promulgati nei confronti di un ampio spettro di Paesi – tra cui India, Brasile, Cina e, più recentemente, Iran – segnando un passaggio verso un utilizzo più visibile, meno selettivo e politicamente esplicito della coercizione commerciale.

La **risposta cinese** nel 2025 si concentra invece in modo più deciso su singole filiere. Il 4 aprile Pechino

introduce nuove restrizioni e controlli all'export di terre rare e materiali critici, il 4 ottobre, all'esportazione dei semiconduttori assemblati in Cina dell'azienda europea Nexperia. In entrambi i casi, l'obiettivo non è il blocco generalizzato dei flussi, bensì l'utilizzo selettivo di colli di bottiglia industriali per generare effetti sistemici a valle lungo le catene globali del valore.

> *In chiave prospettica, il quadro tendenziale per il 2026 è quello di un utilizzo ormai consolidato degli strumenti di Economic Warfare, calibrato in funzione dei vincoli strutturali propri di ciascun attore*

In questo quadro anche l'Intelligence ha garantito il suo apporto info-valutativo nel simulare il possibile impatto dei dazi sull'economia nazionale. Ciò, tenuto conto degli effetti destabilizzanti che le tariffe doganali comunque comportano tanto sulla crescita economica globale e sulle dinamiche commerciali mondiali, quanto sui fondamentali macroeconomici e sulla resilienza delle catene globali del valore.

Al contempo, benché Stati Uniti e Cina restino gli attori centrali nel campo dell'EW, va anche rilevato che l'escalation osservata coinvolge pure gli altri player internazionali. Nel caso dell'**Unione europea**, si è assistito a una **progressiva interiorizzazione della logica dell'Economic Warfare come rischio strutturale** che ha, tra l'altro, portato alla promulgazione di politiche di derisking, come RESourceEU Action Plan dello scorso dicembre, orientate al consolidamento all'interno dell'Europa di determinate lavorazioni e capacità produttive considerate strategiche.

Diversa è la **posizione della Federazione Russa**, che nel 2025 continua a rappresentare il principale caso di applicazione prolungata di strumenti di guerra economica. Il perdurare delle sanzioni ha incentivato Mosca a una riconfigurazione dei flussi commerciali ed energetici, a un maggiore ricorso a intermediari e Paesi terzi e allo sviluppo di strategie di parziale dedollarizzazione e di aggiramento dei regimi restrittivi. In tal senso, l'esperienza russa evidenzia come un utilizzo estremo e prolungato dell'Economic Warfare spinga l'attore colpito a costruire architetture commerciali e finanziarie alternative che, pur risultando meno efficienti rispetto a quelle originarie, consentono un certo grado di resilienza e contribuiscono alla progressiva trasformazione dell'ordine economico internazionale istituzionalizzato nel secondo dopoguerra.

In chiave prospettica, il quadro tendenziale per il 2026 è quello di un utilizzo ormai consolidato degli strumenti di Economic Warfare, calibrato in funzione dei vincoli strutturali propri di ciascun attore. Nel caso cinese, la dipendenza dai mercati esteri e la necessità di preservare condizioni di apertura commerciale suggeriscono la prosecuzione di un approccio prevalentemente difensivo e calibrato,

volto a massimizzare l'effetto dissuasivo della propria capacità di incidere tramite i controlli su minerali e terre rare senza compromettere la stabilità sistemica. Sul versante statunitense, al contrario, l'elevata variabilità della politica economica e commerciale rende plausibile uno scenario caratterizzato da forti oscillazioni nell'intensità e direzionalità dell'utilizzo di tali strumenti. L'Unione europea, infine, appare indirizzata a confermare una postura essenzialmente reattiva, orientata alla gestione della vulnerabilità e alla riduzione dei rischi piuttosto che all'esercizio diretto della coercizione.
Questo trend strutturale resta tuttavia esposto al rischio di accelerazioni improvvise, qualora lo scoppio di nuovi conflitti o l'ampliamento di quelli esistenti spingesse gli attori coinvolti verso un ricorso più esteso e meno selettivo alla leva economica come strumento di pressione strategica.
In questo quadro, la posizione di un Paese come l'Italia, fortemente integrato nelle catene globali del valore e caratterizzato da una specializzazione manifatturiera avanzata ma dipendente da input esterni critici, risulta particolarmente esposta alle dinamiche dell'Economic Warfare. Più che nella capacità di esercitare direttamente leve coercitive, la sfida principale risiede nella gestione delle proprie vulnerabilità strutturali, nella comprensione del ruolo occupato dai nodi produttivi nazionali all'interno delle reti globali e nella capacità di anticipare come l'utilizzo politico dei flussi economici possa incidere sulla continuità operativa delle filiere strategiche. In tal senso, la **tutela della sicurezza economica** si configura sempre meno come obiettivo settoriale e **sempre più come dimensione trasversale della politica industriale, commerciale e di sicurezza nazionale**, in un contesto internazionale segnato da una competizione geopolitica strutturalmente più conflittuale.

ATTIVITÀ RELATIVE ALLA NORMATIVA GOLDEN POWER

2025

- 903 notifiche
- 178 pre-notifiche
- 583 notifiche pervenute nell'ambito del meccanismo di scambio comunitario ai sensi del Regolamento(UE) 2019/452

2024

- 660 notifiche
- 175 pre-notifiche
- 411 notifiche pervenute nell'ambito del meccanismo di scambio comunitario ai sensi del Regolamento(UE) 2019/452

CRIPTOVALUTE: PROFILI DI RISCHIO, SICUREZZA DEGLI INVESTIMENTI E MERCATI NON REGOLAMENTATI

Il mondo della **cripto-finanza** si è trasformato da fenomeno di nicchia a **componente strutturale**, seppur ancora minoritaria, **dell'ecosistema finan-**

ziario globale. Ciò è confermato anche dalla capitalizzazione delle criptovalute che oscilla, nel 2025, intorno ai 3,5 mila miliardi di dollari. A titolo di confronto, si stima che la ricchezza globale si attesti intorno ai 600 mila miliardi di dollari e che le criptovalute ne rappresentino circa lo 0,6%, ma con dinamiche di crescita e di rischio non proporzionate alle dimensioni ancora relativamente contenute.

Sul piano securitario, l'elemento principale all'attenzione degli Organismi informativi è la diffusione di questo strumento sui mercati. Gli utilizzatori globali di criptovalute hanno superato i 650 milioni, mentre l'offerta di prodotti e servizi nel sistema finanziario tradizionale connessi al mondo delle criptovalute continua a crescere, con particolare riferimento a sistemi di conversione, strumenti derivati ed Exchange Traded Fund (ETF). In altri termini, le criptovalute e, più in generale la cripto-finanza, non sono più un fenomeno marginale confinato agli ambienti tecnologici e, pertanto, il monitoraggio dell'Intelligence deve tenere in considerazione come la combinazione tra crescita di volumi, diffusione degli strumenti e natura transfrontaliera delle transazioni porti il mondo della cripto-finanza a presentare aree di criticità, che finiscono per interessare, inevitabilmente, anche i circuiti della finanza tradizionale.

Sul versante interno, la **cripto-finanza** rappresenta un **moltiplicatore di complessità per le attività di prevenzione e contrasto alle attività criminali**. Queste ultime fanno leva sullo pseudonimato offerto dalle criptovalute che, combinato con tecniche di offuscamento e l'uso di piattaforme non regolamentate, rende complesso il tracciamento dei flussi. Non solo le criptovalute, ma più in generale i cripto-asset, sono ormai integrati in schemi di pagamento e riciclaggio, spesso in abbinamento con social media, dark web e circuiti di underground-banking. A ciò si aggiunge la **nascita di specifiche categorie di criptovalute a forte vocazione anonimizzante (c.d. privacy coins)** che, pur rappresentando una quota minoritaria del mercato, sono particolarmente attrattive per operatori che intendono sottrarsi a ogni forma di tracciamento.

A livello internazionale, si registra, inoltre, il **crescente ricorso alle criptovalute da parte di attori statali ostili o sottoposti a sanzioni internazionali**. In particolare, tali entità usano sistematicamente i citati asset finanziari, adottando altresì modus operandi ormai consolidati e incentrati su furti informatici su larga scala, nonché su successive conversioni in valuta tradizionale. Di fatto, questi attori stanno usando le criptovalute come sistema dei pagamenti alternativo ai circuiti finanziari in dollari.

In chiave prospettica, l'utilizzo delle criptovalute da parte della criminalità organizzata e degli attori statali ostili tenderà a spostarsi sempre più verso transazioni esterne ai canali regolamentati. Pertanto, nonostante il graduale rafforzarsi dei presidi presso gli intermediari del mondo cripto, le controparti illecite tenderanno a privilegiare operatori informali, piattaforme decentralizzate e scambi peer-to-peer.

L'attenzione degli Organismi informativi non manca di rivolgersi anche a possibili criticità di natura sistemica. Gli **strumenti cripto**, infatti, pur rappresentando ancora una quota minoritaria degli asset finanziari globali, stanno raggiungendo dimensioni tali da poter **generare effetti di ricchezza, liquidità e fiducia**, soprattutto in presenza di forti rialzi o crolli improvvisi dei prezzi. Per questo motivo risulta cruciale monitorare i canali di trasmissione tra il mondo cripto e l'infrastruttura finanziaria tradizionale al fine di prevenire eventuali fenomeni di destabilizzazione suscettibili di profilare effetti domino a livello internazionale.

> *La cripto-finanza rappresenta un moltiplicatore di complessità per le attività di prevenzione e contrasto alle attività criminali*

In tale contesto, l'Intelligence ha dovuto prendere atto del **ruolo della cripto-finanza, quale forza di interconnessione tra i mercati regolamentati e quelli non regolamentati**. Questi due mondi sono ormai in contatto senza un confine netto, creando così un ecosistema unico nel quale capitali e informazioni circolano con estrema rapidità da un comparto all'altro. Conseguentemente, eventuali fenomeni di instabilità che si manifestino tanto nella finanza regolamentata quanto in quella non regolamentata possono tradursi in minacce per l'operatività delle infrastrutture finanziarie strategiche e per gli assetti di finanza pubblica.

L'attenzione degli Organismi informativi, sul **versante della finanza regolamentata**, è stata focalizzata sulle minacce endogene, che nascono all'interno del settore, e su quelle esogene, che derivano da soggetti esterni interessati a inserirsi in segmenti strategici del mercato nazionale. In particolare, il monitoraggio è stato volto verso quelle dinamiche di cambiamento e trasformazione degli assetti del settore finanziario suscettibili di profilare eventuali fenomeni di instabilità. Invece, nel **campo della finanza non regolamentata**, l'attenzione informativa ha riguardato, tra l'altro, il crescente interesse, da parte di attività criminali e attori statali ostili, a sfruttare sofisticati meccanismi per confondere le tracce e sfruttare i punti di minore controllo del sistema finanziario.

In chiave prospettica, le minacce continueranno a manifestarsi lungo la linea di frattura tra fattori interni ed esterni agli operatori. Oggi, l'interconnessione tra banche, assicurazioni, fondi e mercati impone di monitorare con attenzione le dinamiche suscettibili di minare la fiducia di investitori e cittadini, innescando reazioni che mettono sotto pressione la stabilità del sistema finanziario. Parallelamente, le iniziative di gruppi stranieri o di Paesi esteri guidati da logiche extra-economiche permarranno un ulteriore fronte di attenzione. L'ingresso, in posizioni nevralgiche delle infrastrutture finanziarie, di soggetti legati a Stati con interessi

non allineati potrebbe, in alcuni scenari, tradursi in forme di dipendenza strategica, sottrazione di know-how critico, esfiltrazione di dati o pratiche selettive del credito per favorire imprese/settori collegati a specifici gruppi o Paesi.

Per quanto concerne le attività criminali e gli attori statali ostili, gli schemi di occultamento delle identità e della provenienza dei fondi faranno leva su tecniche sempre più avanzate. La riduzione del margine operativo per le attività illecite all'interno del perimetro vigilato spingerà gruppi criminali e soggetti ostili a utilizzare in modo ancora più intensivo i segmenti non regolamentati, puntando su velocità di esecuzione, complessità tecnica e frammentazione dei flussi. Non si può escludere che questi attori faranno ricorso agli strumenti forniti dalle più avanzate frontiere tecnologiche dell'intelligenza artificiale e della criptofinanza, anche in combinazione, rendendo sempre più complesso tracciare i flussi.

L'EVOLUZIONE DELLE MINACCE ALLE INFRASTRUTTURE CRITICHE

Le **infrastrutture critiche** rappresentano uno dei pilastri su cui si reggono i sistemi socio-economici contemporanei. Le reti energetiche e quelle di trasporto, il settore finanziario, i servizi idrici e sanitari, nonché le infrastrutture digitali costituiscono solo alcuni esempi dei molteplici assetti che concorrono nel plasmare un'architettura sempre più complessa e interconnessa. Consapevole della rilevanza che assumono tali infrastrutture in termini di tutela della sicurezza nazionale, l'Italia ha provveduto a rafforzare il proprio impianto normativo sulla materia recependo:

- la **direttiva(UE) 2022/2555 (NIS 2)**, con il **decreto legislativo 4 settembre 2024, n. 138**, che ha previsto specifiche misure volte a garantire un elevato livello di sicurezza informatica;
- la **direttiva(UE) 2022/2557 (CER)**, con il **decreto legislativo 4 settembre 2024, n. 134**, che ha ridefinito l'approccio alla sicurezza e alla resilienza dei soggetti critici.

Tanto premesso in termini generali, occorre focalizzare l'angolo visuale sulle **infrastrutture energetiche**, in quanto impianti industriali costosi, sofisticati e vitali per gli altri processi produttivi, nonché obiettivi di pregio in ogni teatro di conflitto. La loro rilevanza non deriva solo dal valore economico degli asset, ma anche dalla funzione sistemica che svolgono. Questo dato, già evidente nei contesti di guerra "convenzionale", è stato dimostrato con particolare efficacia nel conflitto russo-ucraino, dove reti elettriche, gasdotti e impianti di raffinazione sono oggetto di sistematici attacchi cinetici e atti di sabotaggio. In prospettiva italiana, l'esposizione non è solo quella dei singoli impianti, ma dell'architettura complessiva del sistema. Ci si riferisce, nel senso:

- alla rete elettrica, con nodi di trasmissione e trasformazione ad alta criticità;

- alla catena del gas, basata su importazioni, stoccaggi e terminali costieri;
- alla filiera petrolifera, in cui raffinerie e terminali marittimi rappresentano punti nevralgici per l'approvvigionamento di prodotti finiti e intermedi.

In questi sistemi, colpire un anello selezionato può generare effetti a cascata molto superiori al danno locale, con impatti immediati su mobilità, telecomunicazioni, riscaldamento, produzione industriale e, più in generale, continuità dei servizi essenziali.

In tale quadro, l'**evoluzione tecnologica** corrente sta **ridefinendo** profondamente i **profili della minaccia alle infrastrutture critiche energetiche**. A fronte di una accresciuta centralità della disponibilità costante dell'energia – in particolare del vettore elettrico – per assicurare le funzioni essenziali alla società, si è assistito a un crescente focus sull'interruzione del servizio, anche a prescindere dalla distruzione fisica degli impianti. In un **sistema** come quello **italiano**, dove l'**elettricità sostiene tanto l'economia digitale quanto la crescente elettrificazione degli usi finali**, la perdita di continuità (anche breve ma estesa) può risultare strategicamente "sufficiente" per ottenere un effetto politico, psicologico o economico. Attacchi cyber o ibridi, condotti anche sfruttando le finestre di opportunità create dagli eventi meteorologici estremi, possono potenzialmente compromettere la stabilità degli approvvigionamenti energetici con il ricorso a risorse limitate e rendendo complessa ogni forma di attribuzione. Nello specifico, la **combinazione tra stress fisico** (manomissioni, incendi, allagamenti, ondate di calore) e **manipolazione digitale** (interferenze sui sistemi di supervisione, degradazione delle comunicazioni, indisponibilità selettiva di funzionalità) **consente di amplificare l'effetto dell'evento e di ostacolare la risposta**. In altri termini, ritardare il ripristino o aumentare l'incertezza operativa potrebbe essere efficace quanto la distruzione. Lo stesso vale per la filiera del gas, ove l'impossibilità di gestire correttamente pressioni, flussi, capacità di bilanciamento e disponibilità degli stoccaggi potrebbe tradursi in limitazioni "a valle" (industria energivora, termoelettrico, riscaldamento), anche senza alcun danneggiamento strutturale delle condotte o delle centrali.

> *"Attacchi cyber o ibridi, condotti anche sfruttando le finestre di opportunità create dagli eventi meteorologici estremi, possono potenzialmente compromettere la stabilità degli approvvigionamenti energetici*

La pervasività di questo scenario è legata alla diffusione delle reti autonome e alla convergenza di sistemi informatici (IT) e sistemi che controllano macchine e processi fisici (OT), un tempo separati

e ora sempre più interconnessi. Attualmente, la **digitalizzazione e pratiche operative** (come l'accesso remoto per la manutenzione) hanno **esteso enormemente la superficie d'attacco**, includendo fornitori, subappaltatori, catene di aggiornamento software e dispositivi di campo. Nel caso italiano, tale fenomeno riguarda tanto la trasmissione e distribuzione elettrica (stazioni, cabine, automazioni di rete, apparati di protezione e controllo), quanto le infrastrutture gas (telecontrollo, valvole e stazioni di compressione) e gli impianti oil & downstream

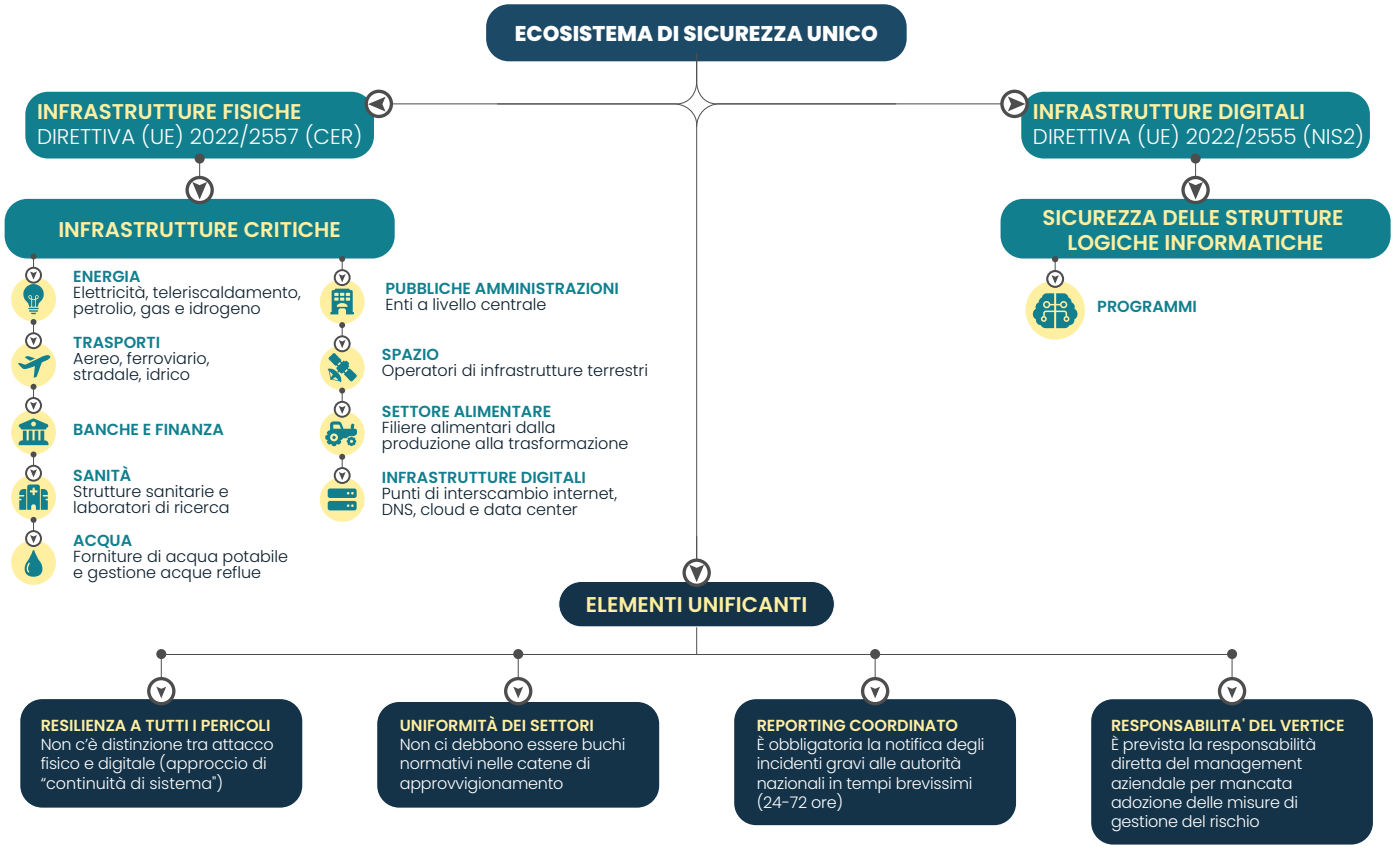
> *L'evoluzione del sistema energetico nel senso della complessità e della frammentazione di produzione e consumo (non solo elettrici) è destinata a introdurre un ulteriore profilo di minaccia*

(raffinerie, depositi, terminali marittimi), dove i processi industriali sono orchestrati da sistemi OT complessi e spesso eterogenei per età e standard. In prospettiva, soprattutto per quanto attiene all'elettricità, l'intero sistema sarà sempre più definito e gestito da software (basti pensare all'integrazione di capacità di generazione diffusa e non programmabile nella rete, all'accumulo distribuito, alla gestione attiva della domanda) e il crescente ricorso a comunicazioni macchina-macchina, indispensabile per gestire la complessità dei sistemi, diventerà al contempo moltiplicatore di rischio. Ciò posto, il punto critico emerge non solo dalla possibilità di "spegnere" un impianto, ma altresì da quella di introdurre condizioni operative ambigue: falsare misure, ritardare segnali, alterare set-point o saturare canali di comunicazione, infatti, può indurre decisioni sbagliate, attivare protezioni, generare congestioni o instabilità. Inoltre, l'interdipendenza tra infrastrutture energetiche e reti di telecomunicazioni è particolarmente sensibile in un contesto nazionale caratterizzato da dorsali di comunicazione, data center, sistemi di sincronizzazione e servizi digitali, che sono indispensabili per far funzionare il sistema elettrico e, allo stesso tempo, ne dipendono. Ne derivano crescenti rischi "incrociati", in cui un incidente o un attacco in un dominio (es. telecomunicazioni, cloud, forniture software, satellitare o radio, ecc.) si riverbera sulla capacità di controllo, supervisione e ripristino della rete elettrica e delle attività che ne dipendono.

L'**evoluzione del sistema energetico** nel senso della complessità e della frammentazione di produzione e consumo (non solo elettrici) è destinata a **introdurre un ulteriore profilo di minaccia**, legato all'**esplosione del numero di punti ingresso potenziale al sistema, che allargano la superficie di attacco fisica e logica dei sistemi energetici**. In tale cornice, l'Italia vede crescere la numerosità di attori, asset e interfacce: impianti distribuiti, prosumer, piattaforme di aggregazione, dispositivi intelligenti, componenti connessi e servizi digitali

che intermediano la gestione dell'energia. Analogamente, nella catena del gas e dei combustibili, l'integrazione di terminali di gas naturale liquefatto (GNL), stoccaggi e logistica portuale introduce ulteriori interfacce tra mondo industriale, sistemi informativi e operatori terzi, aumentando la probabilità di vulnerabilità "perimetrali" o di supply chain. Tutto ciò apre la strada al **targeting al margine**, ossia alla possibilità di compromettere la continuità dell'accesso all'energia colpendo componenti secondarie ma altamente interconnesse del sistema, come una stazione di compressione, un nodo di misura, una piattaforma di prenotazione capacità, un apparato di telecontrollo, un servizio di connettività per siti periferici o una procedura operativa "normalmente" considerata ancillare. In questo scenario, minacce particolarmente insidiose sono quelle legate all'effetto-sciame (molteplici e piccoli punti compromessi che, coordinati, producono instabilità o perdita di controllo) e agli attacchi alla fiducia nei dati (alterazione dei segnali di controllo, delle misure e delle metriche

DALLA DIFESA ALLA RESILIENZA



previsionali) che stanno alla base del funzionamento dei sistemi automatici. L'effetto può estendersi oltre il singolo vettore, in quanto la riduzione della disponibilità di gas può comprimere la generazione termoelettrica e aggravare la tenuta della rete elettrica, mentre un'interruzione elettrica prolungata può limitare la capacità di movimentazione e pompaggio in oleodotti, raffinerie e terminali marittimi ovvero ridurre l'operatività di sistemi critici per la sicurezza e la gestione emergenziale. In definitiva, la minaccia tende a spostarsi dalla distruzione "visibile" dell'asset alla compromissione "invisibile" della sua affidabilità, con un obiettivo strategico che non è solo quello di sottrarre energia, ma anche di rendere la stessa meno governabile, meno prevedibile e più costosa da garantire.

> *Si sta assistendo a una significativa evoluzione tecnologica nell'offerta di energia, con eolico e fotovoltaico che si sono affiancati in modo ormai strutturale alle fonti fossili nei panieri energetici mondiali*

IMPATTO DELLA TECNOLOGIA SULLA GENERAZIONE ENERGETICA

L'**innovazione tecnologica** emersa nell'ultimo decennio ha **cambiato** profondamente le **traiettorie evolutive della domanda energetica**, con una tendenza a una crescente elettrificazione dei consumi finali nei servizi, nelle abitazioni e nei trasporti. A ciò si aggiunge la crescita di domanda elettrica per i servizi di telecomunicazione e informatici, che, grazie alla costruzione massiva di data center e centri di calcolo, anche legati all'IA, appare destinata a conoscere una crescita consistente nei prossimi decenni.
In modo speculare, si sta assistendo a una significativa **evoluzione tecnologica nell'offerta di energia**, con eolico e fotovoltaico che si sono affiancati in modo ormai strutturale alle fonti fossili nei panieri energetici mondiali. Sulla spinta dell'incremento di capacità produttiva, soprattutto in Cina, di impianti di generazione rinnovabile e grazie ai consistenti sussidi iniziali erogati in tutte le economie avanzate, queste fonti sono ormai giunte a essere pienamente competitive nel costo dell'energia prodotta. Quando arrivano a dominare il paniere elettrico, tuttavia, le rinnovabili non programmabili comportano anche significativi rischi per la stabilità della rete e necessitano di essere accompagnate da investimenti in tecnologie complementari nella generazione, nell'accumulo e nella gestione delle reti.
Tra le soluzioni di rilievo per la sicurezza delle reti

elettriche ad alta penetrazione di rinnovabili, il **nucleare** ha il **potenziale per giocare un ruolo di primo piano nei servizi necessari a mantenere stabili le reti** (inerzia, regolazione, riserva) **e nella diversificazione del paniere elettrico**, senza compromettere la decarbonizzazione. In particolare, nonostante le incertezze su costi e tempistiche di installazione, gli **small modular reactor** e, in prospettiva, gli **advanced modular reactor di quarta generazione** possono rappresentare una soluzione tecnologica adeguata a inserirsi in modo armonico nei panieri elettrici delle economie industrializzate.

Questi impianti, grazie alla loro natura modulare, consentono la realizzazione sia di piccole centrali che possono essere installate direttamente nei siti industriali, sia di impianti relativamente grandi, composti da moduli aggregati, a servizio delle reti, a cui offrono flessibilità e un migliore dimensionamento della capacità produttiva rispetto al fabbisogno. Producendo in modo costante e a basso costo marginale, infatti, i reattori possono essere utilizzati per fornire potenza alla rete nei momenti di minore produzione da rinnovabili, sostituendo in parte la necessità di installare capacità di accumulo. Specularmente, nei momenti di eccesso di offerta da rinnovabili, i reattori possono dinamicamente deviare la potenza destinata alle reti e usarla per alimentare processi industriali a zero emissioni, come la produzione di idrogeno attraverso l'elettrolisi, consentendone l'utilizzo su vasta scala per attività produttive (siderurgia, chimica e altri processi ad alta temperatura). Inoltre, i reattori possono essere impiegati anche per la cogenerazione di calore per i processi industriali termici o per il teleriscaldamento, aumentando l'efficienza complessiva dei processi.

La **maturazione delle tecnologie relative ai reattori di piccola taglia** è particolarmente significativa non solo per la diversificazione delle fonti impiegate nei panieri energetici decarbonizzati, ma anche per ridurre la dipendenza strutturale derivante dalla posizione dominante dei sistemi industriali asiatici nelle filiere di generazione da fotovoltaico e di produzione di batterie, incluse le relative filiere di lavorazione delle materie prime necessarie. Nei fatti, la filiera tecnologica nucleare, sebbene attraversata da significative interdipendenze globali, è ancora sostanzialmente nel perimetro della capacità industriale europea e occidentale. Inoltre, la produzione delle materie prime necessarie ad alimentare le centrali è ubicata anche in aree geografiche fuori dall'influenza dei principali attori economici asiatici.

GLI IMPATTI SUL SISTEMA PRODUTTIVO ITALIANO

L'**evoluzione tecnologica** sta determinando una **trasformazione profonda dei sistemi produttivi** e, al tempo stesso, degli **equilibri sul piano della sicurezza nazionale**. In particolare, la fase geopolitica attuale, segnata da un incremento delle

tensioni geopolitiche e da iniziative di riarmo, ha reso evidente nei Paesi UE che la capacità di generare tecnologia ha impatti più profondi rispetto alle attività di protezione della stessa, in quanto, in un mondo interconnesso, il know-how è una conoscenza che nel tempo si diffonde inevitabilmente. Oggi più che mai, **avere sistemi economici in grado di generare innovazione diventa un punto cruciale per le capacità militari degli Stati**, anche in considerazione della imponente osmosi tra innovazioni civili e applicazioni strategiche.

Si fa riferimento, in particolare, alle innovazioni nei segmenti della robotica, digitalizzazione, energia e intelligenza artificiale. I significativi progressi conseguiti in questi campi negli ultimi anni sono il risultato di investimenti e capacità di assumere rischi da parte di operatori, principalmente, privati che hanno beneficiato di esternalità, sinergie cumulative e know-how sviluppati anche in altri settori. In particolare, uno dei fattori maggiormente rilevanti di tale evoluzione può essere individuato nella presenza di ecosistemi del capitale di rischio sviluppati, in grado di assicurare al venture capital, al private equity e ai mercati finanziari di operare come meccanismi di selezione e accelerazione, convogliando al contempo le risorse verso realtà promettenti, nonché sostenendo la crescita di imprese innovative e favorendo il trasferimento delle competenze. Al contrario, ove questi canali siano deboli, la trasformazione tecnologica tende a procedere con maggiore lentezza e con una distribuzione più diseguale, lasciando così ampie porzioni del tessuto produttivo su modelli a minore produttività e minore capacità di competere.

Alla luce di tali dinamiche, i Paesi UE stanno affrontando tensioni strutturali tra obiettivi regolatori, assetti di finanza pubblica e capacità di attrazione dei capitali. Questi ultimi si sono progressivamente spostati verso contesti percepiti come più favorevoli, anche spinti dalla combinazione tra burocrazia, complessità normativa e pressione fiscale che ha caratterizzato i tessuti industriali e finanziari in Europa. Ciò ha prodotto un progressivo orientamento dei flussi di capitale e delle iniziative imprenditoriali verso aree considerate più rischiose sul piano geopolitico. Tale effetto, oltre a essere cumulativo, rende complessa l'inversione della tendenza, in quanto l'afflusso di capitali in specifiche zone geografiche del mondo crea un ecosistema che, a sua volta, attrae ulteriori risorse, alimentando un circolo "virtuoso". Pertanto, per poter recuperare terreno occorrono non soltanto

> *"La capacità di generare tecnologia ha impatti più profondi rispetto alle attività di protezione della stessa, in quanto, in un mondo interconnesso, il know-how è una conoscenza che nel tempo si diffonde inevitabilmente*

mirati investimenti, ma anche un contesto generale abilitante. **La competitività tecnologica** può infatti **svilupparsi solo grazie all'apporto generato da un ambiente idoneo a ridurre gli ostacoli all'iniziativa privata, anche sostenuto tramite specifici programmi pubblici**.

In tale ottica, a livello nazionale, emerge anche la sfida di creare condizioni abilitanti per l'impiego del risparmio verso attività di investimento a beneficio del tessuto produttivo, incrementando così la disponibilità del capitale domestico ed estero per sostenere innovazione, crescita e rafforzamento delle catene del valore.

Gli aspetti descritti diventano per l'Italia di estrema importanza in considerazione della struttura del suo tessuto industriale, caratterizzato da una prevalenza di piccole e medie imprese-PMI. Tale composizione, seppure vanti flessibilità e alta specializzazione, presenta vulnerabilità nella transizione tecnologica. Le PMI possono infatti dover fare fronte a difficoltà, tra l'altro, nel reperire risorse finanziarie, nel reclutare competenze e talenti, nonché nel sostenere gli investimenti in cyber sicurezza. Ne deriva, quindi, che il rischio tecnologico può diventare un rischio competitivo, con effetti sulla posizione delle imprese nelle catene del valore internazionali.

In questo quadro, il **ruolo della politica industriale** diventa **centrale** in qualità di architettura che ne abilita l'attivazione, contribuendo a **rendere più attrattivo il Paese per investitori e imprese ad alta intensità di conoscenza**. Attrarre capitali, inclusi quelli esteri, assume un ruolo ambivalente ma strategico. Da un lato, il capitale estero può portare risorse finanziarie, accesso a mercati, tecnologie e pratiche manageriali che accelerano la modernizzazione. Dall'altro, può comportare rischi di iniziative con logiche extra-economiche che comportano delocalizzazioni, spostamento dei centri decisionali e perdite nella funzionalità di asset critici, soprattutto in settori strategici. L'obiettivo, dunque, non è quello di ridurre l'apertura, ma di qualificarla, orientandola verso iniziative che rafforzino la base industriale nazionale, aumentino la capacità di innovare e consolidino filiere resilienti.

Al contempo, **sul piano securitario**, emergono importanti **sfide di gestione della trasformazione tecnologica**, con particolare riferimento a resilienza dei sistemi produttivi e al mercato del lavoro. In particolare, la tecnologia aumenta la complessità delle catene del valore e ciò necessita di un presidio della resilienza del sistema produttivo e dell'affidabilità dei partner. Inevitabilmente, questa tipologia di impatti non si esaurisce nella fabbrica, ma interessa anche il lavoro umano dove la transizione modificherà sempre più i profili professionali e richiederà formazione nonché riqualificazioni continue.

BIOTECNOLOGIE E SICUREZZA NAZIONALE

L'attuale fase geopolitica internazionale ha spinto i Paesi UE e l'Italia a porre particolare attenzione, nel più ampio contesto dello sviluppo tecnologico,

anche al **segmento delle biotecnologie**. La **strategicità** di queste ultime per la sicurezza nazionale risiede infatti nella loro **capacità di operare come snodo tra sicurezza, salute e sviluppo industriale**. **Sul piano delle capacità militari**, le biotecnologie incidono in modo crescente sulla protezione del Paese, nonché sulla prevenzione e gestione delle minacce biologiche, che possono essere impiegate in forma deliberata o manifestarsi come effetti collaterali di situazioni di crisi.

Parallelamente, le **biotecnologie** sono diventate una **componente strutturale della sicurezza sanitaria**. Le recenti crisi pandemiche hanno mostrato come la capacità di sviluppare, produrre e distribuire rapidamente soluzioni biomediche innovative sia un fattore decisivo per la resilienza delle infrastrutture economiche e sanitarie di un Paese. In altri termini, il ruolo delle biotecnologie per il futuro della medicina è centrale, in quanto l'innovazione in questo campo sta trasformando radicalmente le frontiere e le capacità di cura delle infrastrutture sanitarie, migliorando l'efficacia dei trattamenti e riducendo i costi per i sistemi nazionali.

Le biotecnologie rappresentano un campo nel quale si giocano contemporaneamente la competitività del sistema produttivo e la crescita economica. Per un Paese come l'Italia, valorizzare questo ambito significa non solo proteggere l'attuale posizione di eccellenza del settore farmaceutico nazionale, ma altresì rafforzarne le capacità di crescita, con esternalità positive anche per il resto del tessuto produttivo.

L'incremento delle biotecnologie influenza tuttavia in modo particolarmente acuto, oltre al citato tema dello sviluppo di un ecosistema finanziario adeguato, anche quello della circolarità dell'innovazione. In particolare, l'**evoluzione delle biotecnologie** è profondamente **connessa a competenze e know-how che afferiscono ad altri ambiti tecnologici e industriali**, come l'intelligenza artificiale, la microelettronica e la robotica. La ricerca biomedica moderna si basa sull'analisi di grandi volumi di dati biologici,

> *Le biotecnologie rappresentano un campo nel quale si giocano contemporaneamente la competitività del sistema produttivo e la crescita economica*

sull'automazione dei processi di laboratorio, sulla modellizzazione computazionale e sull'integrazione tra hardware e software avanzati. Di conseguenza, la crescita delle biotecnologie beneficia direttamente degli investimenti e delle innovazioni che avvengono anche nei settori contigui.

Tutto ciò comporta la **necessità di costruire ambienti favorevoli all'innovazione**, nei quali la politica industriale svolga un ruolo abilitante, evitando di direzionare le risorse verso ambiti specifici, in modo da favorire la formazione di ecosistemi tecnologici integrati. In tali contesti, infatti, i capitali

possono fluire più facilmente tra settori diversi, generando esternalità positive e sinergie cumulative. Questo meccanismo è analogo a quello che ha reso possibile lo sviluppo recente dell'intelligenza artificiale, che non è il risultato di un singolo progresso isolato, ma l'esito di investimenti cumulativi in capacità di calcolo, infrastrutture digitali, algoritmi, formazione avanzata e applicazioni industriali. Allo stesso modo, le biotecnologie possono svilupparsi pienamente solo all'interno di un contesto in cui ricerca scientifica, capitale umano, infrastrutture e finanza innovativa crescono in modo coordinato.

Il confronto internazionale rende questa esigenza ancora più evidente. I sistemi industriali di Stati uniti e Cina stanno investendo in modo massiccio nel settore, in quanto considerato dagli operatori una priorità strategica di lungo periodo. Gli **Stati Uniti** beneficiano di un ecosistema particolarmente dinamico, caratterizzato da una forte integrazione tra università di eccellenza, grandi imprese farmaceutiche, start up e mercati dei capitali estremamente sviluppati. La **Cina**, dal canto suo, sta combinando ingenti investimenti pubblico-privati, pianificazione strategica, rapida crescita delle capacità industriali e scientifiche, con l'obiettivo di ridurre le dipendenze tecnologiche e conquistare posizioni di leadership in segmenti chiave.

Inoltre, rileva la questione del reclutamento dei "talenti" europei (anche italiani) da parte di Pechino, causa di possibile perdita di know-how scientifico e tecnologico.

L'**UE** dispone di una base scientifica solida, di competenze di alto livello e di un tessuto industriale rilevante, ma soffre di una frammentazione dei mercati, di una minore disponibilità di capitali di rischio e di una difficoltà strutturale nel trasformare l'eccellenza scientifica in leadership industriale globale. Il posizionamento europeo nel settore delle biotecnologie è dunque ambivalente. Da un lato, esistono nicchie di eccellenza e una capacità di ricerca di primo piano. Dall'altro, il ritardo nella scala degli investimenti e nella creazione di campioni industriali limita la capacità di competere con i principali attori globali.

> *"La necessità di costruire ambienti favorevoli all'innovazione, nei quali la politica industriale svolga un ruolo abilitante, evitando di direzionare le risorse verso ambiti specifici, in modo da favorire la formazione di ecosistemi tecnologici integrati*

Oltre all'applicazione nel settore sanitario, le biotecnologie rivestono un ruolo abilitante e trasformativo anche in settori quali l'agricoltura, l'ambiente, le filiere alimentari e la bioproduzione. In particolare:

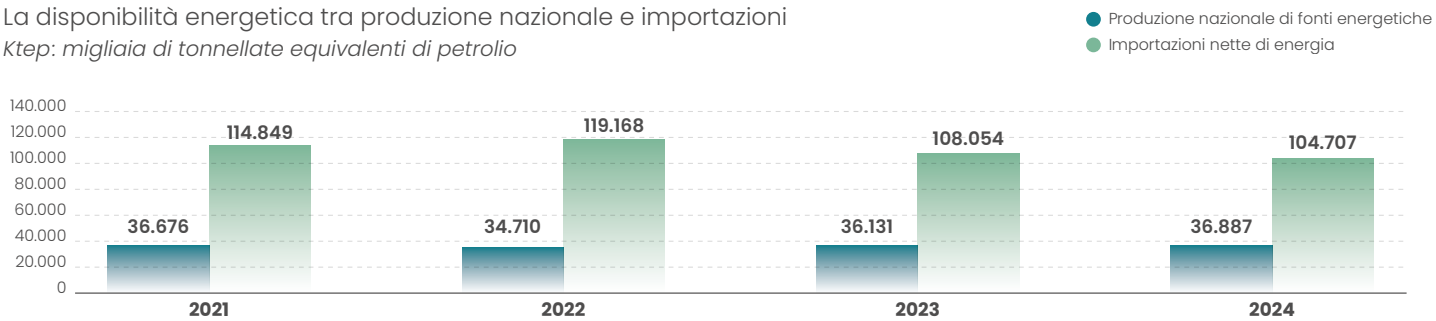
- **biotecnologie per l'agricoltura**. Utili per rendere più resistenti le varietà vegetali, preservando la biodiversità, aumentare le produzioni senza estendere le superfici coltivate, ridurre i consumi di acqua in agricoltura e gli effetti delle aggressioni di parassiti e avversità ambientali, caratterizzare gli alimenti, garantendone (attraverso l'impronta digitale genetica) l'origine, la composizione e le caratteristiche reali;
- **biotecnologie per l'industria**. Il loro ruolo risiede nella capacità di rendere i processi produttivi più efficienti, sostenibili e meno dipendenti dalle risorse fossili. Si va dalla biotrasformazione, mediante catalisi enzimatica, per la riqualificazione di processi industriali, alla preparazione di composti chimici per fermentazione, passando per la produzione di bioplastiche, il biorisanamento e la produzione di bioenergia.

L'APPROVVIGIONAMENTO ENERGETICO ITALIANO

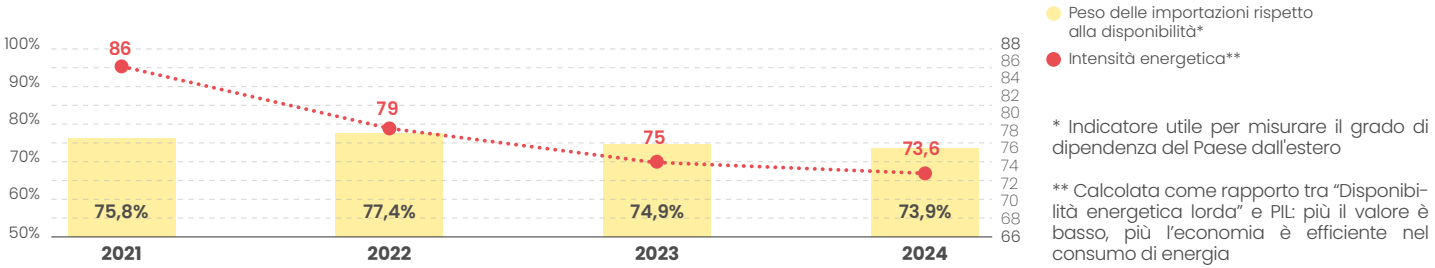
In un modo a crescente conflittualità, l'esigenza di diversificare le fonti di approvvigionamento energetico si somma alla crescente domanda di disponibilità costante di energia per sostenere numerose funzioni essenziali dello Stato. Tutto ciò rende le infrastrutture energetiche, dal punto di vista dell'intelligence, un settore, tra quelli critici per la sicurezza nazionale, meritevole di particolare attenzione.

Il bilancio energetico italiano

La disponibilità energetica tra produzione nazionale e importazioni
Ktep: migliaia di tonnellate equivalenti di petrolio



La dipendenza dall'estero e l'intensità energetica



* Indicatore utile per misurare il grado di dipendenza del Paese dall'estero

** Calcolata come rapporto tra "Disponibilità energetica lorda" e PIL: più il valore è basso, più l'economia è efficiente nel consumo di energia

Focus energia elettrica

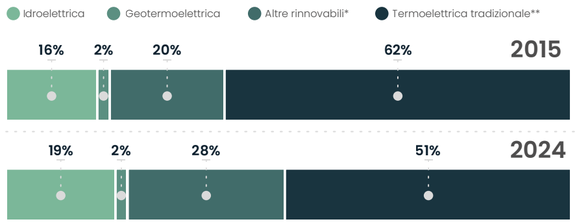
La richiesta in Italia

312,6 mld
di chilowattora
di energia elettrica
richiesti in Italia nel 2024

-4,3%
la variazione della richiesta
di energia elettrica
nel 2024 rispetto al 2015

83,7%
la porzione della richiesta
coperta nel 2024
dalla produzione nazionale

La produzione nazionale

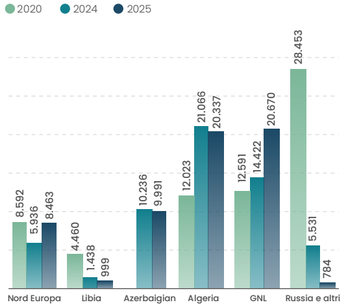


* solare, eolico, rifiuti solidi urbani, biogas, ecc.
** da carbone, gas naturale, prodotti petroliferi e altri combustibili

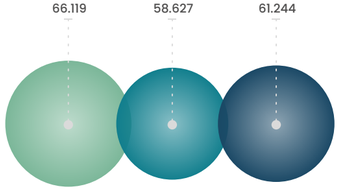
Infrastrutture e punti di ingresso del gas in Italia

Importazione di gas per origine

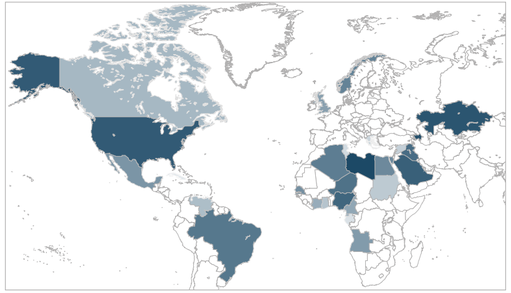
Elaborazione su dati
(Milioni di standard di metri cubi a 38,1 MJ/m³)



Totale

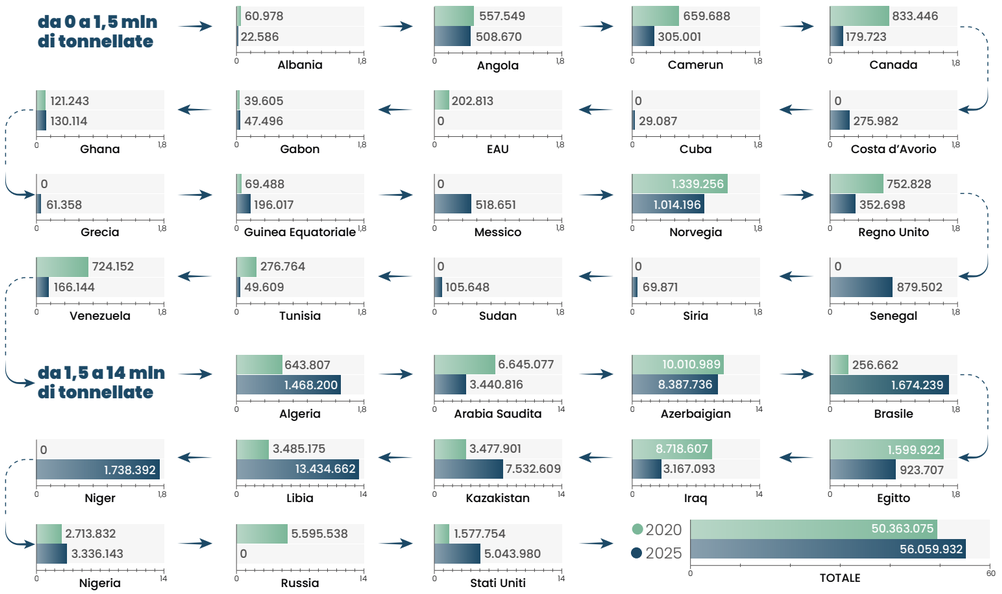


Le importazioni di petrolio greggio per Paese nel 2025 | quantità scaricata (ton) - elaborazione su dati



Libia	13.434.662
Azerbaigian	9.387.736
Kazakistan	7.532.609
Stati Uniti	5.043.980
Arabia Saudita	3.440.816
Nigeria	3.336.143
Iraq	3.167.093
Niger	1.738.392
Brasile	1.674.239
Algeria	1.468.200
Norvegia	1.014.196
Egitto	923.707
Senegal	879.502
Messico	518.651
Angola	508.670
Regno Unito	352.698
Camerun	305.001
Costa D'avorio	275.982
Guinea Equatoriale	196.017
Canada	179.723
Venezuela	166.144
Ghana	130.114
Sudan	105.648
Siria	69.871
Grecia	61.358
Tunisia	49.609
Gabon	47.496
Cuba	29.087
Albania	22.586
TOTALE	**56.059.932**

Importazione di petrolio greggio per Paese - confronto tra 2020 e 2025



Confronto dell'importazione di petrolio da alcuni Paesi produttori (2024-2025)

ALGERIA
2024: 1.086.668
2025: 1.468.200
+35,11%

ANGOLA
2024: 914.794
2025: 508.670
-44,40%

BRASILE
2024: 603.300
2025: 1.674.239
+177,51%

CAMERUN
2024: 570.566
2025: 305.001
-46,54%

COSTA D'AVORIO
2024: 183.626
2025: 275.982
+50,30%

GABON
2024: 494.521
2025: 47.496
-90,40%

EGITTO
2024: 549.237
2025: 923.707
+68,18%

GHANA
2024: 508.764
2025: 130.114
-68,18%

GRECIA
2024: 21.620
2025: 61.358
+183,80%

GUINEA EQUATORIALE
2024: 406.831
2025: 196.017
-51,82%

LIBIA
2024: 11.915.608
2025: 13.434.662
+12,75%

TUNISIA
2024: 134.492
2025: 49.609
-63,11%

SENEGAL
2024: 69.110
2025: 879.502
+1172,61%

VENEZUELA
2024: 331.726
2025: 166.144
-49,92%

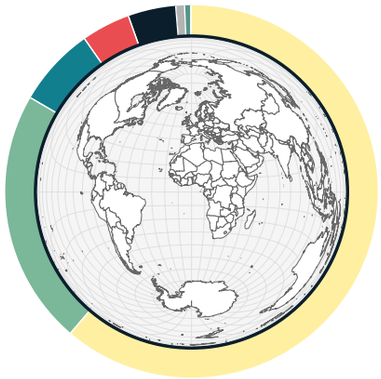
LA DASHBOARD
DEGLI INDICATORI STRATEGICI

3

ECONOMIA

Povertà estrema nel mondo

2020



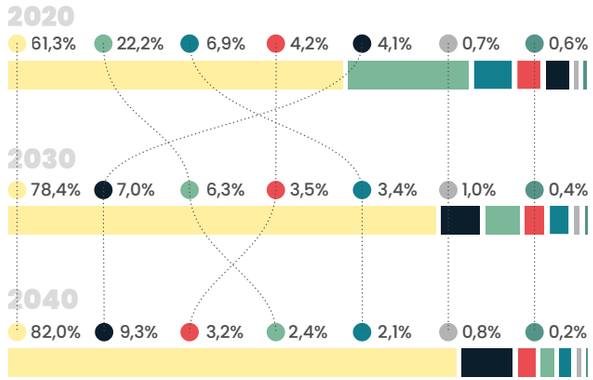
nel **2020** il

61,3%

della povertà estrema nel mondo è concentrata in Africa Sub-Sahariana

- 61,3% Africa Sub-Sahariana
- 22,2% Asia Meridionale
- 6,9% Asia Orientale e Pacifico
- 4,2% America Latina e Caraibi
- 4,1% Medio Oriente e Nord Africa
- 0,7% Altri Paesiad alto reddito
- 0,6% Europa e Asia Centrale

2030 - 2040



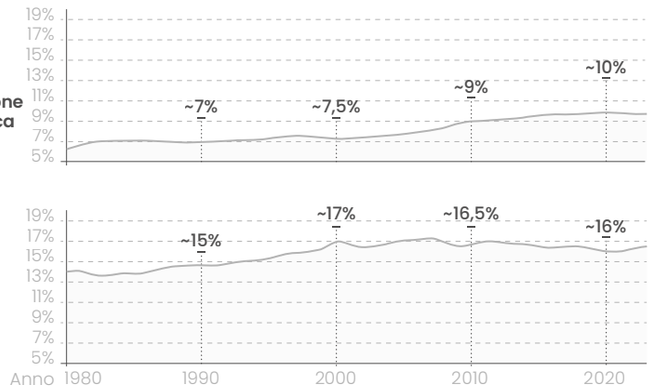
Povertà estrema nel mondo

La lotta alla povertà non rappresenta solo un'azione di giustizia sociale, ma costituisce anche un fattore di stabilizzazione delle società e degli assetti politici e di sicurezza. Dagli anni Novanta ad oggi la popolazione mondiale in condizione di povertà estrema (soglia massima di reddito pari a 3 dollari al giorno) è in calo, passando complessivamente da oltre 2,2 miliardi di persone a circa 0,8 miliardi. Il dato rilevante è la progressiva concentrazione della povertà estrema in due aree del mondo, con evidenti conseguenze di natura politica, economico-sociale e securitaria: 1) Africa Sub-Sahariana; 2) Nord Africa e Medio Oriente. Le proiezioni al 2030 e al 2040 confermano questa linea di tendenza: nel 2040 l'82% della povertà estrema nel mondo sarà concentrata nell'Africa Sub-Sahariana, e il 9,3% in Nord Africa e Medio Oriente.

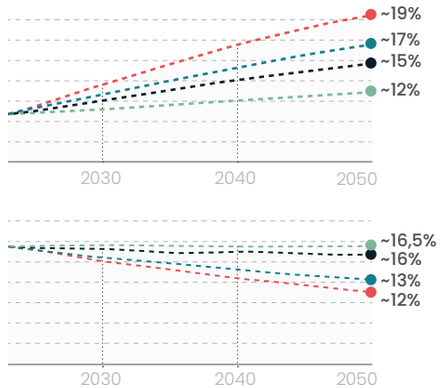
Disuguaglianza nella distribuzione del reddito

BOTTOM 50%
Reddito globale (post tassazione) detenuto dal **50% della popolazione mondiale meno ricca**

TOP 1%
Reddito globale (post tassazione) detenuto dall'1% **della popolazione mondiale più ricca**



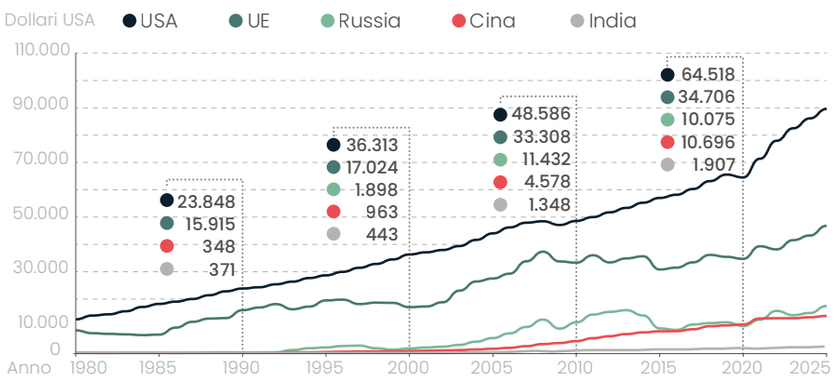
2025 - 2050



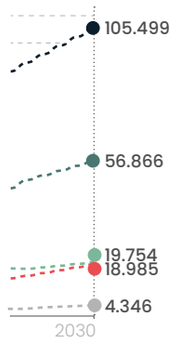
Disuguaglianza nella distribuzione del reddito

Un altro fattore di potenziale instabilità è costituito dalla disuguaglianza nella distribuzione del reddito. Secondo la Banca Mondiale, l'83% dei Paesi del mondo (pari a circa il 90% della popolazione mondiale) vive in condizioni di elevata disuguaglianza.
Il dato rilevante la sicurezza e la stabilità politica sta nel legame tra democrazia e disuguaglianza: l'ultimo rapporto del G20 (novembre 2025) indica come i Paesi con elevata disuguaglianza hanno sette volte più probabilità di subire un declino democratico rispetto ai Paesi più egualitari.
Le proiezioni per i prossimi 25 anni sono correlate alle misure redistributive prima e/o dopo la tassazione dei redditi: in assenza di correttivi, la tendenza alla crescita delle disuguaglianze rimarrà inalterata.

PIL pro capite (prezzi correnti)



2025 - 2030



USA	2025 89.599	2030 105.499	+18%
UE	2025 46.805	2030 56.866	+21%
RUSSIA	2025 17.446	2030 19.754	+13%
CINA	2025 13.806	2030 18.985	+38%
INDIA	2025 2.818	2030 4.346	+54%

PIL pro capite (prezzi correnti)

Tra i grandi attori globali (USA, UE, Cina, Russia), gli Stati Uniti sono, e rimarranno nel futuro prossimo, il Paese con il più alto livello di PIL pro capite. Il divario tra il PIL pro capite USA e quello dell'Unione Europea è costantemente cresciuto negli ultimi 15 anni, e viene stimato in ulteriore crescita nei prossimi cinque: la differenza pari a circa 43 mila dollari nel 2025 aumenterà a oltre 48 mila dollari nel 2030.
Ancor più rilevante il divario tra Russia e USA da un lato, e quello tra Russia e UE dall'altro. Il PIL pro capite russo, dal periodo dell'occupazione della Crimea, subisce un netto divario rispetto a quello statunitense ed europeo, e le proiezioni per i prossimi cinque anni confermano tale divario. La crescita del PIL pro capite europeo è stimata nel 2030 pari al 21% (rispetto al 2025), quella statunitense al 18%, e quella russa solo al 13%.

4. LE RETI DEL CRIMINE TRANSNAZIONALE

La ricerca informativa ha interessato, anche nel 2025, le principali formazioni criminali, che tendono ad associare, alle tradizionali attività illecite, una spiccata propensione a ingerirsi nel tessuto socio-economico.

In particolare, le organizzazioni criminali italiane continuano a essere attori centrali nel panorama dei traffici illeciti nazionali e internazionali. La loro capacità di radicamento territoriale, unita a una forte proiezione transnazionale, consente loro di adattarsi ai cambiamenti dei mercati illegali, mantenendo ruoli primari soprattutto nel narcotraffico, ma anche nel commercio di armi, nel traffico di migranti, nella tratta di esseri umani e nella gestione illegale dei rifiuti. Accanto a questi traffici, si conferma la tendenza a infiltrarsi nei gangli delle pubbliche amministrazioni.

L'interesse dell'intelligence è stato rivolto anche in direzione delle strutture criminali straniere, a partire dalle reti cinesi, nigeriane, albanesi e montenegrine caratterizzate da modelli organizzativi flessibili e da una spiccata vocazione internazionale, spesso complementare o integrata con le consorterie italiane.

I traffici illeciti permangono la fonte principale di alimentazione degli affari gestiti dalla criminalità organizzata, costituendo una minaccia per la sicurezza globale e per il benessere dei Paesi. In tale quadro, è emersa la capacità di adattarsi e rimodulare le strategie, modificando le rotte dei traffici, investendo sui beni maggiormente appetibili, insinuandosi nelle economie legali e creando mercati illeciti "in-

visibili". Si è assistito a una profonda trasformazione dei flussi di droga, guidata per lo più dai rilevanti cambiamenti nell'economia criminale globale e dalla possibilità di sfruttare il dominio digitale (dark web) per le transazioni.

Quanto al traffico di armi, è stata registrata una tendenza all'incremento della circolazione di armi leggere e da guerra provenienti principalmente dall'Europa Orientale e dai Balcani occidentali.

Il traffico di esseri umani costituisce spesso un elemento trasversale e complementare ad altre filiere criminali, con utilizzo delle stesse infrastrutture, in particolare per il narcotraffico e per il commercio di armi.

Il riciclaggio di capitali illeciti rimane il principale volano di infiltrazione nel tessuto economico-finanziario formale, attraverso tecniche in continua evoluzione, che integrano sempre più frequentemente sistemi di pagamento paralleli (criptovalute) e circuiti finanziari occulti.

La corruzione continua a rappresentare un ulteriore fattore trasversale, che agevola il condizionamento di processi amministrativi, economici e politici, generando una significativa alterazione della governance e costituendo un moltiplicatore di opportunità per la criminalità.

Nel 2025, è proseguito il focus informativo sulla sicurezza ambientale, divenuta una dimensione strategica per la tutela degli interessi nazionali, ove l'intreccio tra reti criminali organizzate e degrado ambientale riveste implicazioni che trascendono il mero danno ecologico per interessare la tutela della salute, degli ecosistemi e della biodiversità, gli obiettivi di economia circolare, nonché la stabilità sociale, la sicurezza alimentare e la continuità dei processi di transizione energetica.

PROSPETTIVE DI INTERESSE DELLA CRIMINALITÀ ORGANIZZATA

Le **principali formazioni criminali** dimostrano la tendenza ad **associare, alle tradizionali attività illecite**, la spiccata **propensione a ingerirsi nel tessuto socio-economico**, forti di un'ampia disponibilità di risorse finanziarie liquide e di un network relazionale che consente loro di proiettare la propria sfera d'influenza in chiave internazionale.

A questa minaccia criminale di tipo "tradizionale", si affianca una più "sofisticata" di matrice economico-criminale, espressione di strutturati comitati affaristici in grado di elaborare articolati schemi di riciclaggio, reati finanziari, societari e tributari, nonché di ricorrere alla corruzione e all'ingerenza nei processi decisionali delle amministrazioni pubbliche, distorcendo la concorrenza e captando risorse pubbliche.

L'**approccio della criminalità** assume un respiro, quindi, **sempre più sovranazionale e a connotazione affaristica**. Questa tendenza seguirà il processo evolutivo che caratterizza lo scenario mondiale, interessato da cambiamenti politici, economici, sociali e tecnologici. Le mafie hanno infatti dimostrato nel tempo non solo di sapersi adeguare a quello che accade nella società, ma perfino di anticipare le opportunità speculative e procacciare nuove risorse, dimostrando raffinata capacità relazionale nella gestione di affari illeciti, anche con governi autoritari e organizzazioni terroristiche. Quest'ultimo aspetto qualifica ulteriormente il crimine organizzato come un rischio per la sicurezza nazionale degli Stati democratici.

Tali interconnessioni si coniugano poi con la **spinta delle reti criminali a potenziarsi tecnologicamente** per muoversi velocemente in uno spazio ibrido, caratterizzato da mercati economici iper connessi, dove i confini tra economia legale e illegale sono sempre più permeabili.

Come anticipato, un altro aspetto nodale sarà rappresentato dall'evoluzione tecnologica. Al riguardo, le organizzazioni criminali sfruttano già ampiamente le opportunità offerte:

- dalle comunicazioni crittografate, essenziali nella gestione degli affari illeciti;
- dal dark web, divenuto mercato ideale per lo scambio di illicit goods;
- dalle cryptovalute, che garantiscono l'anonimato delle transazioni finanziarie illecite.

Nel tempo a venire, inoltre, l'utilizzo criminale dell'IA diverrà per le mafie uno strumento formidabile per velocizzare, ampliare, remunerare e nascondere ancora meglio le proprie attività.

L'azione di contrasto alle mafie dovrà essere pertanto supportata da strumenti che siano tecnologicamente evoluti, muovendosi per anticipare e non inseguire le mosse delle organizzazioni criminali.

Risulterà fondamentale l'implementazione normativa, nazionale e sovranazionale, tesa a migliorare la cooperazione internazionale nell'azione

di contrasto e a regolamentare le evoluzioni del mondo digitale, soprattutto per quanto riguarda i fornitori dei servizi sulla rete.

CRIMINALITÀ NAZIONALE E STRANIERA

Le organizzazioni criminali italiane – **'Ndrangheta, Camorra, Cosa Nostra e consorterie pugliesi** – **continuano a rappresentare attori centrali nel panorama dei traffici illeciti nazionali e internazionali**. La loro capacità di radicamento territoriale, unita a una forte proiezione transnazionale, consente alle stesse di adattarsi ai cambiamenti dei mercati illegali, mantenendo **ruoli primari** soprattutto nel **narcotraffico**, ma anche nel **commercio di armi**, nello **sfruttamento della tratta di esseri umani** e nella **gestione illegale dei rifiuti**.

L'azione criminale non si ferma tuttavia ai traffici, come dimostra la **tendenza a infiltrarsi nei gangli delle pubbliche amministrazioni**, testimoniata anche dai vari scioglimenti decretati per infiltrazione della criminalità organizzata nel corso del 2025. In linea di massima, permane dunque una propensione a utilizzare forme di corruzione dei pubblici funzionari e di condizionamento delle procedure di assegnazione dei lavori a evidenza pubblica.

Accanto a queste mafie, operano sul territorio nazionale anche **strutture criminali straniere**. Ci si riferisce, in particolare, a reti cinesi, nigeriane, albanesi e montenegrine caratterizzate da modelli organizzativi flessibili e da una spiccata vocazione internazionale, spesso complementare o integrata con le consorterie italiane.

La **criminalità cinese** in Italia mantiene un basso profilo, anche se recentemente sono state rilevate frequenti forme di intimidazione violenta all'interno della diaspora. Tale consesso criminale continuerà a essere particolarmente attivo nella realizzazione di **articolati schemi di frode fiscale**, che si aggiungono alle **operazioni illecite che producono concorrenza sleale**, alle forme di **usura ed estorsione** (principalmente verso i connazionali), nonché alla **corruzione**, alla luce altresì delle notevoli disponibilità finanziarie di provenienza illecita. Le formazioni criminali cinesi sono da tempo specializzate, infatti, nel riciclaggio e nell'attività finanziaria illecita, tanto da aver realizzato un vero e proprio **sistema parallelo di finanza clandestina** (a disposizione anche della criminalità organizzata nazionale e dei gruppi criminali stranieri) per effettuare trasferimenti di valuta al di fuori dei canali ordinari e controllati.

Le **organizzazioni criminali nigeriane**, di stampo cultista e strutturate in maniera cellulare, restano particolarmente attive nella **tratta di esseri umani a scopo di sfruttamento sessuale e lavorativo**, oltre che nel **narcotraffico** di eroina e cocaina mediante l'impiego di corrieri ovulatori.

La **criminalità albanese**, infine, si conferma come **uno degli attori più dinamici nel narcotraffico**, soprattutto per quanto riguarda la cocaina e la marijuana, grazie a reti consolidate lungo le rotte del Mediterraneo e dei Balcani.

In definitiva, i gruppi criminali, autoctoni o stranieri, continueranno ad adattare i loro metodi alle opportunità che si presenteranno e ai contesti in cui potranno operare, dando priorità alla flessibilità e alla capacità di creare partenariati di affari. I cartelli transnazionali della droga sono un ottimo esempio di questo approccio pragmatico, come testimonia la consolidata cooperazione tra 'Ndrangheta, cartelli sudamericani, gruppi criminali albanesi operanti nei Balcani e intermediari presenti in Africa occidentale.

Inoltre, le reti criminali manifesteranno sempre più la tendenza a non dominare intere filiere, ma presidieranno i punti chiave così da consolidarsi come partner "affidabili".

La volontà di stringere alleanze fra le diverse compagini, in un contesto storico, come quello attuale, connotato da divisioni più che da intese fra Stati, dimostra ancora una volta la capacità della criminalità ad adattarsi al cambiamento e a prosperare negli scenari in continua evoluzione.

LINEE EVOLUTIVE DEI TRAFFICI ILLECITI

I **traffici illeciti** rappresentano la **fonte principale di alimentazione degli affari gestiti dalla criminalità organizzata**, costituendo una minaccia per la sicurezza globale e per il benessere dei Paesi. In un contesto mondiale attraversato da turbolenze geopolitiche, economiche e tecnologiche, i gruppi criminali riescono ad adattarsi e rimodulare strategie, modificando le rotte dei traffici, investendo sui beni maggiormente appetibili, insinuandosi nelle economie legali e creando mercati illeciti "invisibili". Mai, come nell'epoca attuale, l'azione criminale è apparsa più fluida, adattandosi a contesti mutevoli, capitalizzando sulle vulnerabilità emergenti e sfruttando le intersezioni tra problemi di governance, interessi economici e cambiamenti tecnologici. In questo contesto in continua evoluzione, le reti criminali internazionali mostrano un sempre maggiore livello di interconnessione, che si allarga a macchia d'olio interessando anche le organizzazioni italiane, spesso legate a doppio filo con cartelli latinoamericani, gruppi balcanici, reti asiatiche e consorterie africane. La descritta **struttura reticolare dei moderni traffici illeciti, basata su intese e accordi tra consessi criminali di diversa provenienza**, assicura una maggiore resilienza alle operazioni di contrasto e una rapida capacità di riconfigurazione. In questa prospettiva, pertanto, i rapporti operativi tra gruppi italiani e criminalità straniera sono destinati a rafforzarsi.

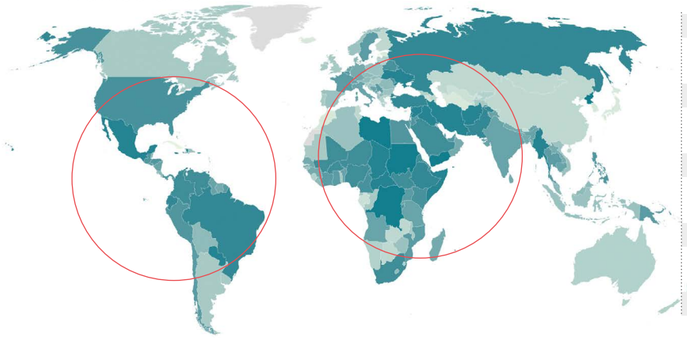
Le linee evolutive dei traffici illeciti sono caratterizzate da una complessa architettura di rotte transnazionali che collegano le aree di produzione, le zone di transito e i mercati di destinazione finali.

I **FLUSSI DELLA DROGA** stanno attraversando profonde trasformazioni, guidate soprattutto dai rilevanti cambiamenti nell'economia criminale globale, che si adegua ai mutamenti geopolitici e logistici contemporanei. Il calo nella produzione di eroina in

1.0 5.0 10.0 Valori degli indicatori della tipologia di traffico

In crescita | Invariato | In diminuzione | Aree geografiche con valori elevati

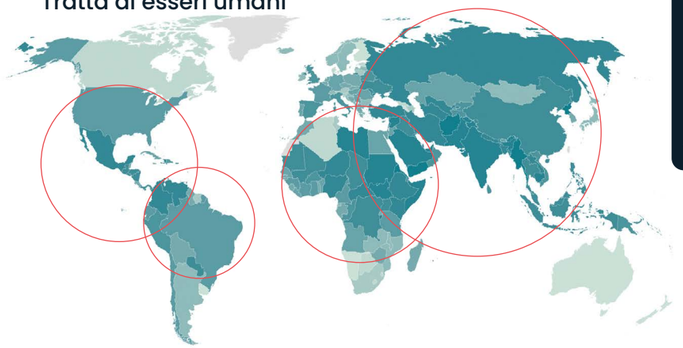
Traffico di armi



Linee di tendenza negli ultimi 5 anni

Afghanistan	↗	Libia	=
Rep. Centrafricana	↗	Messico	↗
Ciad	↗	Myanmar	↗
Rep. Dem. del Congo	↗	Paraguay	↗
Iran	↗	Somalia	↗
Iraq	=	Sudan	↗
Giamaica	↗	Siria	=
Corea del Nord	↗	Ucraina	=
Libano	↗	Yemen	↗

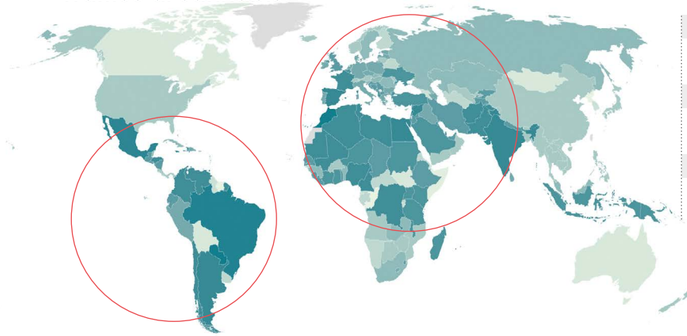
Tratta di esseri umani



Linee di tendenza negli ultimi 5 anni

Afghanistan	↗	Pakistan	↗
Burundi	=	Arabia Saudita	=
Cambogia	↗	Somalia	↗
Eritrea	=	Sud Sudan	=
India	↗	Sudan	↗
Corea del Nord	↗	Siria	=
Libia	↘	Emirati Arabi Uniti	=
Myanmar	↗	Yemen	↗

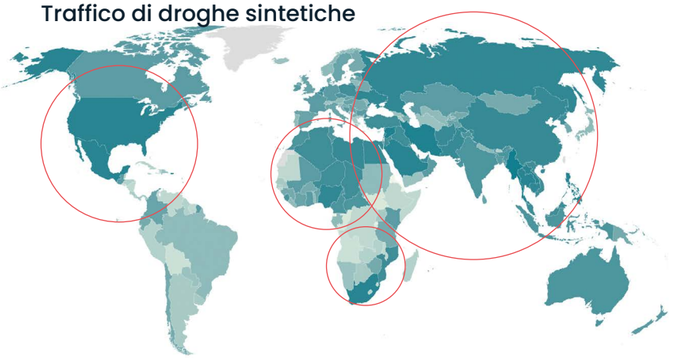
Traffico di cannabis



Linee di tendenza negli ultimi 5 anni

Argentina	↗	Messico	=
Brasile	↗	Marocco	=
Egitto	↗	Paraguay	=
India	=	Spagna	↗
Giamaica	↘	St. Vincent/Grenadine	=
Libano	=	Siria	=

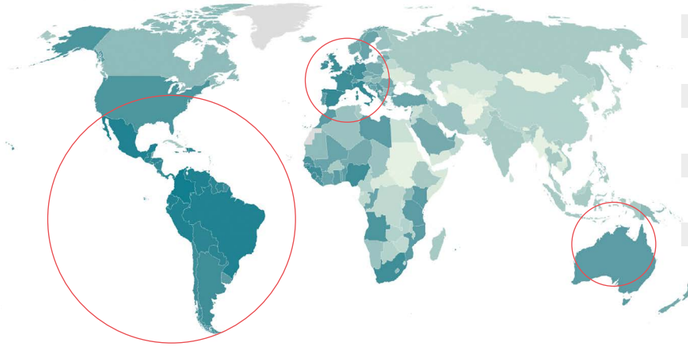
Traffico di droghe sintetiche



Linee di tendenza negli ultimi 5 anni

Afghanistan	=	Filippine	=
Cambogia	↗	Russia	↗
Iran	↗	Arabia Saudita	↗
Laos	↗	Sud Africa	↗
Libano	↗	Siria	=
Messico	=	Thailandia	↗
Myanmar	↗	Ucraina	↗
Nigeria	↗	USA	↗

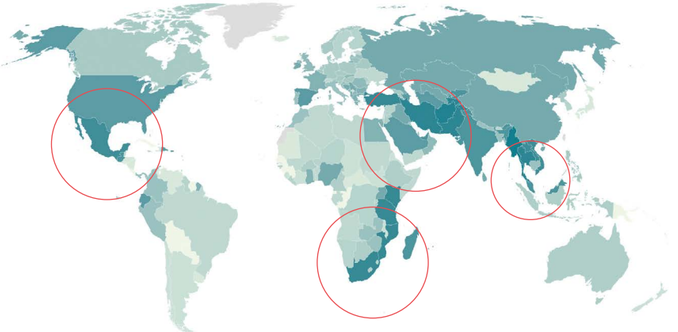
Traffico di cocaina



Linee di tendenza negli ultimi 5 anni

Bolivia	=	Honduras	↗
Brasile	=	Messico	=
Colombia	=	Panama	=
Ecuador	↗	Paraguay	↗
Guatemala	=	Perù	=
Guinea-Bissau	↗	Suriname	=
Guyana	↗	Venezuela	=
Haiti	↗		

Traffico di eroina



Linee di tendenza negli ultimi 5 anni

Afganistan	↘	Seychelles	↗
Iran	↘	Sud Africa	↗
Kenya	↗	Tagikistan	=
Mauritius	=	Tanzania	↗
Mozambico	↗	Thailandia	↗
Myanmar	=	Turchia	=
Pakistan	=		

> *I flussi della droga stanno attraversando profonde trasformazioni, guidate soprattutto dai rilevanti cambiamenti nell'economia criminale globale*

Afghanistan, l'aumento delle forniture di cocaina, la costante crescita del mercato degli oppioidi sintetici e la parziale legalizzazione della cannabis in alcuni Paesi stanno infatti rimodellando gli schemi di produzione, traffico e consumo in tutto il mondo.
In particolare, si segnala che:

- la **cocaina**, prodotta prevalentemente in America Latina, raggiunge i mercati europei principalmente attraverso il percorso marittimo dall'Oceano Atlantico (ove giocano un ruolo centrale i porti di Rotterdam, Anversa, Amburgo; quanto all'Italia, Genova e Gioia Tauro sono gli hub più interessati) e il tragitto terrestre attraverso la regione del Maghreb e poi il Mediterraneo. Le rotte terrestri utilizzano anche i Balcani occidentali quale zona di transito privilegiata, con epicentri criminali localizzati in Albania, dalla quale si dipanano numerosi flussi verso il territorio italiano e nord-europeo;
- il traffico di **eroina e oppioidi sintetici** segue percorsi provenienti dall'Asia (Triangolo d'oro – Myanmar, Thailandia e Laos – e Mezzaluna d'oro – ricompresa tra Afghanistan, Pakistan e Iran), transitando attraverso la Turchia e i Balcani, prima di raggiungere l'Europa. Sebbene la produzione di oppio sia diminuita a seguito del divieto di coltivazione del papavero da oppio vigente in Afghanistan dal 2022, il mercato sembra mostrare una certa stabilità, sostenuto da scorte abbondanti e da fonti di approvvigionamento alternative (Myanmar in particolare, ritornato ai vertici della produzione mondiale di oppioidi a causa della guerra civile in atto dal 2021);
- si sta assistendo a una progressiva espansione delle **metamfetamine e di altre sostanze sintetiche**, le cui principali aree di produzione europee si attestano nei Paesi Bassi e in Belgio. La collaborazione tra gruppi balcanici, mafie italiane e reti criminali asiatiche potrebbe intensificarsi proprio nel segmento delle droghe sintetiche, dove costi di produzione bassi e margini di guadagno elevatissimi favoriscono una produzione difficilmente tracciabile. Le rotte principali nel settore delle droghe sintetiche convergono sulla distribuzione in Europa settentrionale. Per quanto riguarda l'Italia, si evidenzia la crescita del fenomeno delle micro spedizioni e l'uso crescente del dark web per l'acquisto;
- l'emergente duopolio cocaina/droghe sintetiche non dimostra tuttavia che eroina e cannabis stiano perdendo terreno nel narcotraffico globale. La **cannabis**, in particolare, rimane la droga di più ampia diffusione, spinta da una combinazione di fattori sociali e culturali, nonché dai suoi effetti apparentemente meno dannosi

rispetto ad altre sostanze, ma anche per il suo basso costo di produzione.

Inoltre, la coesistenza di mercati legali e illegali per la cannabis pone in evidenza la complessa relazione esistente tra regolamentazione del consumo di stupefacenti e interessi criminali.

Se, da un lato, la legalizzazione può indebolire alcune economie illecite, dall'altro, può spingere i criminali a nuove "scelte di mercato", portandoli così a commerciare altre sostanze, spesso più dannose (emblematici, nel senso, gli effetti letali causati dalla diffusione del fentanyl, soprattutto in Nord America). Al riguardo, un esempio concreto è dato delle droghe sintetiche, che si stanno espandendo a livello globale, evidenziando l'inizio di un importante cambiamento strutturale nei mercati della droga. Tale evoluzione merita specifica attenzione, non solo per la sua capacità di rimodellare le dinamiche del narcotraffico, spingendo la criminalità a massimizzare i profitti, ma anche per i significativi rischi che possono derivare per la salute. In questa prospettiva, rilevano i risultati raggiunti in Italia con l'adozione del "**Piano nazionale di prevenzione contro l'uso improprio del fentanyl e di altri oppioidi sintetici**", che ha rappresentato un modello coordinato a livello inter-istituzionale per offrire una risposta preventiva di sensibilizzazione sul fenomeno e, al tempo stesso, di contrasto mirato all'insorgere dei segnali di diffusione di nuove sostanze psicotrope.

Il **TRAFFICO DI ARMI**, strettamente correlato ai conflitti internazionali e alle tensioni geopolitiche, mostra una **tendenza all'incremento della circolazione di armi leggere e da guerra** provenienti principalmente dall'Europa Orientale e dai Balcani occidentali. I teatri conflittuali aperti nel mondo (da quello russo/ucraino ai conflitti in Africa e nel vicino Oriente) aumentano il potenziale rischio di diffusione di armamento di provenienza illecita e questo rende essenziale un attento monitoraggio delle catene di approvvigionamento e delle rotte del traffico. Al riguardo, un aspetto innovativo di tale traffico sarà quello legato alla **vendita di componentistica per la costruzione e l'assemblaggio di armi utilizzando materiali dual use**, anche attraverso progettazioni (supportate da IA) e stampa di elementi in 3D. Dal quadro delineato, emerge come anche in questo ambito le opportunità offerte dal web per l'acquisto e la spedizione con false dichiarazioni identificative renderanno molto complessa l'azione di controllo.

Il **TRAFFICO DI ESSERI UMANI** costituisce un **elemento trasversale e complementare alle altre filiere criminali**. Occorre evidenziare che ben 2/3 dei migranti irregolari nel mondo sono in balia della criminalità organizzata, prede vulnerabili, attratte con inganno e sottoposte a coercizione dalle reti criminali. Spesso le organizzazioni si appoggiano alle medesime infrastrutture utilizzate per il narcotraffico e il commercio di armi, sfruttando le rotte marittime, terrestri e aeree. Nel contesto attuale l'utilizzo di tecnologie e l'im-

piego di piattaforme digitali diventeranno uno strumento strategico per sollecitare i "clienti", organizzare viaggi e controllare le vittime, nonché per assicurare pagamenti rapidi e sicuri (tramite criptovalute e avvalendosi di money transfer).

Il **COMMERCIO DI PRODOTTI CONTRAFFATTI** (con valori stimati che ammontano annualmente a centinaia di miliardi di dollari), oltre alle ingenti perdite economiche che si concretizzano sotto forma di minori entrate per le aziende e mancati introiti fiscali per gli Stati, genera altresì sfiducia nei consumatori e, in alcuni casi (si pensi ai prodotti farmaceutici ed elettronici), mette a repentaglio la salute pubblica, senza trascurare, tra l'altro, l'effetto critico legato alla gestione dei prodotti contraffatti come rifiuti speciali (come i tessuti di bassissima qualità, caratterizzati da un ciclo d'uso limitato e molto vicino al principio dell' "usa e getta").

Un fattore di spinta del fenomeno della contraffazione è dato dall'aumento dei costi dei prodotti originali, legato per lo più all'andamento dell'attuale contesto economico e all'aumento dei prezzi delle materie prime. Vi è inoltre una stretta correlazione con lo sfruttamento della manodopera, soprattutto nei Paesi dove le garanzie per i lavoratori sono molto labili. La crescita costante della contraffazione sarà pertanto sempre più legata all'innovazione tecnologica, che ha radicalmente abbassato le barriere all'ingresso per gli attori criminali. Le piattaforme di commercio digitale stanno diventando il luogo ideale per l'offerta e l'acquisto dei prodotti contraffatti, che vengono pubblicizzati e acquistati in modo anonimo, con l'utilizzo di sistemi di pagamento spesso non tradizionali, tra cui portafogli digitali e criptovalute. Anche in tale contesto l'intelligenza artificiale potrà essere utilizzata per favorire gli scopi illeciti, coadiuvando i contraffattori nella progettazione di repliche sofisticate, con velocità e precisione sempre crescenti, nonché creando campagne pubblicitarie e individuando potenziali consumatori attraverso strumenti di marketing personalizzati.

FENOMENI TRASVERSALI: RICICLAGGIO, RUOLO DEI SOGGETTI ECONOMICI COMPIACENTI E CORRUZIONE

Il **riciclaggio di capitali illeciti** rimane il **cardine economico mediante il quale le organizzazioni criminali operano nel tessuto economico-finanziario formale**. Le **tecniche di riciclaggio** si sono **evolute** significativamente, integrando sempre più frequentemente **sistemi di pagamento paralleli (criptovalute) e circuiti finanziari occulti**, come l'"underground banking" posto in essere dalla criminalità cinese per operare al di fuori dei sistemi bancari formali, facilitando trasferimenti internazionali di fondi illeciti senza alcuna tracciabilità. Entro tale cornice, la criminalità continuerà a sfruttare società operanti in Paesi non collaborativi, trust opachi, circuiti bancari compiacenti e reti di professionisti collusi. A questo scenario si affiancano **taluni attori economici** che **forniscono reti tecno-**

logiche, documentazione e supporto logistico ai traffici o canali per il riciclaggio di fondi illeciti, attraverso i sistemi finanziari e i mercati immobiliari. Questi soggetti "esterni" finiscono per integrarsi con la criminalità, in un connubio fatto di interessi e reciproca utilità, divenendo indispensabili per il funzionamento delle economie illecite.

La **corruzione** rappresenta un **ulteriore fattore trasversale**, che agevola l'infiltrazione nei processi amministrativi, economici e politici, generando una significativa alterazione della governance e costituendo un moltiplicatore di opportunità per le organizzazioni criminali. Essa rappresenta, pertanto, l'elemento abilitante che consente alle organizzazioni criminali di operare con relativa impunità sia nel settore pubblico che in quello privato.

LA PROSPETTIVA DI CONTRASTO: L'IMPORTANZA DELLA COOPERAZIONE INTERNAZIONALE

Di fronte a questa complessa architettura criminale transnazionale, la **cooperazione internazionale tra Autorità giudiziarie, Forze di polizia e Servizi di intelligence** rappresenta il perimetro più efficace per difendere gli Stati, i cittadini e i sistemi economici e sociali dalla minaccia criminale. Tuttavia, emerge dal contesto geopolitico contemporaneo il paradosso per cui, di fronte all'attuale maggiore sofisticatezza e interconnessione delle minacce criminali globali, gli Organismi internazionali incontrano difficoltà strutturali e un indebolimento nel consenso politico.

Le **iniziative multilaterali**, storicamente determinanti nel coordinamento delle operazioni di contrasto e nell'armonizzazione dei quadri normativi, risultano sottoposte a pressioni significative dovute a frammentazioni geopolitiche, risorse limitate e conflitti di interesse tra Stati. I percepiti segnali di una possibile diminuzione della cooperazione tra Paesi rappresentano un vulnus nel contrasto alle economie illecite, soprattutto rispetto a quelle operanti a livello transfrontaliero. L'indebolimento della fiducia e della solidarietà tra Stati riduce altresì la capacità del sistema di contenere reti criminali la cui influenza si estende sistematicamente oltre le giurisdizioni nazionali.

Le prospettive future richiedono, quindi, una rinnovata valorizzazione dei meccanismi di cooperazione internazionale, con particolare riguardo ai canali bilaterali e plurilaterali. Gli Organismi di cooperazione giudiziaria e di polizia, insieme alle Agenzie di intelligence dovranno pertanto intensificare gli sforzi di coordinamento per tracciare e interdire i flussi criminali, creando al contempo sinergie per contrastare il narcotraffico, il riciclaggio e le reti di corruzione che sottendono le filiere criminali contemporanee. Nel senso, sarà essenziale lo **sviluppo di quadri normativi internazionali convergenti** (si pensi alla regolazione delle criptovalute e al rafforzamento dei meccanismi di trasparenza nei flussi finanziari transfrontalieri) e l'**allineamento degli strumenti tecnologici di supporto alle investigazioni**.

Un altro aspetto nodale sarà quello di **continuare ad affiancare al contrasto delle condotte illecite** specifiche **misure** atte ad assicurare la sistematica **sottrazione delle risorse economiche ai gruppi criminali**. Nel senso, l'azione dell'Intelligence potrà risultare determinante, specie laddove riuscirà ad anticipare il manifestarsi delle fenomenologie criminali, fornendo elementi di valutazione e informativi, da un lato, ai decisori politici, affinché implementino le misure di prevenzione della minaccia, dall'altro, agli Organi di polizia, così da favorirne l'azione repressiva.

USO DELLE DISTRIBUTED LEDGER TECHNOLOGY A FINI DI RICICLAGGIO

La prospettiva di contrasto alla criminalità organizzata deve avere quale elemento qualificante l'individuazione dei canali di finanziamento delle attività illecite e del reimpiego di capitali nell'economia legale. **Colpire le fonti di approvvigionamento delle risorse finanziarie** rappresenta, infatti, l'**obiettivo prioritario nella lotta alle mafie**.

Il riciclaggio di capitali illeciti costituisce, quindi, una "minaccia all'interno della minaccia", connotata dalla ricerca continua di nuovi spazi e modalità per dissimulare e reimpiegare il frutto finanziario delle attività criminali.

Le tecniche investigative a contrasto delle organizzazioni mafiose sono ormai da tempo strutturate sull'individuazione dei canali che consentono di riciclare la ricchezza proveniente dalle attività illecite, immettendola nel tessuto economico legale. Questo indirizzo, che è entrato nella cultura investigativa e giudiziaria con la frase **"follow the money"**, è sempre più valido, nonostante oggi l'orizzonte del riciclaggio si sia aperto agli ecosistemi digitali che, esistendo al di fuori dei tradizionali canali di intermediazione finanziaria, rendono ancora più difficile seguire le "tracce" del denaro sporco (o forse meglio dire delle cripto attività illecitamente utilizzate).

In questa frontiera virtuale l'attività di riciclaggio non mira tanto a nascondere le transazioni, quanto a camuffare e rendere irriconoscibile il collegamento tra i proventi illeciti e l'identità del soggetto che ne dispone.

I **cripto asset** diventano, quindi, **veicolo di conversione del denaro di provenienza illecita**, oltre a poter costituire lo strumento di regolazione degli affari criminali (si pensi al traffico di stupefacenti o di armi).

Per trasformare il denaro sporco in valori virtuali la criminalità utilizza le piattaforme exchange centralizzate, che consentono di acquistare criptovalute utilizzando moneta fiat (anche semplicemente un ATM per criptovalute può assolvere a tale funzione). Dopo questo passaggio di "inserimento" ("immissione" – "on ramp") nel sistema virtuale, la fase successiva è quella di offuscare la provenienza e destinazione dei valori ("stratificazione" – "layering"), sfruttando la frammentazione dei fondi ovvero spostandoli rapidamente tra sistemi digitali differenti, tendenzialmente in Paesi diversi.

In questo passaggio le tecniche di "mixer", parcellizzando e mescolando i depositi di numerosissimi utenti, rescindono quasi definitivamente la connessione tra i fondi originari e quelli di destinazione.
Esistono poi le **piattaforme decentralizzate**, quelle dove si muovono esclusivamente le criptovalute e sono basate su movimenti che avvengono solo sulla blockchain di riferimento. Queste piattaforme facilitano lo scambio peer to peer e, pertanto, non prevedendo l'intervento di intermediari abilitati, consentono di evitare ogni forma di controllo sull'identità degli utenti.
Attualmente, gli **asset più utilizzati per fini illeciti sono le stablecoin**, basate sul principio di collegamento diretto con il valore di una moneta fiat, che le rende più sicure rispetto al rischio di volatilità delle altre criptovalute.
A disposizione dell'utilizzo illecito si pongono, inoltre, le cc.dd. **privacy coin**, asset che risultano completamente opachi e che garantiscono l'effettivo anonimato delle transazioni. A differenza delle altre criptovalute, che sulle loro blockchain lasciano traccia con codici alfanumerici identificativi collegati alle singole transazioni, le privacy coin (vietate in vari Paesi del mondo) utilizzano tecniche crittografiche volte a rendere opachi originatori e destinatari, attraverso meccanismi di anonimizzazione e offuscamento delle transazioni (es. firme ad anello, indirizzi "stealth" e/o prove a conoscenza zero), frammentando le firme digitali e generando indirizzi sempre nuovi, che durano il tempo della transazione, oltre a essere noti soltanto a chi invia e a chi riceve i valori.
In definitiva, emergono molteplici modalità di utilizzo malevolo delle nuove tecnologie, che la criminalità può distorcere anche al fine di reimpiegare i proventi illeciti nel sistema economico ("integrazione" – "off ramp"). Forse è proprio questa la fase più debole dell'architettura tipica del riciclaggio, dato che, nel momento in cui le risorse devono essere impiegate sul mercato per acquistare beni e realizzare investimenti, abbandonano il mondo virtuale andando incontro ai tradizionali metodi di contrasto.

> *"A disposizione dell'utilizzo illecito si pongono le cc.dd. privacy coin, asset che risultano completamente opachi e che garantiscono l'effettivo anonimato delle transazioni*

Ciò nonostante, è sempre possibile che questa "virtualità" permanga, in quanto le **criptovalute** potrebbero essere utilizzate **per acquistare beni "non fungibili"**, come ad esempio le opere d'arte "virtuali" (immagini, video, audio – cc.dd. Non Fungible Token-NFT), successivamente rivendibili anche ad acquirenti in buona fede.
Tornando, quindi, alla fondamentale indicazione "follow the money", emerge oggi la necessità di rafforzarla con il concetto di **"follow the virtual money"**, che implica la necessità di disporre di

strumenti normativi e tecnologici adeguati, nonché costantemente aggiornati nell'azione di contrasto all'utilizzo illecito delle criptovalute, che deve essere orientata alla deanonimizzazione delle transazioni e alla individuazione e conseguente sottrazione delle risorse alla criminalità. Sarà pertanto sempre più rilevante l'analisi della blockchain, utilizzando adeguati strumenti computazionali e le capacità offerte dall'IA per riconoscere schemi, comportamenti, tempistiche e frequenza delle transazioni.

SICUREZZA AMBIENTALE E INTERESSI CRIMINALI

La sicurezza ambientale rappresenta una dimensione strategica per la tutela degli interessi nazionali, in un contesto globale caratterizzato da crescenti pressioni sulle risorse naturali, cambiamenti climatici e una progressiva infiltrazione criminale nei settori legati all'ambiente. L'**intreccio tra reti criminali organizzate e degrado ambientale** riveste implicazioni che trascendono il mero danno ecologico per interessare la tutela della salute, degli ecosistemi e della biodiversità, gli obiettivi di economia circolare, nonché la stabilità sociale, la sicurezza alimentare e la continuità dei processi di transizione energetica.

Le minacce investono, quindi, ambiti interconnessi. Esempi in tal senso sono offerti dalla gestione criminale del ciclo dei rifiuti, dall'inquinamento industriale e dal traffico illecito di materiali pericolosi, dalla deforestazione (con il connesso fenomeno degli incendi boschivi). In tale quadro, rileva, altresì, il **processo di decommissioning degli impianti nucleari dismessi**, oltre che il **contrasto dei rischi derivanti dalla gestione, detenzione e traffico di materiali chimici, biologici, radiologici e nucleari (CBRN)**.

I reati legati all'ambiente sono pertanto destinati ad assumere rilevanza crescente, anche a causa della loro redditività economica, che attrae interessi criminali e affaristici. Le "eco-mafie", inoltre, risultano sempre più articolate e transnazionali, tanto da avvalersi con sempre maggiore frequenza di entità giuridiche di diritto estero costituite in Paesi con normative in materia ambientale meno rigide. Un'architettura, questa, che viene anche favorita da operazioni di riciclaggio internazionale e dal ricorso alla corruzione di pubblici funzionari.

I **profili di minaccia** possono essere così elencati:

- le **attività industriali ad alto impatto ambientale**, con particolare riguardo a quelle interessate da processi produttivi chimici, siderurgici e petroliferi, continuano a essere esposte a fenomeni di inquinamento del suolo, dell'aria e delle acque, talvolta derivanti da omissioni, comportamenti negligenti o deliberate elusioni delle normative. Le dinamiche di riconversione energetica e decarbonizzazione rischiano di lasciare spazio a queste criticità, creando vulnerabilità nelle fasi di conversione degli impianti e delle filiere produttive. In tali ambiti possono

> *L'intreccio tra reti criminali organizzate e degrado ambientale riveste implicazioni che trascendono il mero danno ecologico per interessare la tutela della salute, degli ecosistemi e della biodiversità, gli obiettivi di economia circolare, nonché la stabilità sociale, la sicurezza alimentare e la continuità dei processi di transizione energetica*

insinuarsi gli interessi della criminalità, tradizionalmente interessata ad aggredire le aziende in difficoltà o in trasformazione, sfruttando situazioni di debolezza per infiltrarsi nella gestione dei servizi ambientali o per favorire pratiche illecite di smaltimento. Al riguardo, uno dei settori oggetto di attenzione è quello della contaminazione da sostanze per/polifluoralchiliche (PFAS), largamente impiegate in numerosi processi industriali ed estremamente dannose per la salute;

- il **ciclo dei rifiuti** rimane uno dei comparti più esposti alle interferenze criminali. Lo smaltimento irregolare dei rifiuti urbani, speciali e pericolosi rappresenta una fonte di profitto elevatissima, alimentata da differenziali di costo tra procedure legali e pratiche illegali (rilevante, nel senso, anche al traffico illegale di rifiuti da apparecchiature elettriche ed elettroniche, in considerazione non solo dei danni ambientali che possono derivare dagli illeciti smaltimenti, ma anche a causa dell'assenza di cautele volte ad assicurare il corretto e proficuo riciclo finalizzato al recupero delle materie prime critiche);
- i **processi di recupero di energia mediante termovalorizzazione**, in parallelo con la catena del "riciclo", costituiscono una misura di stabilizzazione per impedire situazioni emergenziali, soprattutto nelle grandi aree urbane. Significativo, in tale contesto, il rischio di esposizione delle procedure di realizzazione degli impianti e della scelta dei siti ove realizzarli ai condizionamenti della criminalità, oltre alle criticità connesse al conferimento di materiali speciali non idonei all'incenerimento;
- i **rifiuti speciali** – specie ove derivanti da attività sanitarie, industriali e tecnologiche – e, tra gli stessi, i materiali radioattivi di origine non elettronucleare, la cui gestione impropria può generare danni irreversibili per la salute umana e per l'ambiente;
- il tema del **"nucleare"**, legato nel nostro Paese alla gestione degli impianti in dismissione, anche alla luce del fatto che il decommissioning costituisce un processo lungo, delicato e costoso sul quale possono convergere profili di natura illecita, ma anche rischi di mala gestio. In particolare, negli ultimi anni è aumentata a livello globale la quantità di materiali industriali contaminati (come tubature e componenti metalliche) entrati in catene di approvvigionamento legittime, sfruttando carenze strutturali nella prevenzione dello smaltimento non autorizzato di sorgenti radioattive;

- il **traffico illecito di materiali chimici, biologici, radiologici e nucleari**, anche attraverso le rotte consolidate del contrabbando internazionale, espone al rischio che tali beni finiscano in laboratori non autorizzati, dove, attraverso l'impiego di tecnologie a basso costo e intelligenza artificiale, possono essere realizzati prodotti e sostanze nocive per uso criminale o terroristico (si pensi, ad esempio, ad agenti patogeni, ma anche alla sintesi di nuove sostanze psicotrope sintetiche);
- la **tutela della filiera agroalimentare** rappresenta un settore strategico dell'economia italiana, oltre che un ambito all'interno quale è possibile rilevare molteplici condotte fraudolente incidenti sulla qualità dei prodotti (sofisticazioni, adulterazioni), sulle dichiarazioni di origine (falsificazione) e sulla concorrenza leale (contraffazione dei marchi proprietari e del "Made in Italy"). Gli interessi criminali si coniugano, tra l'altro, con quelli di attori esterni interessati non solo a penetrare illegalmente il mercato italiano con prodotti a bassa qualità (non sottoposti ai rigidi controlli previsti dalla normativa nazionale e dell'Unione europea), ma altresì a sfruttarne illegalmente il relativo brand all'estero;
- la **"deforestazione"**, riferibile al consumo di suolo agricolo (con perdita di aree coltivabili e conseguente danno al settore) e boschivo (per i danni alla biodiversità, l'erosione e il rischio geologico). Anche su questo aspetto l'incidenza delle condotte criminali (si pensi agli incendi boschivi dolosi) e i profili di mala gestio possono arrecare danni gravissimi che sfociano nel dispendio di risorse pubbliche per mitigarne gli effetti.

Tanto premesso, i sistemi di prevenzione, controllo e intelligence ambientale rappresentano un'esigenza fondamentale nella prospettiva di salvaguardare la salute dei cittadini e tutelare l'ecosistema. In questo senso, la creazione di piattaforme digitali interoperabili, contenenti i dati ambientali a disposizione degli Organismi deputati alla pianificazione e al controllo, potrebbe rappresentare un importante potenziamento della governance in tema di tutela e sicurezza dell'ambiente. Anche in questo caso, l'utilizzo di sistemi di IA, addestrati alle esigenze di osservazione di immagini e dati satellitari, analisi delle informazioni, rilevamento delle emergenze e criticità, potrà essere di fondamentale utilità per superare bias cognitivi e favorire, al contempo, un'azione ancora più coordinata da parte di tutte le Autorità competenti.

La protezione dell'ambiente e delle risorse naturali non può infatti prescindere da un approccio integrato, che unisca capacità tecniche, strumenti normativi avanzati e una costante collaborazione tra istituzioni nazionali, Organismi europei e partner internazionali. **Garantire la sicurezza ambientale significa difendere la salute dei cittadini e la competitività economica del Paese**, in uno scenario connotato dall'interconnessione tra criminalità organizzata e impropri interessi speculativi, anche di matrice estera.

5. LE DINAMICHE DELLA MINACCIA INTERNA

Nel 2025, gli sviluppi della minaccia interna hanno confermato, e talvolta accentuato, alcune delle tendenze già emerse negli ultimi anni.

Con riferimento all'estrema destra internazionale, la dimensione online resta centrale rispetto a percorsi di radicalizzazione che assumono sempre di più uno spiccato carattere transnazionale. Gli ecosistemi digitali svolgono un ruolo determinante soprattutto nell'ambito della radicalizzazione giovanile, dove si continua a registrare un progressivo abbassamento dell'età di inizio dei processi di radicalizzazione e un'ulteriore compressione delle tempistiche. Parallelamente, si è consolidata la tendenza a sviluppare profili ideologici "misti", nei quali spesso convivono in modo atipico elementi estrapolati dal suprematismo bianco e dal jihadismo.

Quanto allo scenario contestativo ed eversivo interno, resta centrale il tema dell'opposizione alla guerra, agli investimenti bellici e all'"imperialismo", anche in funzione degli sviluppi delle crisi internazionali.

L'attivismo anarco-insurrezionalista si conferma come il vettore di minaccia più concreto, anche alla luce dei recenti attentati compiuti nel contesto delle proteste contro i Giochi Olimpici Milano-Cortina ai danni della rete ferroviaria nazionale. Nel 2025 l'attenzione dei circuiti libertari si è concentrata soprattutto sulla denuncia delle ricadute interne delle guerre, attraverso la critica all'aumento della spesa militare e all'asserita spinta verso la militarizzazione della società, nonché sul contrasto alla "repressione", nel cui solco s'inseri-

scono le mobilitazioni contro i recenti interventi legislativi in materia di sicurezza. Particolare attenzione è stata rivolta altresì al tema dell'intelligenza artificiale, la cui "filiera" è stata considerata quale obiettivo da colpire nella prospettiva di "sabotare la guerra". Inoltre, tale tecnologia viene vista come un nuovo strumento di accumulazione capitalista, in cui il valore dei dati generati dagli utenti diventa l'oggetto di una "corsa all'oro" digitale.

Gli ambienti dell'oltranzismo marxista-leninista hanno anch'essi riservato un'attenzione strumentale agli sviluppi delle crisi internazionali in corso, con l'obiettivo di dare maggiore risonanza a iniziative antimilitariste e anti-atlantiste, nonché di collocare il sostegno alla causa palestinese in una cornice anticapitalista.

Analogamente, l'eterogeneo movimento antagonista ha cavalcato l'onda mobilitativa contro il conflitto a Gaza per favorire la convergenza tra tematiche e istanze diverse, nonché per ricompattare il fronte del dissenso facendo leva sull'antisionismo, sulla denuncia della c.d. "economia di guerra" e sulle sue ricadute in ambito socio-economico. Tale mobilitazione, nel corso del 2025, si è progressivamente sovrapposta al percorso di lotta contro il c.d. "Decreto sicurezza". In questa cornice, la campagna anti-repressiva ha stigmatizzato l'asserita criminalizzazione del dissenso ProPal, anche in seguito ad alcune operazioni di polizia giudiziaria condotte contro militanti coinvolti nelle violenze occorse durante iniziative di piazza.

SVILUPPI DELLA MINACCIA

Nel 2025 gli sviluppi della minaccia interna hanno confermato, e talvolta accentuato, alcune delle tendenze già emerse negli ultimi anni. Con riferimento all'**estrema destra internazionale**, la dimensione online resta centrale - sia a livello individuale sia di gruppo – rispetto a percorsi di radicalizzazione che assumono sempre di più uno spiccato carattere transnazionale. Gli ecosistemi digitali svolgono un ruolo determinante soprattutto nell'ambito della radicalizzazione giovanile, dove si continua a registrare un progressivo abbassamento dell'età di inizio dei processi di radicalizzazione – che coinvolgono anche soggetti infra-quattordicenni – e un'ulteriore compressione delle tempistiche. Parallelamente, si è consolidata la tendenza a sviluppare **profili ideologici "misti"**, nei quali spesso convivono in modo atipico **elementi estrapolati dal suprematismo bianco e dal jihadismo**. In tali casi, più che una reale adesione ideologica, ciò che emerge è una propensione al consumo di contenuti violenti presenti online, rafforzata da generiche pulsioni antisistema e da dinamiche di emulazione.

Quanto all'evoluzione dello **scenario contestativo ed eversivo interno**, resta centrale il tema dell'opposizione alla guerra, agli investimenti bellici e all'"imperialismo", anche in funzione degli sviluppi delle crisi internazionali , in particolare dell'andamento del conflitto in Medio Oriente.

L'**attivismo anarco-insurrezionalista** si conferma come il vettore di **minaccia più concreto** anche alla luce dei recenti attentati compiuti nel contesto delle proteste contro i Giochi Olimpici Milano-Cortina ai danni della rete ferroviaria nazionale. Nel 2025 l'attenzione dei **circuiti libertari** si è concentrata soprattutto sulla denuncia delle ricadute interne delle guerre, attraverso la critica all'aumento della spesa militare e all'asserita spinta verso la militarizzazione della società, nonché sul contrasto alla "repressione", nel cui solco s'inseriscono le mobilitazioni contro i recenti interventi legislativi in materia di sicurezza.

Gli ambienti dell'**oltranzismo marxista-leninista** hanno anch'essi riservato un'attenzione strumentale agli sviluppi delle crisi internazionali in corso, con l'obiettivo di dare maggiore risonanza a iniziative antimilitariste e anti-atlantiste, nonché di collocare il sostegno alla causa palestinese in una cornice anticapitalista. Non è mancato un rinnovato attivismo in favore dei "rivoluzionari prigionieri", sviluppato anche in concorso con omologhi circuiti internazionali, che ha cercato sinergie con le componenti del dissenso più attive sul fronte del sostegno alla causa palestinese.

Analogamente, l'eterogeneo movimento antagonista ha cavalcato l'onda mobilitativa contro il conflitto a Gaza per favorire la convergenza tra tematiche e istanze diverse, nonché per ricompattare il fronte del dissenso facendo leva sull'antisionismo, sulla denuncia della c.d. "economia di guerra" e sulle sue ricadute in ambito socio-economico. Tale

mobilitazione, nel corso del 2025, si è progressivamente sovrapposta al percorso di lotta contro il c.d. "Decreto sicurezza". In questa cornice, la campagna anti-repressiva ha stigmatizzato l'asserita criminalizzazione del dissenso ProPal, anche in seguito ad alcune operazioni di polizia giudiziaria condotte contro militanti coinvolti nelle violenze occorse durante iniziative di piazza.

LA PROSPETTIVA ANTI-TECNOLOGICA

Nel quadro descritto, l'**opposizione alla tecnologia** è un **tema strumentalizzato dal dissenso antagonista** per favorire la convergenza tra i diversi fronti della contestazione. Tramite la critica alla tecnologia e alla sua natura "dual-use", varie componenti del dissenso hanno infatti collegato il conflitto nella Striscia di Gaza alle tradizionali tematiche d'area, quali la critica alla "repressione" e al sistema carcerario, l'antimilitarismo, l'antifascismo, l'anticapitalismo e la lotta contro le nocività.

La prospettiva anti-tecnologica è, in effetti, trasversale al composito panorama dell'estremismo endogeno, benché si declini con sfumature diverse tra i sodalizi anarco-insurrezionalisti, gli ambienti marxisti-leninisti e l'eterogeneo fronte antagonista. Un tratto comune è la **convinzione** che la **tecnologia** sia innanzitutto uno **strumento sviluppato e impiegato dallo Stato in funzione repressiva**.

In quest'ottica, l'opposizione alla guerra nei diversi teatri internazionali e la denuncia di pratiche repressive nel contesto nazionale sarebbero due facce della stessa medaglia. L'impiego delle tecnologie in ambito bellico – nei sistemi d'arma, di sorveglianza e di raccolta informativa – è infatti presentato come una fase sperimentale, che preluderebbe all'adozione delle stesse tecnologie anche in ambito interno. Analoga critica si estende anche ai processi di automazione e digitalizzazione, usati sia in ambito industriale che civile, come emerge dalle contestazioni contro le Smart Cities.

Su tale sfondo, gli **ambienti estremisti** hanno visto nella **mobilitazione pro Palestina** un'opportunità per **veicolare una propaganda** che ha assunto toni sempre più radicali, nella quale istanze antisioniste sono state innestate su una lettura della **tecnologia come strumento che favorirebbe la progressiva militarizzazione della società**. In quest'ottica rileva in particolare la chiamata al blocco e al sabotaggio della c.d. "logistica di guerra".

L'OPPOSIZIONE ALL'INTELLIGENZA ARTIFICIALE

I **circuiti più oltranzisti** hanno riservato particolare **attenzione all'intelligenza artificiale** (IA) e ai suoi molteplici campi di applicazione. Un'attenzione che, specialmente negli ambienti anarco-insurrezionalisti, già negli anni passati si era tradotta in "azioni dirette" violente. Nella propaganda d'area, l'opposizione all'IA è un tema sempre più utilizzato per rafforzare la saldatura tematica tra opposizione alla

> *Gli ecosistemi digitali svolgono un ruolo determinante soprattutto nell'ambito della radicalizzazione giovanile, dove si continua a registrare un progressivo abbassamento dell'età di inizio dei processi di radicalizzazione e un'ulteriore compressione delle tempistiche*

tecnologia, antimilitarismo e antirepressione.
In quest'ottica, la critica alle attività militari di Israele, anche attraverso il prisma dell'intelligenza artificiale, viene estesa alla filiera bellica nazionale, nonché ai rapporti tra l'industria militare e la ricerca accademica. La **"filiera dell'IA"**, con particolare riguardo ai data center, alle aziende legate al comparto della Difesa, ai centri di ricerca privati e alle collaborazioni in ambito universitario è considerata quale **obiettivo da colpire nella prospettiva di "sabotare la guerra"**.
Parallelamente, l'**IA** è anche vista come un **nuovo strumento di accumulazione capitalista**, in cui il valore dei dati generati dagli utenti diventa l'oggetto di una "corsa all'oro" digitale. È nell'ambito dell'opposizione a tale "capitalismo tecnologico" che sono da rintracciare le motivazioni di alcuni attacchi compiuti nel 2025.

LE NUOVE TECNOLOGIE COME ELEMENTO ABILITANTE

Se la postura anti-tecnologica accomuna le varie anime dell'antagonismo interno, diverso è l'approccio che emerge nei **circuiti virtuali dell'estrema destra suprematista e "accelerazionista" internazionale**. In tali ambienti, infatti, le **nuove tecnologie** sono usate come **elementi abilitanti per rafforzare la capacità di diffusione della propaganda** estremista, veicolare idee e simbologie, nonché plasmare sottoculture digitali che contribuiscono a definire un'identità di gruppo. Si tratta, perlopiù, di tecnologie commerciali di facile reperibilità, caratterizzate da modalità d'impiego non particolarmente sofisticate. In questo modo, la soglia d'accesso agli ambienti e ai linguaggi digitali d'area viene mantenuta bassa, facilitando l'avvicinamento di nuovi affiliati.
Gli ambienti accelerazionisti continuano a impiegare strategie di manipolazione degli algoritmi delle piattaforme social al fine di amplificare la diffusione della propaganda d'area, anche usando approcci diversificati da un social all'altro per massimizzarne l'impatto e sviluppare un ecosistema digitale estremista che sia presente su molteplici piattaforme.
Si conferma il ricorso ad applicativi di **intelligenza artificiale generativa** – anche attraverso tecniche di elusione dei parametri di sicurezza – per la produzione di immagini, meme e video che diventano virali anche nei circuiti digitali non estremisti. L'in-

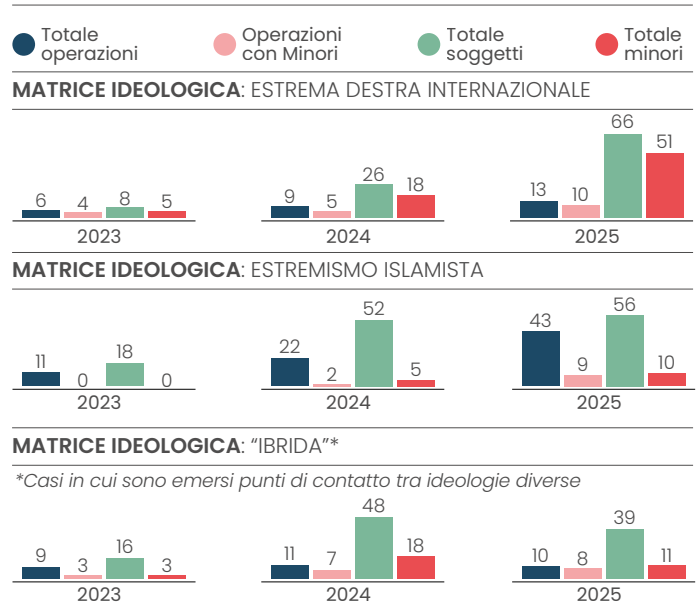
tento è di aumentare l'appeal della propaganda presso audience diversificate al fine di normalizzare il messaggio estremista. Di rilievo, inoltre, l'**impiego crescente di tecnologie per l'anonimizzazione online**.

Una serie di operazioni di polizia effettuate nel corso dell'ultimo biennio hanno infine confermato l'interesse dei circuiti virtuali accelerazionisti all'acquisto o all'autoproduzione di armi da fuoco ottenute tramite stampanti 3D. Un dato che conferma l'interesse a utilizzare le nuove tecnologie non solo con finalità propagandistiche, ma anche in un'ottica più operativa.

DINAMICHE DELLA RADICALIZZAZIONE GIOVANILE

Dalle indagini condotte sul territorio nazionale nei confronti degli **ambienti accelerazionisti**, ma anche di quelli **contigui all'estremismo di matrice jihadista**, emerge una chiara **tendenza all'abbassamento dell'età dei soggetti coinvolti**. La quota dei minorenni è in costante crescita, così come è in aumento il numero di soggetti infra-quattordicenni che si posizionano anche in stadi avanzati di radicalizzazione. Tali sviluppi sono una conseguenza anche del ruolo, spesso determinante, che gioca la tecnologia nei processi di radicalizzazione giovanile. Questi ultimi, infatti, presentano, con frequenza crescente, una fase iniziale caratterizzata non dall'adesione a un'ideologia estremista, bensì

PRINCIPALI OPERAZIONI DI POLIZIA GIUDIZIARIA CON COINVOLGIMENTO DI MINORI



TREND 1

Marcato aumento del numero di operazioni di polizia giudiziaria con coinvolgimento di minori

A prescindere dalla matrice ideologica, tra il 2023 e il 2025 il numero totale di operazioni di polizia giudiziaria che coinvolgono minori passa da 7 (2023) a 14 (2024) a 27 (2025):

+285% tra il 2023 e il 2025

TREND 2

Aumento del numero di operazioni di polizia giudiziaria con coinvolgimento di minori rispetto al totale delle operazioni condotte

A prescindere dalla matrice ideologica, tra il 2023 e il 2025 aumenta in modo costante la percentuale delle operazioni di polizia giudiziaria che coinvolgono minori rispetto al totale delle operazioni condotte:

27% nel 2023
33% nel 2024
41% nel 2025

TREND 3

Per ciascun anno analizzato, la quota di minori coinvolti in operazioni di polizia giudiziaria è marcatamente più alta nei casi riconducibili all'estrema destra internazionale, rispetto a quelli riconducibili alle altre due matrici ideologiche considerate.

Nel 2023 il	**63%**	(5 su 8), contro lo 0% (0 su 18) degli estremisti islamisti e il 19% (3 su 16) dei soggetti con matrice ideologica "ibrida".
Nel 2024 il	**69%**	(18 su 26), contro il 10% (5 su 52) degli estremisti islamisti e il 38% (18 su 48) dei soggetti con matrice ideologica "ibrida".
Nel 2025 il	**77%**	(51 su 66), contro il 18% (10 su 56) degli estremisti islamisti e il 28% (11 su 39) dei soggetti con matrice ideologica "ibrida".

dalla **fascinazione per la violenza**, alimentata da una progressiva desensibilizzazione rispetto ai contenuti violenti reperibili online, fruibili su piattaforme social mainstream anche in contesti non necessariamente estremisti. L'incontro di persona con soggetti radicalizzati non è una precondizione necessaria per attivazioni aggressive, che spesso – soprattutto nell'ambito dell'estrema destra internazionale – si verificano dopo interazioni esclusivamente virtuali. Nei casi in cui emergono forme di adesione a un'ideologia, queste in realtà non appaiono particolarmente strutturate, ma strumentali a giustificare, e per certi versi legittimare, il ricorso alla violenza.

TRAIETTORIE FUTURE DELLA MINACCIA INTERNA

Sulla base delle considerazioni svolte, si possono tratteggiare alcune **possibili direttrici di sviluppo futuro della minaccia interna**:

- quanto alla **radicalizzazione giovanile**, è probabile che proseguirà la tendenziale perdita di centralità dell'ideologia come elemento cardine dei processi di radicalizzazione. A tal proposito, anche in considerazione dell'impatto che le piattaforme social possono avere sulla psicologia degli utenti più giovani, è plausibile attendersi una maggior rilevanza di quei processi di radicalizzazione in cui la ricerca di un senso di appartenenza, nonché di gratificazione e di riconoscimento da parte del gruppo, giocano un ruolo determinante. In questo quadro, è plausibile un rafforzamento della prospettiva nichilista, capace di conferire al compimento di atti violenti un'elevata intensità emotiva. Non è da escludere, quindi, la possibile attivazione - anche violenta - di soggetti radicalizzatisi in ambienti virtuali accelerazionisti, o caratterizzati da commistioni ideologiche, riconducibili a circuiti transnazionali;
- in merito alla **scena antagonista ed eversiva**, è probabile che continuerà a reagire alle attività di contrasto quali arresti e sgomberi, promuovendo mobilitazioni in chiave antirepressiva, nonché a risentire dell'andamento delle principali crisi internazionali. Tali ambienti continueranno ad adoperarsi per promuovere una convergenza tra diversi fronti di lotta, tentando di "capitalizzare" l'ampia portata mobilitativa che ha caratterizzato il sostegno alla causa palestinese. Favorire una saldatura tra la contestazione per il conflitto a Gaza e altre campagne di solidarietà internazionale, come le mobilitazioni in favore delle rivendicazioni curde, quelle a supporto delle proteste in Iran o

> *Gli ambienti accelerazionisti continuano a impiegare strategie di manipolazione degli algoritmi delle piattaforme social al fine di amplificare la diffusione della propaganda d'area*

contro l'intervento statunitense in Venezuela, verrà vista come un'opportunità per normalizzare il ricorso a forme di protesta più radicali già adottate nell'ambito del movimento ProPal.

In caso di sviluppi positivi della congiuntura internazionale, gli ambienti estremisti potrebbero comunque tentare di capitalizzare il séguito che ha avuto la mobilitazione ProPal in una prospettiva di più lungo periodo, ad esempio riconfigurando l'antimilitarismo come opposizione alle politiche di riarmo, anche rafforzando la collaborazione con omologhe reti transnazionali.

Rinnovato slancio, poi, potrebbero trovare i circuiti più attivi sul fronte ambientale, sfruttando la sovrapposizione tra grandi eventi, avvio di grandi opere e il prosieguo della transizione energetica del Paese;

- quanto, infine, all'area della **destra radicale**, pur rimasta sostanzialmente ai margini delle proteste di piazza che hanno caratterizzato il 2025, è prevedibile che proseguirà nell'impegno a ritagliarsi spazi di visibilità con il lancio di iniziative su tematiche quali il contrasto all'immigrazione. Un ambito, questo, che potrebbe alimentare una più accesa conflittualità, anche violenta, con ambienti antagonisti attivi nel sostegno ai migranti e nell'opposizione ai rimpatri. Più in generale, andrà dunque attentamente monitorato il rischio di un aumento dei livelli di conflittualità e violenza nell'ambito della dinamica di contrapposizione tra orientamenti ideologici di matrice opposta.

GRANDI EVENTI – L'ANNO GIUBILARE

L'**attività d'intelligence** durante l'**anno giubilare 2025** ha rappresentato un pilastro fondamentale per la sicurezza nazionale, concorrendo a garantire il regolare svolgimento degli eventi in un contesto geopolitico complesso. Per garantire un'adeguata cornice di sicurezza, a partire dal dicembre 2024, è stato implementato il raccordo informativo tra l'Intelligence e gli attori istituzionali esterni coinvolti a vario titolo, attraverso una **Cabina di Regia dedicata agli eventi giubilari**.

Tale modalità organizzativa è risultata particolarmente utile per gestire un evento di portata internazionale che ha visto l'afflusso nella Capitale, a partire dall'apertura della Porta Santa del 24 dicembre 2024, di più di 33 milioni di pellegrini provenienti da oltre 185 nazioni, numero superiore a quello registrato per il Giubileo del 2000, e il susseguirsi di quasi 40 "grandi eventi".

Nello specifico, per il **Giubileo dei Giovani**, particolarmente significativo per numero di pellegrini – oltre 1 milione, provenienti da 146 Paesi – e soggetti istituzionali e del mondo privato coinvolti, l'Agenzia interna ha istituito anche specifici moduli di coordinamento finalizzati a valutare mirate attività di sensibilizzazione in direzione di alcuni attori ritenuti particolarmente sensibili in tale contesto. Inoltre, sono state avviate una serie di iniziative mirate a intensificare il monitoraggio nei diversi ambiti

della ricerca informativa, che ha coinvolto in prima battuta i settori del controterrorismo e della minaccia cibernetica. In tale contesto, sono stati intensificati gli scambi con gli attori istituzionali coinvolti, tra cui le Forze di Polizia e il Sistema Informativo per la Sicurezza dello Stato del Vaticano (SISS). È stata altresì organizzata una riunione straordinaria dell'assemblea capitolina, nonché riunioni mirate del Comitato Provinciale per l'Ordine e la Sicurezza Pubblica alle quali ha partecipato personale della Comunità Intelligence.

Il meccanismo di coordinamento posto in essere ha inoltre consentito di fronteggiare **eventi di carattere straordinario con possibili ricadute significative sotto il profilo della sicurezza**: la scomparsa, il 21 aprile 2025, di Papa Francesco e le celebrazioni dei suoi funerali, con la presenza di circa 400.000 fedeli e oltre 170 delegazioni straniere; il conseguente Conclave che ha portato all'elezione di Papa Leone XIV e alla sua successiva intronizzazione avvenuta il 18 maggio, cerimonia che ha richiamato nella Capitale 156 delegazioni estere. Tale ultimo avvenimento ha visto il Sistema Paese Italia al centro di una serie di eventi eccezionali, per numero di persone e autorità nazionali e straniere coinvolte.

I profili di rischio connessi agli eventi giubilari sono stati portati all'attenzione del Comitato di Analisi Strategica Antiterrorismo/CASA, al cui interno vengono settimanalmente condivise le risultanze info-operative delle Forze di polizia e della componente Intelligence che vi partecipa. Inoltre, all'interno del **CASA** è stato istituito un **Tavolo Tecnico dedicato al Giubileo**. La sicurezza dell'evento nel dominio cibernetico è stata garantita attraverso il Comitato Analisi Strategica Cyber (CASC), dove partecipa anche personale dell'Intelligence.

Nell'ambito del monitoraggio dell'ecosistema cyber, oltre ad intensificare l'attività in direzione di eventuali narrazioni propagandistiche o campagne disinformative, durante l'intero anno giubilare sono state poste in essere attività preventive al fine di individuare precocemente eventuali minacce che potessero compromettere l'infrastruttura digitale vaticana. Particolare attenzione è stata inoltre riservata al **monitoraggio delle infrastrutture critiche** a vario titolo coinvolte negli eventi giubilari, con particolare riguardo ai settori di energia, telecomunicazioni e infrastrutture, con un focus sul settore dei trasporti e sui rischi rappresentati da un potenziale attacco cibernetico alla loro rete, ipotesi esplorata anche attraverso una delle esercitazioni per la gestione di un evento critico progettate nel corso dell'anno.

Il modello organizzativo descritto si è rivelato in grado di creare **efficaci sinergie operative**, anche interistituzionali, che hanno consentito lo **svolgimento in sicurezza dell'evento giubilare**.

6. L'EVOLUZIONE DEL FENOMENO IMMIGRATORIO IRREGOLARE

Il fenomeno dei flussi migratori irregolari, con le sue implicazioni strategiche, ha mantenuto primario interesse per il Sistema di Informazione per la Sicurezza. Nel biennio 2024-2025, il numero di migranti che hanno raggiunto le nostre coste hanno mostrato una netta contrazione, passando dal picco di 157.651 sbarcati, registrato nel 2023, ai 66.617 del 2024, sostanzialmente eguagliati dai 66.296 arrivi censiti al 31 dicembre 2025.

Nel 2025 il flusso è rimasto pressoché invariato rispetto all'anno precedente, con un lieve aumento legato soprattutto alla maggiore attività sulla rotta del Mediterraneo Centrale, in particolare dalle aree costiere della Tripolitania. Dalla Cirenaica, al contrario, le partenze verso l'Italia sono rimaste contenute, anche per via dell'aumento dei flussi osservati in direzione della Grecia, verso la quale il flusso, negli ultimi due anni, si è andato progressivamente strutturando fino a giungere a oltre 19.000 sbarchi a Creta al 31 dicembre 2025. L'intensificarsi delle partenze dalla Libia occidentale è riconducibile a un insieme di fattori: dinamiche geopolitiche, nuove misure di controllo dei confini (come l'azione di contenimento tunisina), instabilità locale e la capacità delle reti di trafficanti di spostare i percorsi verso questa zona, diventata uno dei principali punti di uscita dal Nord Africa verso l'Europa.

In tale quadro, è emerso come il progresso della tecnologia digitale rappresenti un elemento caratterizzante anche per le dinamiche

migratorie, operando sia come fattore di vulnerabilità, sia quale elemento di rafforzamento dell'azione di contrasto. Sotto il profilo delle minacce, le piattaforme digitali sono impiegate dai trafficanti per commercializzare servizi di trasporto illegale, reclutare vittime attraverso promesse fraudolente e facilitare il pagamento dei viaggi mediante transazioni su canali finanziari non tracciabili.

SITUAZIONE DEI FLUSSI MIGRATORI IRREGOLARI NEL 2025

Il fenomeno dei flussi migratori, con le sue implicazioni strategiche, resta di primario interesse per il Sistema di Informazione per la Sicurezza. Nel **biennio 2024-2025**, i **flussi** che hanno raggiunto le nostre coste hanno mostrato una **netta contrazione**, passando dal picco di 157.651 sbarcati, registrato nel 2023, ai 66.617 del 2024, sostanzialmente eguagliati dai 66.296 arrivi censiti al 31 dicembre 2025.

Nel 2025 il flusso è rimasto pressoché invariato rispetto all'anno precedente, con un lieve aumento legato soprattutto alla **maggiore attività** sulla **rotta del Mediterraneo Centrale**, in particolare dalle aree costiere della Tripolitania. Dalla Cirenaica, al contrario, le partenze verso l'Italia sono rimaste contenute, anche per via dell'aumento dei flussi osservati in direzione della Grecia, verso la quale il flusso, negli ultimi due anni, si è andato progressivamente strutturando fino a giungere a oltre 19.000 sbarchi a Creta al 31 dicembre 2025.

> *Continuerà a rafforzarsi il trend, già osservabile negli ultimi anni, che vede prevalere le migrazioni di natura economico-strutturale rispetto a quelle determinate da crisi o conflitti armati*

L'**intensificarsi** delle **partenze** dalla **Libia occidentale** è riconducibile a un insieme di **fattori**:

- dinamiche geopolitiche;
- nuove misure di controllo dei confini (come l'azione di contenimento tunisina);
- instabilità locale e capacità delle reti di trafficanti di spostare i percorsi verso questa zona, diventata uno dei principali punti di uscita dal Nord Africa verso l'Europa.

POTENZIALE EVOLUZIONE PER IL 2026

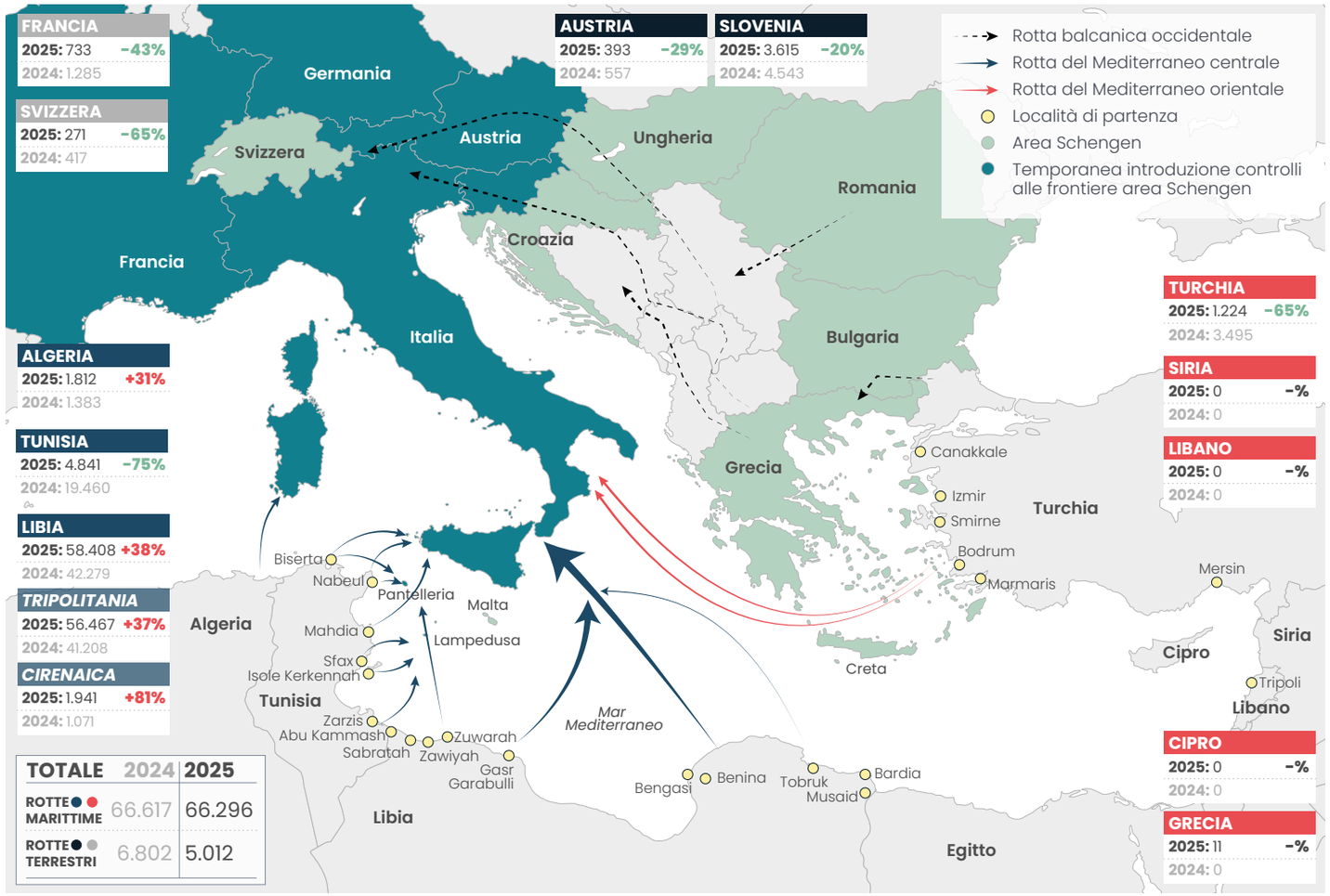
Il **fenomeno migratorio verso l'Italia nel 2026** si configura come una **realtà strutturale in evoluzione**, piuttosto che una crisi emergenziale. Le pressioni migratorie rimarranno verosimilmente significative e multidimensionali, alimentate non da eventi episodici ma da fattori cronici di fondo.

Continuerà a rafforzarsi il trend, già osservabile negli ultimi anni, che vede **prevalere** le **migrazioni di natura economico-strutturale** rispetto a quelle determinate da crisi o conflitti armati. Tale dinamica riguarda in particolare alcune delle principali nazionalità giunte in Italia nel 2025, che con alta probabilità rimarranno centrali anche nei flussi del 2026.

In particolare:

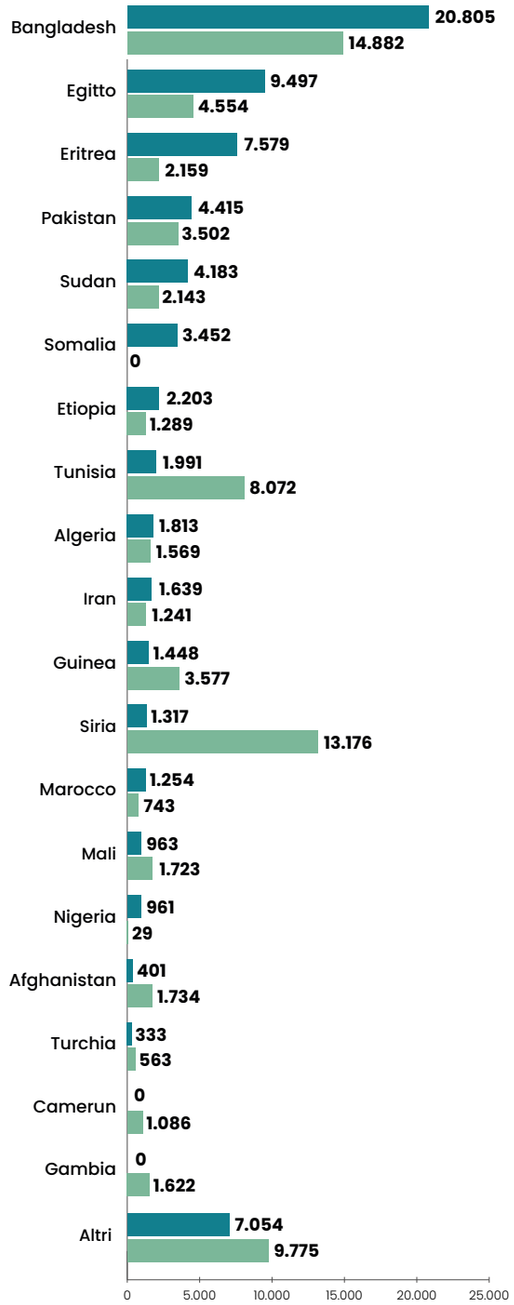
- **Bangladesh** – Si confermerà verosimilmente come la prima nazionalità in arrivo, potenzialmente pari a circa un terzo del totale, trainata da fattori strutturali combinati: inflazione elevata sui beni di base, svalutazione del taka (la valuta

LE ROTTE MIGRATORIE NEL MEDITERRANEO

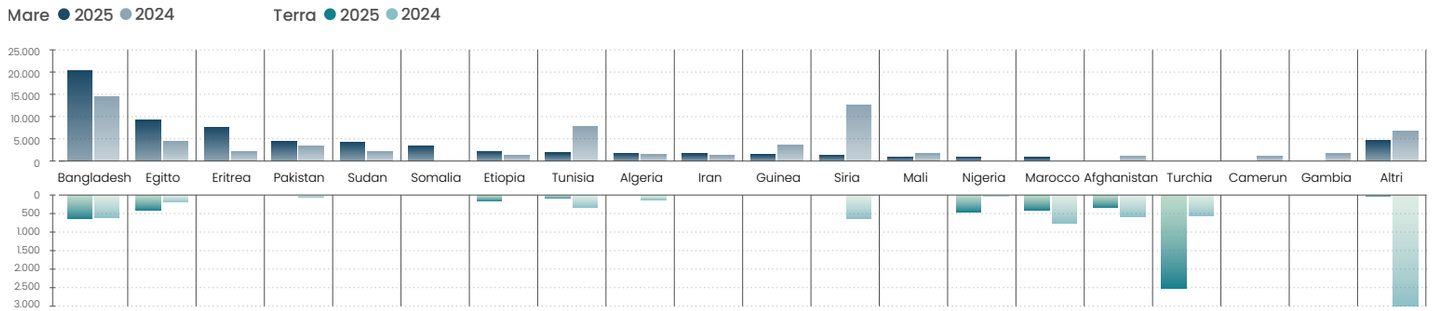


TOTALE	2024	2025
ROTTE MARITTIME	66.617	66.296
ROTTE TERRESTRI	6.802	5.012

Prime 18 nazionalità entrate in Italia (confronto 2025 2024)



Arrivi via mare e terra (confronto 2024-2025)



bengalese) che riduce il valore reale delle rimesse, impatti ricorrenti delle inondazioni monsoniche, densità demografica molto elevata e instabilità politica.

- **Egitto** – Nonostante gli accordi con l'UE, il Paese continuerà a generare flussi consistenti, in ragione di una crisi economica strutturale: inflazione molto alta, forte svalutazione della valuta, riduzione delle riserve valutarie e mercato del lavoro incapace di assorbire la crescente forza lavoro giovanile. A ciò si aggiunge la cronica scarsità idrica nel bacino del Nilo, che indebolisce la produttività agricola e alimenta mobilità interna ed esterna.
- **Pakistan** – I flussi potrebbero aumentare moderatamente (+10-15%), spinti da inflazione persistente, elevata disoccupazione e sottooccupazione giovanile, crisi energetica reiterata e volatilità politica, elementi che alimentano la propensione migratoria soprattutto tra le fasce più giovani.
- **Eritrea e Sudan** - anche per l'anno in corso i flussi relativi a queste due nazionalità si confermeranno, presumibilmente, in termini numerici analoghi al 2025, a causa delle condizioni economiche e di sicurezza che affliggono entrambi i Paesi.

Nel complesso, tali dinamiche mostrano, e confermano, una **graduale trasformazione qualitativa del fenomeno migratorio**: giovani adulti che si muovono principalmente per pressioni economiche profonde, spesso aggravate da fattori ambientali e climatici. Questo rende i flussi più prevedibili e più costanti, ma anche più difficili da interrompere con strumenti di deterrenza.

Altri Paesi, parimenti attesi nei flussi, ma interessati da conflitti – come Sudan, Somalia, Iran e Yemen – mostrano un tipo di migrazione alimentata da crisi sovrapposte: guerre interne, carestie, siccità severe, deterioramento dei servizi essenziali e progressivo crollo delle istituzioni. Una combinazione di fattori che innescano percorsi migratori che non si risolvono con soluzioni unidimensionali. Nel 2026 queste **"crisi ibride"** rappresenteranno una **parte consistente del flusso migratorio che interesseranno l'Italia e l'Europa**.

In questa prospettiva, la **Libia** continuerà a rappresentare il fulcro – fragile – del sistema migratorio, e la rotta del Mediterraneo centrale, alimentata quasi totalmente dalle partenze dalle coste libiche, rimarrà con molte probabilità predominante per ragioni geografiche irriducibili: più breve, meno rischiosa delle rotte attraverso il Sahara, logisticamente consolidata da parte dei trafficanti. La **rotta algerina**, sebbene minoritaria, potrebbe rappresentare sempre più una via emergente di fuga dai controlli più stringenti, segnalando una realtà di adattamento costante dei network di traffico. La **rotta balcanica**, pur apparendo in tendenziale declino strutturale, rimarrà fortemente legata alla stabilità del quadrante mediorientale: un conflitto in quell'area potrebbe invertire rapidamente il trend al rialzo.

Il **fattore climatico** acquista importanza crescente: le inondazioni e siccità periodiche più che eventi

eccezionali, vanno ascritti alla normalità ricorrente, che incentiva l'emigrazione come necessità di adattamento familiare.

L'**azione crescente delle autorità e il rafforzamento dei controlli lungo le frontiere** stanno esercitando una pressione costante sulle reti criminali. Queste, sebbene abbiano tentato di adattarsi ai cambiamenti imposti, sono state efficacemente contrastate grazie alla costante ed incisiva azione svolta. In tal senso, gli sforzi profusi hanno permesso nel corso dell'ultimo biennio una considerevole riduzione degli arrivi di migranti sul territorio nazionale e conseguentemente garantito, da un lato, un'opera di fidelizzazione delle forze di sicurezza dei principali Paesi di partenza e, dall'altro, un aumento della stabilità delle aree interessate dal fenomeno criminale.

L'azione di contrasto sulle rotte più consolidate e l'innalzamento delle soglie di sorveglianza costringeranno i sodalizi criminali a riorganizzarsi, deviare i percorsi e rivedere i propri metodi, con un aumento dei costi operativi e una riduzione dei margini di manovra. In questo quadro, la necessità per i trafficanti di adattarsi continuamente rappresenta al tempo stesso un indicatore dell'efficacia del contrasto e la ragione per cui restano indispensabili ulteriori sforzi investigativi e di cooperazione internazionale.

Inoltre, anche le **politiche di esternalizzazione delle frontiere** (accordi Italia-Tunisia, Italia-Libia, finanziamenti UE) **hanno contribuito a produrre effetti misurabili nella riduzione dei flussi dal 2023**. Tale successo è stato consolidato costantemente dall'attività diplomatica, dall'operato dell'intelligence, dal mantenimento del sostegno finanziario, nonchè dalla stabilità politica dei Paesi partner – in primis Tunisia e Libia – che presentano fragilità intrinseche.

> *Lo scenario più probabile per il 2026 è quello di flussi stabili ma di discreta consistenza, ossia un sistema migratorio che tenderà alla normalizzazione di lungo periodo*

Alla luce di tutto questo, lo **scenario più probabile per il 2026** è quello di **flussi stabili ma di discreta consistenza**: un sistema migratorio che tenderà alla normalizzazione di lungo periodo. Non si prevede né un collasso né un'esplosione improvvisa, piuttosto un consolidamento dei livelli attuali, con una pressione costante destinata a mantenersi negli anni. Il 2026 sarà inoltre un anno di prova cruciale per la sostenibilità del modello europeo di esternalizzazione. Se il nuovo **Patto sulla migrazione e l'asilo dell'Unione europea** – la cui entrata in vigore è prevista per giugno – andrà rapidamente a regime in modo armonico nei diversi Stati membri, nei primi mesi di attuazione gli arrivi potrebbero ridursi del 4–5% del flusso totale annuale.

L'impatto, che nel medio periodo si stima significativo, rappresentando un cambio di passo della strategia europea di contrasto ai flussi irregolari,

> *Il progresso della tecnologia digitale rappresenta un elemento che caratterizza anche la dinamica migratoria contemporanea, operando sia come fattore di vulnerabilità, sia quale elemento di rafforzamento dell'azione di contrasto*

apparirà inizialmente limitato perché le nuove regole decorreranno solo dopo il primo semestre, rendendo quindi evidenti gli effetti non prima degli ultimi mesi del 2026.

Al contrario, qualora si presentassero crisi geopolitiche inattese (escalation Sudan, crescente instabilità in Libia), i volumi potrebbero aumentare del 10%÷15%. La **strategia** in atto di **"gestione per contenimento"** mediante una politica di accordi con i Paesi esterni alla UE interessati dai flussi sta mostrando **effetti positivi**, ma resta vulnerabile a repentini mutamenti geopolitici che potrebbero comprometterne l'inefficacia. Per controbilanciare ciò, nel lungo periodo resta vitale **continuare con piani strutturali di investimento** – come il **Piano Mattei** – nei Paesi esposti maggiormente al fenomeno della migrazione economica; e, nel medio periodo, **proseguire politiche volte a favorire i canali di immigrazione legale**, eventualmente formando nei Paesi di origine la manodopera necessaria al mercato italiano ed europeo.

Lo **smantellamento** delle **organizzazioni criminali dedite al traffico di esseri umani** rimane comunque un obiettivo di primaria importanza per anemizzare la "piattaforma logistica" che rende possibile l'esistenza, la sopravvivenza e il replicarsi delle lunghe filiere che dall'Asia e dall'Africa subsahariana giungono fino alle coste occidentali della Libia.

IL FENOMENO MIGRATORIO, TRA MINACCIA IBRIDA E DIMENSIONE TECNOLOGICA

Il **progresso della tecnologia digitale** rappresenta un elemento che caratterizza anche la dinamica migratoria contemporanea, operando **sia come fattore di vulnerabilità, sia quale elemento di rafforzamento dell'azione di contrasto**.

Sotto il profilo delle minacce, le piattaforme digitali—social media, app di messaggistica, sistemi elettronici di pagamento, criptovalute—sono impiegate dai trafficanti per commercializzare servizi di trasporto illegale, reclutare vittime attraverso promesse fraudolente e facilitare il pagamento dei viaggi mediante transazioni su canali finanziari non tracciabili. Tale modalità ha assunto una dimensione autonoma definita "e-trafficking" (o "cyber trafficking").

Parallelamente, negli ultimi anni, il **fenomeno migratorio** ha subito una profonda **trasformazione** che lo avvicina progressivamente alle **minacce non convenzionali**. In questa dimensione, attori ostili—statuali e non statuali—possono strumentalizzare

i flussi migratori irregolari quale leva di coercizione geopolitica nei confronti di altri Stati, conducendo operazioni di minaccia ibrida articolate su molteplici livelli. Tali operazioni si dispiegano tanto sul piano cognitivo, attraverso la diffusione di narrazioni disinformative sulla migrazione, l'amplificazione artificiale di contenuti destabilizzanti tramite bot e l'interferenza sulla pubblica opinione, al fine di erodere la coesione sociale e compromettere la fiducia nelle istituzioni democratiche, quanto su quello materiale, mediante l'uso della migrazione quale strumento di pressione strutturale finalizzato a provocare tensioni sociali, crisi umanitarie controllate e deterioramento della capacità amministrativa degli Stati bersaglio. In questo contesto, la migrazione irregolare si configura come minaccia ibrida che combina elementi materiali e vettori cognitivi.

D'altro canto, **in chiave di prevenzione e contrasto**, l'**Unione europea** ha implementato un'**architettura tecnologica integrata** fondata sull'**acquisizione sistematica di dati biometrici multimodali**—immagini facciali, impronte digitali, analisi posturale. L'Entry-Exit System (EES) registra automaticamente i cittadini extracomunitari ai varchi frontalieri, prevenendo il fenomeno dell'immigration shopping. Tale sistema si integrerà con la banca dati per la gestione dell'asilo e della migrazione (EURODAC) e con il sistema europeo di informazione e autorizzazione ai viaggi (ETIAS), che sfruttano dati biometrici e algoritmi predittivi per applicare screening preventivi sulla base di nazionalità e dati contestuali.

Algoritmi specializzati amplieranno la capacità di valutazione comportamentale del rischio e l'interoperabilità progressiva tra database biometrici consentirà verifiche simultanee su archivi continentali, accelerando i processi di identificazione. Nel **monitoraggio delle frontiere esterne**, l'Unione europea impiega sistematicamente **droni** (RPAS) attraverso Frontex e, in ambito marittimo, tramite i servizi di EMSA, al fine di aumentare la situational awareness operativa, supportare ricerca e soccorso, individuare imbarcazioni sospette e condividere informazioni in tempo reale con le autorità competenti. Queste piattaforme aeree senza equipaggio si integrano con sensori termici e immagini satellitari ad alta definizione, componendo un dispositivo integrato di vigilanza continua sui confini.

Queste evoluzioni qualitative nelle capacità analitiche e di monitoraggio rappresentano quindi un obiettivo strategico che tende alla sostituzione graduale dei tradizionali meccanismi di raccolta informativa con architetture informatiche automatizzate operanti su scala continentale, con ricadute significative nel contrasto ai flussi migratori irregolari.

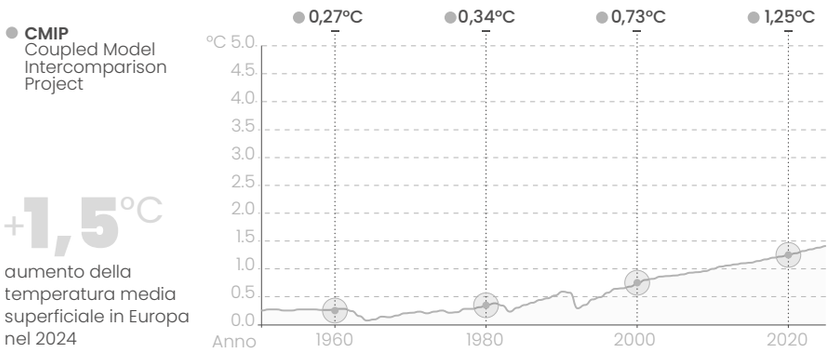
LA DASHBOARD
DEGLI INDICATORI STRATEGICI

4

CLIMA

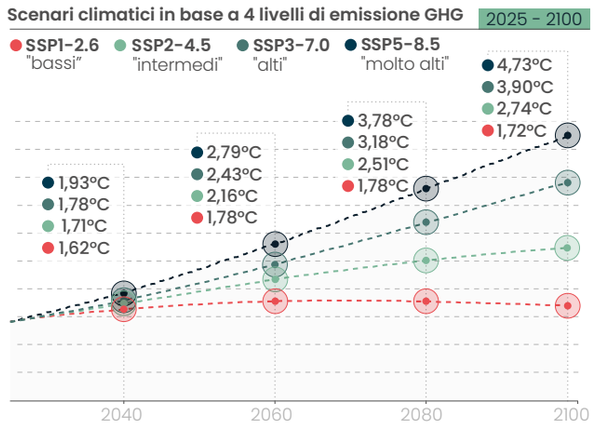
Anomalie della temperatura media superficiale terrestre

(rispetto alla media 1850-1900)



+1,5°C

aumento della temperatura media superficiale in Europa nel 2024

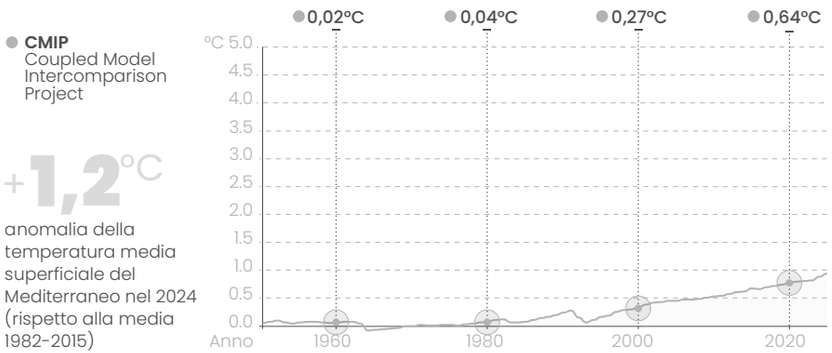


Anomalie della temperatura media superficiale terrestre

La temperatura dell'aria è una delle principali variabili, nella fisica dell'atmosfera, responsabili dei cambiamenti climatici. La sua misurazione, rispetto alla media del periodo pre-industriale (1850-1990), mostra non solo una tendenza crescente, ma anche una accelerazione del suo innalzamento dalla seconda metà degli anni Novanta.
Gli scenari climatici dei prossimi decenni dipendono dai livelli di emissione dei gas serra. Se vengono mantenuti "bassi" (scenario di sviluppo socio-economico denominato SSP1-2.6), l'anomalia termica rispetto alla media pre-industriale potrà mantenersi al disotto della soglia 1,8°C; in caso contrario il riscaldamento globale potrà avere nel futuro impatti e costi rilevanti in termini economici, sociali, e sanitari.

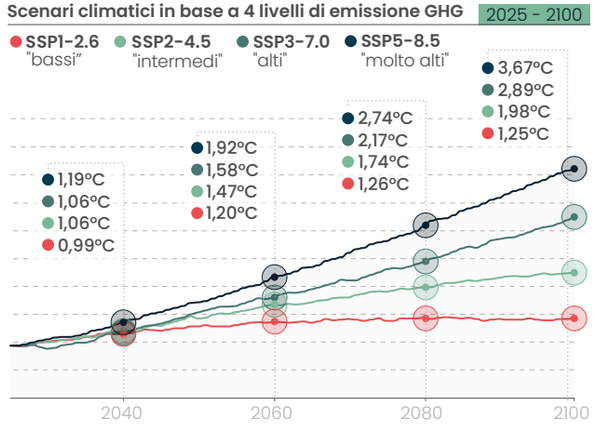
Anomalie della temperatura media superficiale degli oceani

(rispetto alla media 1850-1900)



+1,2°C

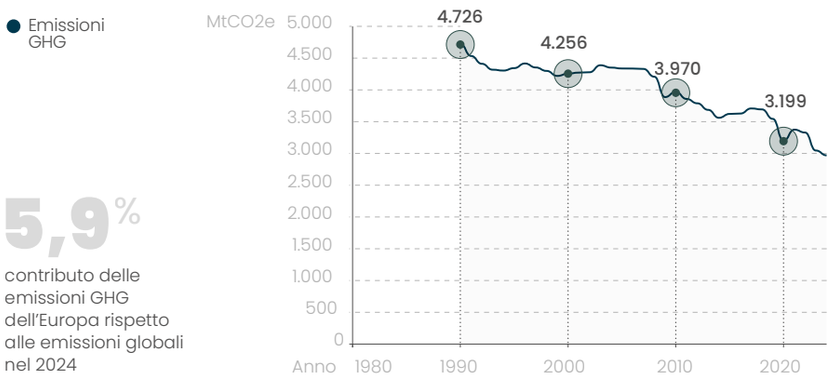
anomalia della temperatura media superficiale del Mediterraneo nel 2024 (rispetto alla media 1982-2015)



Anomalie della temperatura media superficiale degli oceani

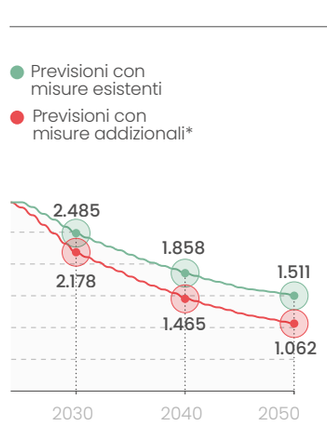
Altrettanto rilevanti per gli equilibri degli ecosistemi sono le anomalie della temperatura media superficiale del mare che, analogamente alla temperatura superficiale terrestre, costituiscono i principali parametri di riferimento per "misurare" il riscaldamento globale.
Anche in questo caso, l'assenza di efficaci misure mitiganti le emissioni globali di gas serra possono prefigurare scenari climatici nei quali gli oceani diventano sempre più serbatoi di enormi quantità di energia, con conseguenze per quanto riguarda la frequenza di eventi meteorologici estremi e l'innalzamento del livello del mare.

Emissioni dei gas serra nei Paesi UE



5,9%

contributo delle emissioni GHG dell'Europa rispetto alle emissioni globali nel 2024



2,8%

contributo delle emissioni GHG dell'Europa rispetto alle emissioni globali nel 2040

**Le misure addizionali si riferiscono al pacchetto per la neutralità climatica "Fit for 55" della Commissione europea (2021)*

Emissioni dei gas serra nei Paesi UE

Le politiche comunitarie sul "green deal" hanno contribuito alla riduzione delle emissioni dei gas serra da parte dei Paesi europei. Nel 2024 le emissioni GHG dell'Unione Europea hanno rappresentato il 5,9% delle emissioni globali.
In uno scenario privo di ulteriori misure mitiganti, il contributo europeo alle emissioni globali nel 2040 si collocano tra il 2,8% e il 3% delle emissioni globali.
Il dato rilevante consiste nel fatto che, nonostante gli sforzi europei, le emissioni di gas serra aumentano nel mondo: dai circa 56,2 GT (CO_2 equivalente) del 2020, in assenza di ulteriori misure contenitive le proiezioni portano i livelli di emissione nel 2050 oltre i 67 GT (CO_2 equivalente).

7. CRISI INTERNAZIONALI E MINACCIA TERRORISTICA

Negli ultimi anni, il panorama della minaccia terroristica ha assunto una dimensione sempre più complessa. Rilevano, nel senso, le molteplici crisi internazionali in atto, caratterizzate da conflitti armati e dinamiche geopolitiche in costante evoluzione, che facilitano il sovrapporsi di diversi fattori di radicalizzazione.
Con riferimento alla crisi di Gaza, nel 2025 sono stati registrati numerosi appelli – veicolati tramite la propaganda jihadista – a condurre attacchi in Europa, specialmente contro quartieri ebraici e ambasciate "ebraiche e crociate".
In Italia, come in altri Paesi europei, sono state condotte diverse operazioni antiterrorismo nei confronti di soggetti a vario titolo connessi con il conflitto mediorientale. Sono inoltre aumentati i rischi derivanti dalle attività di Hamas su suolo europeo, soprattutto per il coinvolgimento nella circolazione di armi e in possibili progettualità ostili contro obiettivi israeliani ed ebraici.
In Iran, la guerra dei dodici giorni del giugno scorso e le proteste scoppiate nel Paese a fine dicembre 2025 hanno aggiunto ulteriore complessità allo scenario mediorientale, alimentando tensioni internazionali e facendo temere un'escalation che potrebbe avere un impatto anche sulla minaccia terroristica.
Quanto alla Siria, dalla caduta di Assad il Paese si trova in una fase di transizione caratterizzata da tensioni e incertezze. Un'instabilità che rafforza il rischio terrorismo nell'area, come testimoniato dall'attacco compiuto nel dicembre 2025 da un miliziano di DAESH infiltratosi nelle

forze di sicurezza siriane. In tale ambito, un'attenzione particolare continua a essere rivolta alla gestione dei foreign terrorist fighters ancora presenti nelle carceri siriane e nei campi nel nord est del Paese.

La "crisi sistemica" che affligge il continente africano ha costituito anch'essa, nel corso del 2025, un terreno fertile per l'espansione delle articolazioni territoriali di DAESH e al-Qaida. Gli assetti europei e nazionali presenti nell'area continuano dunque a essere esposti a possibili azioni ostili. La propaganda di DAESH ha recentemente iniziato a concentrarsi maggiormente anche sulla Libia, considerata quale "porta d'accesso" per raggiungere l'Europa meridionale e intraprendere il jihad contro i "vicini interessi crociati".

In relazione al quadrante afghano, infine, ISKP, pur recentemente indebolita da diverse operazioni di controterrorismo, resta un'organizzazione in grado di raggiungere simpatizzanti e affiliati anche in altri Paesi, e ha confermato le sue spiccate aspirazioni transnazionali, continuando a rappresentare una fonte di rischi anche per l'Europa.

Nel contesto delineato, il ricorso alle nuove tecnologie da parte di individui e gruppi estremisti e terroristici ha reso il quadro della minaccia ancora più articolato. L'uso di chatbot, potenziati dall'IA per indirizzare gli utenti nella ricerca di contenuti terroristici, nonché il ricorso ad "assistenti virtuali" per individuare i luoghi più adatti per compiere un attacco, rappresentano solo alcuni esempi di come tale tecnologia sia stata utilizzata a scopo di minaccia.

Negli ultimi anni, il panorama della **minaccia terroristica** ha assunto una **dimensione sempre più complessa**. Le molteplici crisi internazionali in atto, caratterizzate da conflitti armati e dinamiche geopolitiche in costante evoluzione, facilitano il sovrapporsi di **diversi fattori di radicalizzazione**. Nei momenti di maggiore instabilità globale, infatti, si amplificano e si intrecciano problematiche di tipo politico, sociale, economico e identitario che incidono sulle vulnerabilità individuali e collettive, alimentando interpretazioni estremiste della realtà. In un contesto di questo tipo, i giovani risultano particolarmente esposti a narrazioni che istigano alla violenza.

La **propaganda terroristica**, che nel 2025 ha registrato un **aumento** rispetto all'anno precedente quanto alla diffusione di contenuti jihadisti, continua a dimostrarsi efficace nello sfruttare il protrarsi delle tensioni connesse ai teatri di crisi e nell'intercettare le predette vulnerabilità.

I PRINCIPALI TEATRI DI CRISI

La **crisi di Gaza**, l'instabilità del contesto iraniano, le fragilità del teatro siriano, l'espansione di gruppi terroristici sia nel continente africano sia nel quadrante afghano hanno già avuto, ciascuna con diversi livelli d'intensità, un impatto sul livello della minaccia terroristica.

Con riferimento alla crisi di Gaza, nel 2025 sono stati numerosi gli appelli veicolati tramite la propaganda jihadista a condurre attacchi in Europa,

> *Le molteplici crisi internazionali in atto, caratterizzate da conflitti armati e dinamiche geopolitiche in costante evoluzione, facilitano il sovrapporsi di diversi fattori di radicalizzazione*

specialmente contro quartieri ebraici e ambasciate "ebraiche e crociate". L'attacco alla sinagoga di Heaton Park a Manchester (che ha causato due morti) e la sparatoria contro la comunità ebraica australiana a Bondi Beach (che ha causato quindici morti) costituiscono esempi particolarmente violenti di attacchi terroristici con una chiara matrice antisemita compiuti nel corso del 2025. **In Italia, come in altri Paesi europei** quali Germania, Austria, Svezia e Regno Unito, sono state condotte **diverse operazioni antiterrorismo** nei confronti di soggetti a vario titolo connessi con il conflitto mediorientale. Sono inoltre **aumentati i rischi derivanti dalle attività di Hamas su suolo europeo**, soprattutto per il coinvolgimento nella circolazione di armi e in possibili progettualità ostili contro obiettivi israeliani ed ebraici.

In **Iran**, la guerra dei dodici giorni del giugno scorso e le proteste scoppiate nel Paese a fine dicembre 2025 hanno aggiunto ulteriore complessità allo scenario mediorientale, alimentando tensioni internazionali e facendo temere un'escalation che può avere un impatto anche sulla minaccia terroristica.

Quanto alla **Siria**, dalla caduta di Assad il Paese

si trova in una fase di transizione caratterizzata da tensioni e incertezze. Un'instabilità che rafforza il rischio terrorismo nell'area, come testimoniato dall'attacco compiuto nel dicembre 2025 da un miliziano di DAESH infiltratosi nelle forze di sicurezza siriane, che ha colpito un pattugliamento congiunto siro americano provocando la morte di tre cittadini americani (due militari e un civile). Un'attenzione particolare continua inoltre a essere rivolta alla gestione dei foreign terrorist fighters ancora presenti nelle carceri siriane e nei campi nel nord est del Paese.

La "crisi sistemica" che affligge il **continente africano** costituisce ancora un terreno fertile per l'espansione delle articolazioni territoriali di DAESH e al-Qaida, ed espone gli assetti europei e nazionali presenti nell'area a possibili azioni ostili. La propaganda di DAESH ha recentemente iniziato a concentrarsi maggiormente anche sulla Libia, considerata quale "porta d'accesso" per raggiungere l'Europa meridionale e intraprendere il jihad contro i "vicini interessi crociati".

In relazione al **quadrante afghano**, infine, questo continua a rappresentare il principale safe haven per numerosi gruppi jihadisti nazionali e transnazionali. In tale contesto, l'Islamic State Khorasan Province (ISKP) – pur recentemente indebolita da diverse operazioni di controterrorismo – mantiene una diffusa presenza soprattutto nel Nord-Est del Paese e nella fascia confinaria afghano-pakistana. L'organizzazione ha già dimostrato di poter operare anche al di fuori dell'Afghanistan e continua a rappresentare una fonte di rischi anche per l'Europa. Un'ulteriore minaccia proveniente dall'Afghanistan è rappresentata da Al-Qa'ida (AQ) e dalla sua branca regionale Al-Qa'ida in the Indian Subcontinent (AQIS). Entrambe le formazioni hanno infatti intensificato le attività di propaganda e addestramento condotte sul territorio, in direzione anche di giovani studenti.

INTELLIGENZA ARTIFICIALE E RISCHIO TERRORISMO

In un quadro della minaccia come quello sopra descritto, si innesta un ulteriore fattore: il **ricorso** alle **nuove tecnologie da parte di individui e gruppi estremisti e terroristici**. Sono sempre maggiori, infatti, le evidenze circa il crescente utilizzo delle funzionalità offerte dalle innovazioni tecnologiche e, in particolare, dall'Intelligenza Artificiale (IA).

Si pensi, ad esempio, all'ormai consolidato uso online di chatbot, potenziati dall'IA, in grado di indirizzare gli utenti nella ricerca di contenuti terroristici, inclusi quelli che veicolano istruzioni per l'auto-addestramento e il confezionamento di ordigni esplosivi. Una tendenza riscontrata anche in Italia, dove sono emersi casi di soggetti minorenni che effettuavano – tramite motori di ricerca basati sull'intelligenza artificiale – ricerche online per costruire ordigni rudimentali.

Un'ulteriore funzionalità è il ricorso ad "assistenti virtuali" per individuare il luogo più adatto per il

compimento di un attacco. Tra gli esempi più recenti, quello di un giovane di diciotto anni, ideologicamente legato a DAESH, arrestato dalle Autorità svedesi nel mese di agosto 2025 mentre pianificava un attacco terroristico da condurre al Festival della Cultura di Stoccolma, target selezionato appunto attraverso l'interrogazione di un chatbot.

> *Questo tipo di interazione tra attore solitario e intelligenza artificiale, che in alcuni casi consente di guidare un soggetto in un percorso automatizzato di radicalizzazione può avvenire senza soluzione di continuità, 24 ore su 24*

Questo tipo di **interazione tra attore solitario e intelligenza artificiale**, che in alcuni casi consente di guidare un soggetto in un percorso automatizzato di radicalizzazione senza la necessità di un reclutatore umano, costituisce una sfida importante per il contrasto alla minaccia, in quanto l'attività automatizzata può avvenire senza soluzione di continuità, 24 ore su 24.

Restando nell'ambito del reclutamento a fini terroristici, l'**IA** è altresì in grado di **generare automaticamente e in tempi rapidissimi materiale** grafico, testuale, audio e video di **propaganda estremista** di elevata qualità. Tali contenuti, inclusi deep-fake sempre più realistici, possono essere prodotti o tradotti in diverse lingue, nonché essere adattati a contesti religiosi, culturali e geografici differenti. Parallelamente, attraverso **tecniche di profilazione**, la stessa tecnologia consente di analizzare enormi quantità di dati presenti online (sui social media, sui forum di discussione, sulle piattaforme di gaming online, sul dark web, ecc.) per individuare i soggetti che sono potenzialmente più ricettivi al reclutamento. Una volta individuati, gli algoritmi di intelligenza artificiale possono adattare le risposte che forniscono durante l'interazione con il singolo utente in base alle sue reazioni. La tradizionale propaganda estremista online si converte, dunque, in una **"propaganda adattiva"**, che accresce progressivamente – un click dopo l'altro – la sua capacità persuasiva. Si produce, così, una **duplice accelerazione del rischio**: da un lato, le campagne mediatiche diventano più rapide e più numerose; dall'altro, la creazione di contenuti "su misura", la selezione dei target più vulnerabili e la capacità dell'algoritmo, durante la conversazione con l'utente, di adattarsi a quest'ultimo, consentono di aumentare sensibilmente le chance di successo di un'attività di reclutamento.

Andando al di là dell'ambito del reclutamento, anche l'intersezione tra **intelligenza artificiale e finanziamento al terrorismo** pone sfide crescenti per la sicurezza. Gli algoritmi generativi, ad esempio, permettono a gruppi estremisti di orchestrare ad arte campagne di fundraising legate a falsi progetti umanitari, nel corso delle quali le donazioni raccolte

vengono dirottate verso organizzazioni terroristiche. Le **funzionalità introdotte dall'IA** possono infine essere sfruttate anche **per la pianificazione ed esecuzione di attacchi terroristici**. In tale contesto, l'IA può facilitare l'individuazione degli obiettivi più vulnerabili, sia nel mondo fisico sia in quello digitale, nonché la scelta del momento più opportuno per colpire e delle armi più idonee per massimizzare l'impatto dell'attacco, anche in termini di numero di vittime. Quanto all'utilizzo in fase esecutiva, i gruppi terroristici, ad esempio, hanno già impiegato droni per condurre attività di ricognizione e attacchi mirati; l'integrazione dell'IA aumenta la precisione e la letalità di tali velivoli, soprattutto quando operano in sciami. L'uso dell'IA per l'esecuzione di un attacco potrebbe inoltre riguardare anche lo sviluppo di analisi predittive per anticipare la risposta delle forze di sicurezza, attraverso la simulazione di scenari che possano adeguarsi, anche in tempo reale, a sempre nuove informazioni.

TABELLA 1. IA E RISCHIO TERRORISMO

FUNZIONE IA	MECCANISMO	IMPATTO SUL RISCHIO TERRORISMO
Generazione automatica di propaganda	• Creazione di testi, audio, video, deepfake in più lingue; • Adattamento a contesti religiosi, culturali e geografici; • Radicalizzazione automatizzata tramite chatbot che operano senza soluzione di continuità.	• Aumenta la quantità e la qualità della propaganda; • Aumenta la velocità di produzione e diffusione.
Profilazione e targeting	• Analisi massiva di dati provenienti da social media, forum, piattaforme di gaming e dark web.	• Individuazione dei soggetti più vulnerabili e ricettivi alle narrazioni estremiste.
Propaganda adattiva	• Gli algoritmi adattano i contenuti propagandistici in base alle reazioni dell'utente.	• Aumentano le probabilità di successo del reclutamento.
Finanziamento al terrorismo	• Campagne di fundraising legate a falsi progetti umanitari per dirottare le donazioni.	• Aumento dei flussi e difficile tracciabilità dei finanziamenti al terrorismo.
Pianificazione operativa	• Simulazione predittiva di scenari d'attacco; • Identificazione di obiettivi da colpire; • Scelta del timing dell'attacco e delle armi da usare.	• Ottimizzazione della pianificazione di un attacco; • Aumento delle probabilità di successo.
Esecuzione operativa	• Utilizzo di droni coordinati in sciami e di auto a guida autonoma supportati dall'IA.	• Aumento della letalità degli attacchi; • Ulteriore potenziamento degli attacchi "da remoto".

L'IA NELLA NARRAZIONE JIHADISTA

Nel corso del 2025, diverse case mediatiche legate a DAESH hanno trattato la tematica dell'IA, concentrandosi sui profili relativi alla generazione e traduzione di contenuti, nonché alla diffusione di manualistica per un utilizzo corretto e sicuro di tale tecnologia. Il tema della sicurezza informatica, in quanto oggetto d'interesse da parte di un ampio pubblico, sembra dunque essere stato sfruttato per tentare di attrarre nuovi follower, fornendo al contempo una sorta di "linee guida" sull'utilizzo dell'intelligenza artificiale; un utilizzo presentato, in alcuni casi, persino come un obbligo individuale e "religioso", per difendersi dalle minacce poste dall'IA per mano dei cosiddetti nemici dell'Islam.

L'IA NEL CONTRASTO AL TERRORISMO

Le stesse caratteristiche che rendono l**'IA** un possibile acceleratore della minaccia, possono essere utilizzate per **potenziare le attività di prevenzione e contrasto della radicalizzazione e del terrorismo**. Si pensi, ad esempio, agli **strumenti** impiegati per **individuare contenuti estremisti online ai fini della loro rimozione**, spesso basati su sistemi di riconoscimento linguistico potenziati dall'IA. Analogamente, l'**analisi dei social network** effettuata attraverso gli strumenti dell'intelligenza artificiale permette oggi di cogliere, in tempi molto più rapidi rispetto al passato, le relazioni esistenti tra soggetti radicalizzati, facilitando l'identificazione di membri, ruoli e gerarchie interne ai gruppi, nonché la comprensione dei flussi informativi tra tali soggetti. Nei predetti contesti, i **sistemi online volti a re-indirizzare gli utenti da contenuti estremisti verso testi di contro-narrazione** rappresentano una dimensione proattiva della prevenzione della radicalizzazione ormai sempre più trainata dall'IA.

Tra le attività di prevenzione che fanno ricorso all'intelligenza artificiale, è da menzionare anche l'utilizzo di **chatbot nei confronti di soggetti ad alto rischio di radicalizzazione**, al fine di proporre loro testimonianze di individui de-radicalizzati, o metterli in contatto con reti di supporto psicologico. Attraverso l'analisi incrociata di grandi bacini di dati, l'IA può essere inoltre usata per **supportare le previsioni sui possibili target della minaccia, nonché sui periodi e i luoghi** in cui la **probabilità** che si verifichino **attacchi** risulti più **elevata**. Ciò contribuisce a creare una scala di priorità delle minacce, ottimizzare l'allocazione delle risorse e potenziare le misure di protezione.

Questi strumenti sfruttano dunque gli stessi meccanismi di amplificazione algoritmica alla base delle strategie di reclutamento terroristico online, utilizzando l'intelligenza artificiale non come vettore di radicalizzazione, ma appunto come strumento di prevenzione e contrasto.

Quanto alla dimensione offline, sistemi basati sull'IA, incorporando il riconoscimento facciale e le reti di sensori, stanno migliorando sensibilmente la capacità di rilevare attività sospette e rispondere a

TABELLA 2. IA E CONTRASTO AL TERRORISMO

ESEMPI DI APPLICAZIONE DELL'IA	OPPORTUNITÀ OPERATIVE
Rilevamento e rimozione automatica di contenuti estremisti online	• Scansione su grande scala; • Eliminazione in tempo reale; • Riduzione della capacità di reclutamento e istigazione all'azione violenta.
Analisi delle reti sociali	• Mappatura dei legami tra soggetti radicalizzati che rappresentano una minaccia; • Identificazione di ruoli, gerarchie e flussi informativi.
Re-indirizzamento verso contro-narrazioni	• Intervento proattivo di prevenzione della radicalizzazione.
Utilizzo di chatbot	• Supporto a soggetti ad alto rischio di radicalizzazione; • Instradamento verso servizi di supporto psicologico.
Previsione di target, tempi e luoghi di attacchi	• Generazione di indici di rischio; • Pianificazione preventiva di misure di protezione; • Ottimizzazione nell'allocazione di personale e mezzi.
Analisi di feed video ad alta risoluzione in tempo reale	• Rilevamento rapido di eventi anomali e attività sospette.
Reti di sensori acustici urbani	• Allerta precoce in caso di eventi sonori anomali.
Supporto all'analista che si occupa di terrorismo	• Ausilio anche nelle attività di analisi previsionale.

L'IMPIEGO DELL'IA NELLE STRATEGIE DI SICUREZZA PRESENTA ALCUNE SFIDE DI NATURA ETICA, TECNICA E NORMATIVA.

Sul piano etico, il ricorso all'IA deve confrontarsi con la necessità di non ledere i diritti fondamentali degli individui, inclusa la privacy, evitando – al contempo – che un "addestramento" improprio dei suoi modelli possa produrre effetti discriminatori, ad esempio, su alcuni gruppi sociali.

Dal punto di vista tecnico, l'IA mostra ancora dei limiti nell'operare in contesti tematici e linguistici diversi tra loro. Parallelamente, soggetti ostili e gruppi terroristici stanno accrescendo le loro capacità di eludere i sistemi di monitoraggio basati sull'intelligenza artificiale.

Quanto, infine, all'aspetto normativo, la mancanza di un quadro regolatorio armonizzato a livello internazionale ostacola l'efficacia delle iniziative di contrasto a un uso improprio dell'IA, generando disallineamenti legislativi facilmente sfruttabili per fini illeciti, ostacolando la cooperazione transnazionale.

situazioni di emergenza, incluse quelle legate ad attività terroristiche. L'utilizzo di **sistemi di videosorveglianza avanzati**, capaci di analizzare in tempo reale feed video ad alta risoluzione per rilevare eventi anomali e attività sospette, è già una realtà in diversi Paesi. Analogamente, **sistemi basati su reti di sensori acustici nelle aree urbane** permettono di rilevare e localizzare anomalie, come quelle prodotte da colpi di arma da fuoco.

Infine l'IA, opportunamente guidata dall'operatore umano, può fornire **supporto agli analisti** che si occupano di minaccia terroristica, incluso nelle attività di analisi previsionale.

SCENARI DI EVOLUZIONE DEL TERRORISMO INTERNAZIONALE

Le **crisi internazionali** producono **effetti che hanno una portata globale**.

Le organizzazioni terroristiche hanno già dato prova di abilità nello sfruttare tali effetti, sia per finalità operative, sia per il rilancio mediatico dei propri brand.

In prospettiva futura, è probabile che le **principali sigle del terrorismo internazionale** affineranno sempre di più la capacità di **"capitalizzare" le crisi in atto,** alimentando ulteriormente un trend che, a oggi, le vede declinare i propri messaggi istigatori in modo strumentale rispetto alle loro agende. L'interconnessione tra i diversi quadranti di crisi rischia inoltre di amplificare la proiezione esterna della minaccia, incluso verso l'Europa e l'Italia.

Con riferimento alla **Siria** e alle sue attuali fragilità interne, sarà importante monitorare il tentativo di DAESH di ricostruire il proprio network ed eventualmente potenziare le capacità di proiezione esterna, così come sarà opportuno adoperarsi per limitare il rischio che Foreign Terrorist Fighters detenuti nei campi e nelle carceri presenti nel Paese possano spostarsi verso il territorio europeo. Un rischio rilevante soprattutto in caso di rilasci o fughe incontrollate, come già avvenuto a inizio 2026.

Quanto alle **proiezioni esterne delle tensioni tra Israele e Hamas**, recenti operazioni di polizia condotte in Italia e in altri Paesi europei confermano la necessità di tenere alta l'attenzione sia sui possibili canali di finanziamento al terrorismo, sia sui network che Hamas potrebbe costituire all'estero.

In tale scenario, l'antisemitismo assume un rilievo sempre più internazionale, oltre che trasversale a diverse ideologie estremiste. L'attentato di Bondi Beach e quello contro la sinagoga di Heaton Park, entrambi verificatisi durante delle festività religiose, hanno ulteriormente consolidato la percezione secondo cui i luoghi delle comunità e delle celebrazioni ebraiche siano considerati obiettivi prioritari da colpire, indipendentemente dal contesto geografico in cui si collocano. Il rischio di lungo periodo non consiste, dunque, esclusivamente nel compimento di ulteriori attentati, bensì nel sentimento di normalizzazione della paura che, progressivamente, va radicandosi nei predetti contesti.

Parallelamente, un ampliamento del conflitto me-

> *La sfida principale risiederà probabilmente nella capacità di "guidare" tali tecnologie, che continueranno a rappresentare degli strumenti di potenziamento, e non di sostituzione, delle capacità umane*

diorientale, soprattutto verso l'**Iran**, potrebbe accentuare, nel prossimo futuro, i rischi di propagazione del rischio terroristico anche in Europa. Sull'onda lunga della guerra dei dodici giorni tra Israele e Iran, che nel giugno 2025 ha visto anche il coinvolgimento statunitense, e sulla base di quelli che saranno gli effetti delle proteste esplose in Iran a fine dicembre 2025, cui sono seguiti momenti di grande incertezza e tensione in ambito internazionale, non può infatti escludersi un innalzamento - anche in Europa e in Italia - del rischio terrorismo, soprattutto rispetto a target israeliani o statunitensi. In prospettiva, la propaganda jihadista potrebbe, in modo opportunistico, strumentalizzare un eventuale conflitto che coinvolga Teheran, invocando un "jihad globale" contro il "comune nemico" occidentale.

Quanto all'**Africa**, il trend di progressiva espansione delle formazioni jihadiste nel continente non dà, a oggi, segnali di arresto o rallentamento. Oltre ad attacchi che potrebbero verificarsi contro assetti europei e nazionali presenti nell'area, persiste il rischio di traffici verso l'Europa meridionale sia di armi, sia di risorse finanziarie e umane che potrebbero favorire attività terroristiche.

La **regione saheliana**, inoltre, la cui instabilità può influenzare direttamente anche la sicurezza europea e italiana, si conferma come uno dei principali snodi operativi del jihadismo globale. In prospettiva, un'intensificazione della cooperazione tra diverse articolazioni territoriali di DAESH attive nell'area potrebbe portare a saldature strategiche, con un aumento del rischio di proiezioni esterne.

Sul fronte della minaccia proveniente dall'**Afghanistan**, è probabile che proseguirà il trend già osservato negli ultimi anni, che ha visto una serie di operazioni di polizia giudiziaria portare all'arresto di soggetti affiliati a ISKP in vari Paesi d'Europa. A questo, in termini di proiezione esterna della minaccia, si affianca il rischio posto dallo strutturato apparato mediatico di ISKP che, pur indebolito da recenti operazioni di controterrorismo, riesce ancora a declinare la propaganda del gruppo in diverse lingue regionali, facilitando l'emergere di nuovi processi di radicalizzazione anche in territorio europeo.

In un quadro globale sempre più complesso e interconnesso, le **funzionalità dell'intelligenza artificiale** giocheranno un **ruolo progressivamente più rilevante per le organizzazioni terroristiche internazionali**, sia in termini di creazione, sia di diffusione dei messaggi estremisti.

L'adozione di **sistemi sofisticati di generazione multimediale** permetterà ai gruppi terroristici di creare contenuti di qualità sempre più professionale, anche – ad esempio – attraverso l'impiego

di immagini e voci originali di leader non più in vita, al fine di aumentarne appeal e persuasività.

I giovani continueranno a costituire un target privilegiato di tale propaganda, in linea con un doppio trend che vede, da un lato, il persistente abbassamento dell'età media dei radicalizzati e, dall'altro, l'aumento del numero dei percorsi di radicalizzazione alimentati dalla sfera online e digitale. Come conseguenza, è possibile prevedere tempi di radicalizzazione sempre più brevi, con ciò che ne deriva in termini di difficoltà di intercettare tempestivamente la minaccia.

Sul piano tattico, il possibile uso di **modelli predittivi potenziati dall'IA** per **anticipare** la **risposta delle forze di sicurezza** contribuirà a rendere il contrasto della minaccia sempre più complesso. Il progresso dei sistemi linguistici generativi renderà i chatbot più precisi nel fornire assistenza alla fase di pianificazione degli attacchi, anche grazie alla sempre più stretta integrazione tra strumenti di geolocalizzazione, analisi di immagini e riconoscimento di pattern. Ciò permetterà di sviluppare ulteriormente le capacità di targeting, consentendo di tracciare movimenti individuali e collettivi, individuare luoghi sensibili e stimare finestre temporali di vulnerabilità in modo sempre più accurato. **Sul fronte dell'esecuzione operativa**, l'**IA** costituirà un **fattore di potenziamento della minaccia** in costante evoluzione. In prospettiva, infatti, oltre ai droni, anche le auto a guida autonoma che utilizzano l'IA potrebbero essere utilizzate per condurre attacchi terroristici "da remoto".

In relazione, poi, alle **pratiche di finanziamento al terrorismo**, l'**intelligenza artificiale** è probabilmente destinata ad **agevolare**, in modo sempre più efficace, **trasferimenti di risorse** che potrebbero diventare **sempre più difficili da tracciare**.

Per rispondere efficacemente a tali sfide, gli organi di sicurezza non potranno esimersi dall'investire sempre di più nell'utilizzo delle funzionalità dell'intelligenza artificiale, sia a fini di prevenzione che di contrasto alla minaccia. In tal senso, sarà fondamentale riuscire a **bilanciare** le **necessità di tutela della sicurezza nazionale con quelle relative agli aspetti tecnici, etici e normativi dell'IA**, anche al fine di facilitare una maggiore cooperazione transnazionale. Le valutazioni d'impatto in termini di privacy e diritti costituzionali, la promozione di programmi di ricerca congiunti tra pubblico e privato e la ricerca di un'armonizzazione – a livello internazionale – di un quadro comune di utilizzo dell'IA per il contrasto al terrorismo, che sappia coniugare le necessità del progresso tecnologico al rispetto dei diritti individuali, costituiranno temi di discussione sempre più centrali negli anni a venire.

La **sfida principale** che modellerà l'evoluzione sia della minaccia terroristica, sia delle misure per prevenirla e contrastarla, risiederà probabilmente nella **capacità di "guidare" tali tecnologie**, che continueranno a rappresentare degli strumenti di potenziamento, e non di sostituzione, delle capacità umane.

8. LA MINACCIA IBRIDA ALLE SOCIETÀ DEMOCRATICHE

Sono emersi all'attenzione delle intelligence occidentali, come principali attori ostili, la Federazione Russa e la Repubblica Popolare Cinese.

Quanto alla Russia, è stata confermata la sua capacità di sviluppare strategie, anche di medio-lungo periodo, per perseguire i propri interessi geopolitici. Tra le principali attività attribute a tale attore, rilevano i sabotaggi, le azioni informative e cinetiche ostili, l'impiego della leva energetica e alimentare, le interferenze sul piano politico, le operazioni di spionaggio, l'utilizzo dello strumento militare, le campagne di disinformazione, gli attacchi informatici e il sostegno a gruppi politici estremisti.

Per quanto riguarda le operazioni di manipolazione informativa e interferenza straniere, la Russia ha operato attraverso un ampio ecosistema mediatico - composto da mezzi di informazione statuali e non – anche sfruttando l'IA, in modo da elaborare narrazioni che mirano a evidenziare la supremazia di Mosca, screditare la dirigenza occidentale, nonché minare la fiducia nei confronti delle Istituzioni dell'UE e della NATO.

La Repubblica Popolare Cinese continua a presentare la capacità di sviluppare strategie ibride di medio-lungo periodo impiegando una combinazione di strumenti economici, diplomatici e informativi per espandere la propria influenza globale, condurre campagne di spionaggio ed esercitare pressioni economiche.

Per quanto attiene al contesto europeo, negli ultimi anni, la Cina ha

condotto attività ibride nei confronti degli Stati membri con lo scopo di influenzare i processi decisionali dell'Unione.

A livello politico, la Cina adotta un approccio duale, da leggere in connessione con le priorità economico-finanziarie fissate dal regime. Da un lato, infatti, dimostra impegno nell'attività di dialogo con la diplomazia europea, dall'altro, punta a intensificare i legami bilaterali con i singoli Stati membri.

Quanto all'ambito economico, si è assistito a un nuovo trend, caratterizzato dall'incremento degli investimenti greenfield da parte di Pechino.

Nel 2025, l'attore sinico ha altresì creato interdipendenze in vari settori e sfruttato in certe occasioni la pressione economica.

Permane il focus cinese sul dominio dell'informazione, che si articola attraverso una mirata strategia volta a sfruttare i media nazionali e i social per promuovere narrazioni positive su Pechino e sopprimere le voci più critiche.

FISIONOMIA ED EVOLUZIONE DEL FENOMENO

La **minaccia ibrida** si configura come un insieme coordinato di azioni condotte da attori statuali, che possono avvalersi anche di attori non statuali come agenti esterni o proxy (es. organizzazioni terroristiche o criminali, compagnie militari private o enti commerciali), collocate al di sotto della soglia del conflitto armato convenzionale, con lo scopo di danneggiare, destabilizzare o indebolire un Paese bersaglio, sfruttando le sue vulnerabilità politiche, economiche e sociali, nonché tecniche (es. resilienza cyber). Paesi e Attori - aventi una rilevante magnitudine, capacità e propensione geopolitica e finanziaria - sono gli unici in grado di articolare in modo agile ed efficace azioni coordinate e sinergiche su più domini (diplomatico, dell'informazione, militare, economico/finanziario e intelligence), mobilitando il proprio apparato.

Nell'attuale panorama internazionale la minaccia ibrida rappresenta una **sfida significativa per la sicurezza globale**, tanto che la NATO l'ha identificata come una delle priorità strategiche più importanti del ventunesimo secolo. Essa, infatti, sfoca il confine tra conflitto e competizione strategica, richiedendo risposte che integrino strumenti di difesa civile e militare, oltre che un forte coordinamento tra gli Stati destinatari delle attività ostili.

Per quanto attiene alle **operazioni cinetiche** (che si svolgono nel mondo reale) condotte nel quadro della minaccia ibrida, assumono particolare rilievo i **sabotaggi, spesso dissimulati sotto forma di incidenti**. Gli obiettivi di tali attività sono diversi, inclusi il blocco di settori economici, l'interruzione di servizi essenziali forniti dalle infrastrutture, anche critiche, e possono includere tentativi di assassinio e atti di vandalismo. Tanto premesso sul piano definitorio, occorre osservare come la **tecnologia** rappresenti simultaneamente il **veicolo primario attraverso cui si realizzano le minacce ibride e lo strumento privilegiato per mezzo del quale le democrazie liberali possono dimostrarsi resilienti**. Basti pensare, nel senso, alla possibilità di impiegare sistemi di intelligenza artificiale sofisticati per identificare campagne di disinformazione e deepfake.

In tale quadro, assumeranno un **ruolo sempre più rilevante** le **infrastrutture digitali decentralizzate e ridondanti**, in quanto maggiormente indicate per resistere agli attacchi cibernetici. Più dettagliatamente, blockchain e tecnologie di verifica digitale potranno essere utilizzate per autenticare informazioni e contrastare la manipolazione dell'informazione, esprimendo così un significativo potenziale anche rispetto alla tutela della sicurezza nazionale. Risulteranno pertanto **decisivi**, anche ai fini di una strategia di difesa integrata, gli **investimenti in ambito di cybersecurity, resilienza delle infrastrutture critiche e alfabetizzazione digitale della popolazione**.

Permane la sfida posta dalla costante evoluzione che caratterizza le minacce ibride, tanto da con-

sentire il progressivo adattamento delle stesse ai sistemi di difesa implementati. Tutto ciò si rifletterà, inevitabilmente, sulla necessità di **integrare** le **forme di difesa statica, con la capacità di anticipazione, adattamento e innovazione continua**. Assume dunque una portata eminentemente strategica la ricerca in materia di intelligenza artificiale applicata sia alla sicurezza cibernetica sia all'elaborazione dei segnali.

Le nazioni che investiranno più significativamente nella ricerca di tecnologie di difesa emergenti avranno una maggiore possibilità di mantenere un elevato grado di resilienza di fronte a minacce ibride in continua evoluzione. Nello scenario delineato, i principali attori della minaccia sono attualmente la Federazione Russa e la Repubblica Popolare Cinese. I due Paesi si differenziano, tuttavia, in termini di obiettivi, modalità e strategie messe in atto.

RUSSIA

Quanto alla **Russia**, rileva la sua capacità di **sviluppare strategie anche di medio-lungo periodo, per perseguire i propri interessi geopolitici**. Le attività orchestrate dal Cremlino includono sabotaggi, azioni informative e cinetiche ostili, impiego della leva energetica e alimentare, interferenze sul piano politico, operazioni di spionaggio, utilizzo dello strumento militare, campagne di disinformazione, attacchi informatici e sostegno a gruppi politici estremisti.

> *Nell'ambito della strategia ibrida russa, vengono condotte regolarmente iniziative ostili contro i Paesi europei al fine di minare il sostegno occidentale a favore di Kiev*

Nell'ambito della strategia ibrida russa, vengono condotte regolarmente **iniziative ostili contro i Paesi europei al fine di minare il sostegno occidentale a favore di Kiev**. Mosca segue delle macro-direttrici strategiche volte a destabilizzare la coesione del fronte occidentale, erodere il supporto popolare ed elettorale dei Governi che supportano l'Ucraina, cercare di eliminare o ridimensionare le sanzioni e le restrizioni subite dalla Russia a partire dall'inizio dell'invasione nel febbraio 2022.

La capacità del Cremlino di condurre campagne ibride trova fondamento nell'asimmetria tra i sistemi politici di stampo autoritario e quelli democratici. Nella propria proiezione esterna, Mosca sfrutta valori, diritti e libertà delle società democratiche, dell'economia occidentale e dell'ecosistema dell'informazione e di opinione, per portare avanti **campagne multi-vettoriali e multi-dominio**. Al contempo, la Federazione difende il proprio regime adottando una capillare censura interna, come avvenuto ad esempio con l'imposizione di graduali restrizioni alla piattaforma di messaggistica Telegram e con il blocco dell'accesso a Whatsapp, e rimuovendo ogni

meccanismo di responsabilizzazione della politica nei confronti dell'opinione pubblica russa.

A partire dall'invasione dell'Ucraina, l'Italia ha dovuto fronteggiare diversi tentativi e iniziative ibridi ostili da parte di attori riconducibili alla Russia, indirizzati, tra gli altri, ai domini cibernetico e dell'informazione. Lo sforzo sul fronte ucraino sta determinando un notevole impiego di risorse da parte russa non solo nelle operazioni cinetiche, ma anche in quelle cibernetiche. Sin dalle prime fasi del conflitto, infatti, Mosca ha considerato lo spazio cibernetico come un ambito ove estendere la propria strategia geopolitica, utilizzando attacchi mirati per influenzare eventi politici e sabotare infrastrutture critiche.

> *Le entità russe coinvolte nella pianificazione e condotta delle attività di disinformazione includono figure istituzionali, Organismi di intelligence e funzionari nel territorio russo o dislocati presso le rappresentanze diplomatiche di Mosca all'estero*

Nell'ultimo anno, gli **attacchi cibernetici di matrice russa nei confronti dell'Italia** hanno perseguito maggiormente l'**obiettivo** dello **spionaggio** – in particolare contro la Pubblica Amministrazione centrale – **e** quello di **rendere inutilizzabili i sistemi colpiti**, ostacolandone la ricostruzione.

Parallelamente alle attività cibernetiche di matrice statuale, gli **attacchi** condotti da **attori filorussi nei confronti di obiettivi nazionali** sono caratterizzati dalla presenza di **cyber gang di tipo hacktivist**. Nel 2025, infatti, sono stati condotti un numero sempre maggiore di attacchi DDoS e di web site defacement ai danni di Paesi che sostengono l'Ucraina, tra cui l'Italia.

Nell'ambito delle **operazioni di manipolazione informativa e interferenza straniere (Foreign Information Manipulation and Interference – FIMI)**, la Russia agisce attraverso un ampio ecosistema mediatico composto da mezzi di informazione statuali e non, tra cui canali di comunicazione istituzionale e diplomatica ufficiale, mezzi di informazione statali, reti di proxy, canali social e amplificatori. Le narrazioni mirano a evidenziare la supremazia russa, screditare la dirigenza occidentale, nonché minare la fiducia nei confronti delle Istituzioni dell'UE e della NATO.

Per sviluppare la narrazione, la **tecnica** maggiormente utilizzata dall'attore russo è quella della **distorsione delle informazioni**. Infatti, partendo da notizie ed eventi di attualità, vengono sviluppati contenuti in cui i fatti, tendenzialmente riportati in modo parziale, sono suscettibili di una differente interpretazione (**malinformation**). I contenuti sono pertanto oggetto di riformulazione del contesto o contaminazione delle informazioni, allo scopo di spingere l'audience a trarre conclusioni diverse rispetto al messaggio originale. Al riguardo, emerge come l'impiego della distorsione delle informa-

zioni costituisca un'evoluzione rispetto al passato, quando le risorse legate al Cremlino erano solite diffondere direttamente notizie false (disinformazione pura).

Le entità russe coinvolte nella pianificazione e condotta delle attività di disinformazione includono figure istituzionali, Organismi di intelligence e funzionari nel territorio russo o dislocati presso le rappresentanze diplomatiche di Mosca all'estero.

Un'altra recente evoluzione nella produzione di contenuti è legata all'impiego dell'intelligenza artificiale. In particolare, sono stati riscontrati casi di **diffusione di video generati dall'IA** che mirano a **promuovere fatti e notizie in modo parziale/decontestualizzato o riformulandone il contenuto** per fuorviare l'audience e spingerla a sostenere la tesi dell'attore della minaccia.

Per le sue iniziative in Italia, Mosca si avvale:

- degli ambienti filo-russi e dell'associazionismo russo;
- di singoli soggetti di chiara postura pro-russa, oppure di blogger/reporter, finanziati direttamente e ospitati anche nel territorio russo;
- di profili non immediatamente riconducibili alla Federazione per penetrare ambienti di interesse informativo (contesti Difesa/NATO).

La **Russia** è in grado di **operare** anche in prossimità di **grandi eventi organizzati dai Paesi occidentali, interferendo e manipolando l'informazione**, specie nel dominio web, lanciando allarmi e alimentando dubbi e voci sui rischi per la sicurezza della popolazione, nonché tentando di amplificare il sentimento di sfiducia nei confronti dei Governi e verso le Istituzioni europee.

Tali iniziative sono state affiancate, soprattutto di recente, da azioni asimmetriche concretizzatesi in atti di sabotaggio contro siti strategici coinvolti nel supporto degli sforzi militari dell'Ucraina. Per tali operazioni il Cremlino si è avvalso di soggetti che non hanno la cittadinanza russa, solitamente reclutati online, nel tentativo di incrementare la propria capacità di negare il coinvolgimento nell'azione ostile (plausible deniability).

Sebbene finora non siano stati registrati eventi di natura violenta sul territorio italiano, l'eventuale coinvolgimento di entità o proxy russi in tale tipologia di atti o in azioni di sabotaggio rappresenta una possibile evoluzione del modus operandi della Russia in Europa e riflette il citato approccio maggiormente incline al rischio del Cremlino, specie in termini di ripercussioni sulle relazioni bilaterali.

CINA

La **Repubblica Popolare Cinese** si è gradualmente ritagliata un **ruolo sempre più rilevante** nel panorama delle **iniziative connesse alla minaccia ibrida**. Anche Pechino è in grado di sviluppare una **strategia ibrida di medio-lungo periodo** impiegando una **combinazione** di **strumenti economici, diplomatici e informativi** per espandere la propria influenza globale, condurre campagne di spionaggio

industriale ed esercitare pressioni economiche.

Forte di un sistema capillarmente controllato dal Partito Comunista Cinese, Pechino vede nell'utilizzo integrato di strumenti eterogenei un efficace mezzo di politica estera e mette in campo strategie whole-of-government (che uniscono le attività di diversi Ministeri, pubbliche amministrazioni e agenzie in modo da offrire soluzioni unitarie a particolari problemi o criticità), caratterizzate da una forte componente di deniability.

La Cina approfitta, altresì, della penetrabilità delle economie di mercato estere al fine di ottenere una posizione di vantaggio competitivo a livello internazionale, nonché di aumentare il livello di dipendenza dai prodotti e dalle proprie aziende. Al contempo, presso le opinioni pubbliche straniere, anche grazie a un sapiente sfruttamento delle caratteristiche dell'infosfera, vengono promosse costanti **attività di propaganda tese a rinforzare** una **percezione positiva della realtà sinica** nel dominio informativo.

Inoltre, l'ampliamento del concetto di sicurezza nazionale da parte di Xi Jinping e l'accresciuta assertività cinese all'estero si traducono in una maggiore importanza attribuita dalla dirigenza al "Dipartimento del Lavoro del Fronte Unito" del Comitato Centrale del Partito Comunista Cinese, un'agenzia del PCC che gestisce le relazioni con vari individui e organizzazioni all'interno e all'esterno dei confini cinesi.

Per quanto attiene al contesto europeo, negli ultimi anni, la Cina ha condotto **attività ibride nei confronti degli Stati membri** con lo **scopo di influenzare i processi decisionali dell'Unione**. Pechino mira a ottenere una UE frammentata, una coalizione occidentale debole e un mercato europeo aperto e stabile, da sfruttare come fonte di crescita economica e di acquisizione di conoscenza tecnologica.

A livello politico, la **Cina** adotta un **approccio duale**, da leggere in connessione con le priorità economico-finanziarie fissate dal regime. Da un lato, infatti, dimostra impegno nell'attività di dialogo con la diplomazia europea, con l'obiettivo di evitare un eccessivo allineamento tra Europa e USA. Dall'altro, punta a intensificare i legami bilaterali con i singoli Stati membri, cercando di alimentare e sfruttare a proprio vantaggio le divergenze interne all'Unione.

Tradizionalmente, **in ambito economico**, Pechino faceva largo uso delle merger and acquisitions per penetrare le economie straniere, ma recentemente la direzione strategica ha virato verso un aumento dell'utilizzo degli **investimenti greenfield**, che prevedono la costruzione di nuove infrastrutture nel Paese target e non la mera acquisizione di quelle già esistenti. Questo trend è stato osservato anche in Europa, dove sono in crescita tali investimenti, ad esempio, negli impianti europei di produzione di veicoli e di batterie elettriche. Tale pratica consentirebbe di aggirare i dazi doganali. La Cina continua, altresì, a investire nelle infrastrutture strategiche e

nel settore logistico, con un focus particolare sui principali porti mediterranei nell'ambito della Belt and Road Initiative (BRI).

Gli altri strumenti che Pechino predilige sono la **creazione di interdipendenze economiche e la pressione economica**. La Cina tende ad adottare misure di risposta energiche (formali o informali) in caso di iniziative europee contrarie ai propri interessi. Ad esempio, l'imposizione di dazi commerciali da parte dell'UE nell'ottobre 2024 ha spinto la RPC a imporre, a sua volta, dazi provvisori, di portata limitata e su settori non strategici. Questa iniziativa evidenzia anche come la Cina ricorra sempre più spesso allo strumento legale come parte della propria strategia per portare avanti obiettivi di politica estera.

Per quanto concerne il dominio tecnologico, si è registrato un **incremento** consistente degli **accordi di cooperazione internazionale in ambito di ricerca e sviluppo**. Le principali aree di interesse sono state: quantum computing, IA, tecnologia marittima, agritech e tecnologia informatica. Pechino è in grado, infatti, di fare leva sulle proprie disponibilità economiche, offrendo finanziamenti in cambio di ruoli di direzione e controllo in numerosi progetti di ricerca di alto livello. Al contempo, il governo cinese monitora tutte le attività di collaborazione accademica con l'estero dei propri atenei, imponendo forme di supervisione sui principali temi e sulle controparti.

Tra i diversi domini del potere, quello dell'informazione ha assunto – negli ultimi anni – un ruolo di particolare rilievo nelle strategie siniche. Al riguardo, da quando il Presidente XI Jinping è salito al potere, è divenuta chiara l'intenzione della leadership di rendere la Cina un attore capace di influenzare i dibattiti internazionali. A questo scopo sono state **amplificate e valorizzate** le **attività dei media nazionali e dei think tank all'estero**. La **strategia cinese** è finalizzata a **promuovere narrazioni positive su Pechino e a sopprimere le voci più critiche**. La Cina è potenzialmente in grado di sfruttare i media occidentali acquistando spazi promozionali in cui pubblicare i propri contenuti con uno stile giornalistico in modo da farli apparire quali articoli scritti dalle testate stesse, nascondendo la natura di contenuto sponsorizzato. Anche i social media giocano un ruolo importante in questa strategia mediatica: dal 2019 c'è stato infatti un incremento delle attività sui social da parte di diplomatici cinesi attivi nel diffondere narrazioni positive su Pechino e nel contrastare le opinioni critiche.

In genere, la Cina non veicola contenuti antagonisti rispetto all'Unione europea, al contrario cerca di evidenziare gli aspetti positivi della collaborazione multilaterale-bilaterale. Più frequenti sono, invece, i contenuti critici nei confronti degli Stati Uniti e della NATO.

SCENARI E TECNOLOGIE PER LE CAMPAGNE DI DISINFORMAZIONE

Nel contesto della minaccia ibrida, la **manipolazione informativa** rappresenta **uno degli strumenti più efficaci e pervasivi delle campagne ibride** e, più recentemente, di quella che viene definita guerra cognitiva.

L'**obiettivo primario** delle campagne di disinformazione è da sempre stato quello di **minare la fiducia della popolazione nelle istituzioni democratiche, nelle autorità pubbliche** (generalmente governi e forze dell'ordine, ma anche obiettivi specifici come, ad esempio, il sistema sanitario) **e nei mezzi di informazione tradizionali**, ostacolando così la capacità dei cittadini di prendere decisioni informate. In combinazione con altri strumenti/tool ibridi, come gli attacchi cyber e la coercizione economica, la disinformazione amplifica il caos e la polarizzazione sociale. Recentemente, si è anche assistito a un'evoluzione degli obiettivi delle campagne di manipolazione informativa e ingerenza esterna a livello globale, che non cercano di influenzare unicamente "cosa" pensa l'opinione pubblica, ma anche "come" pensa. L'obiettivo, quindi, non è solo alterare la percezione della realtà, ma agire direttamente sui processi cognitivi, sulle credenze, sulle abitudini e sulle attitudini comportamentali di una specifica audience.

> *L'obiettivo primario delle campagne di disinformazione è da sempre stato quello di minare la fiducia della popolazione nelle istituzioni democratiche, nelle autorità pubbliche e nei mezzi di informazione tradizionali, ostacolando così la capacità dei cittadini di prendere decisioni informate*

L'attuale panorama geopolitico e securitario risulta dunque rimodellato dalla minaccia ibrida, in generale, nonché dalla specifica evoluzione delle tecniche disinformative che portano alla guerra cognitiva. Questi paradigmi di conflitto superano la distinzione tra militare e civile, impiegando una **combinazione sinergica di mezzi cinetici e**, sempre più spesso, **non cinetici, in cui la disinformazione assume il ruolo di vettore strategico**.

Tanto premesso, occorre mettere in luce i diversi scenari strategici in cui le campagne di disinformazione vengono messe in atto per massimizzare il loro impatto. Al riguardo, l'**interferenza elettorale** costituisce un ambito tradizionale. Gli attori ostili diffondono narrazioni false o manipolate, spesso su vasta scala tramite social media, per screditare candidati, alimentare la sfiducia nel processo di voto o esacerbare divisioni interne. L'intento è quello di destabilizzare il Paese colpito minando la legittimità democratica delle sue Istituzioni.

Eventi come la pandemia e la guerra in Ucraina hanno dimostrato quanto le crisi fungano da am-

plificatori. La **disinformazione** viene infatti usata **per diffondere panico, minimizzare la minaccia o giustificare operazioni militari**, come nel caso di false flag (operazioni condotte con l'intento di mascherare l'effettiva matrice delle stesse e attribuirne a terzi la responsabilità), o narrazioni sulla presunta "resa" delle forze avversarie. L'azione mira pertanto a condizionare le percezioni e le convinzioni dei cittadini, rappresentando un aspetto della disinformazione che può essere considerato come guerra cognitiva.

Le **campagne possono** altresì **precedere o accompagnare attacchi fisici o cyber alle infrastrutture critiche**. La diffusione di notizie false su presunti malfunzionamenti o pericoli in atto può preparare il terreno psicologico, aumentando l'impatto di un eventuale attacco e rendendo più difficile la risposta delle Autorità. Anche i **sabotaggi** possono essere utilizzati, non tanto per il loro fine destabilizzante, ma proprio come elemento di guerra psicologica. In tale quadro, rileva anche la **strumentalizzazione di fenomeni sociali**, di cui vengono sfruttate vulnerabilità preesistenti, come i flussi migratori o le tensioni sociali.

La disinformazione tende anche a **minare la coesione e i valori fondanti di alleanze internazionali**, come la NATO o la UE, diffondendo narrazioni che mettono in discussione la loro efficacia, la loro solidarietà interna o i loro obiettivi strategici. In questo scenario possono essere colpiti anche i singoli leader attraverso campagne di manipolazione informativa che propongono riletture fuorvianti di fatti e affermazioni reali.

L'efficacia e la scala delle moderne campagne di disinformazione sono esponenzialmente accresciute dall'integrazione di tecnologie avanzate, che consentono la creazione, la definizione di contenuti manipolatori mirati e la diffusione a una velocità senza precedenti.

L'**IA generativa** è il **motore propulsivo** dell'**attuale ondata di disinformazione**, anche a causa dell'impiego di due strumenti:

- i **Large Language Models (LLMs)**, che permettono la produzione rapida, sostenuta e a basso costo di narrazioni false o distorte, in più lingue e adattate a contesti culturali specifici, rendendo così obsoleti i tradizionali metodi di propaganda manuale;
- il **Deepfake**, attraverso l'uso di reti neurali avversarie (Generative Adversarial Networks - GANs), che consente di creare contenuti multimediali (audio, video, immagini) iperrealistici, tanto da simulare l'aspetto e la voce di persone reali (politici, esperti, influencer, ecc.). Tali strumenti rappresentano una minaccia diretta alla fiducia pubblica e alla capacità di distinguere il vero dal falso, specie quando utilizzati per veicolare disposizioni o annunci falsi in situazioni di crisi.

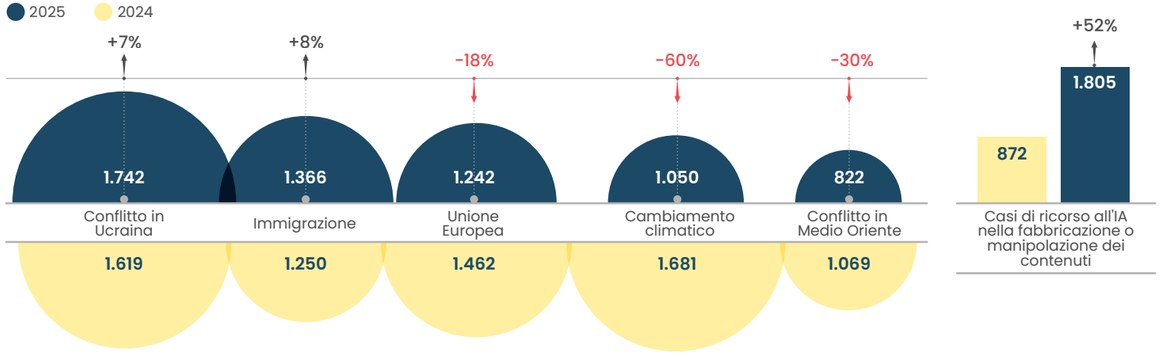
Anche le **piattaforme social e** i **grandi data-set** raccolti **sul comportamento degli utenti** sono **sfruttati per massimizzare l'impatto cognitivo**. Rilevano, nel senso:

- i **sistemi di behavioral analytics**, che con-

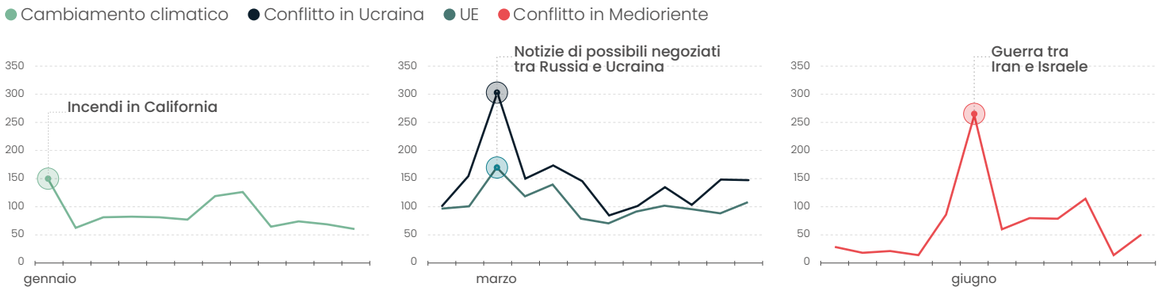
LA DISINFORMAZIONE CONTRO LE DEMOCRAZIE LIBERALI

Tra gli strumenti più efficaci e pervasivi della minaccia ibrida, la disinformazione trova terreno fertile nel moltiplicarsi degli scenari di crisi e nelle opportunità offerte dalle nuove tecnologie. L'erosione della coesione sociale e della fiducia nelle istituzioni è un obiettivo ricorrente, ma spesso funzionale a scopi ulteriori: orientare decisioni, frammentare coalizioni, polarizzare il dibattito e aumentare lo spazio di manovra dell'attore.

Principali temi delle notizie false oggetto di fact-checking da parte della rete European Digital Media Observatory (EDMO)

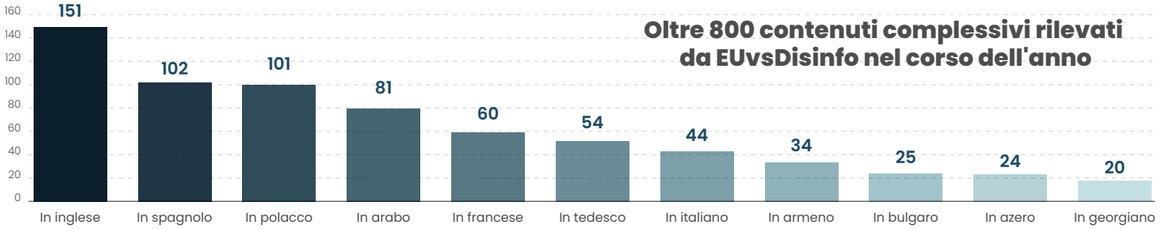


Andamento dei temi oggetto di notizie false nel corso del 2025 (EDMO)



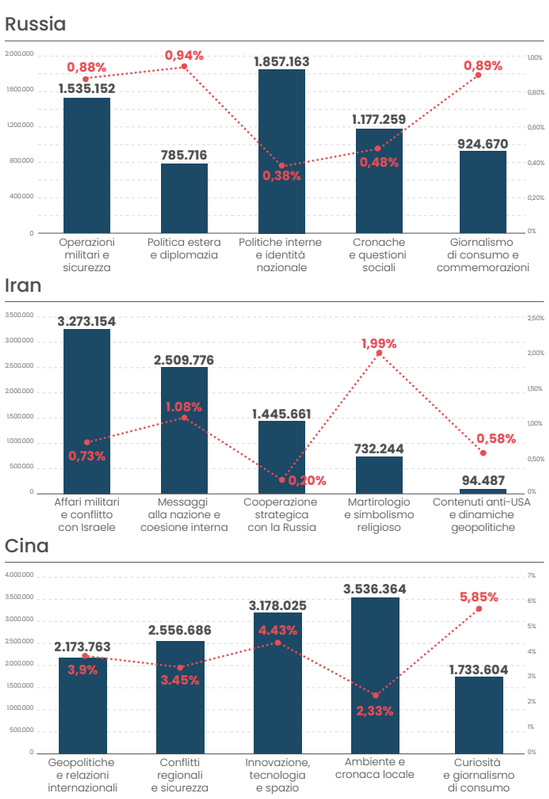
Le lingue della disinformazione russa

I contenuti disinformativi pubblicati da outlet pro-Cremlino rilevati da EUvsDisinfo nelle principali lingue di produzione, escluso il russo



Le narrazioni prevalenti di Russia, Cina e Iran

Per ciascun Paese, i 50 contenuti con più visualizzazioni raccolti nel 2025 da Hamilton[1], pubblicati da canali statali o affiliati allo Stato, sono stati raggruppati in macro-categorie tematiche.

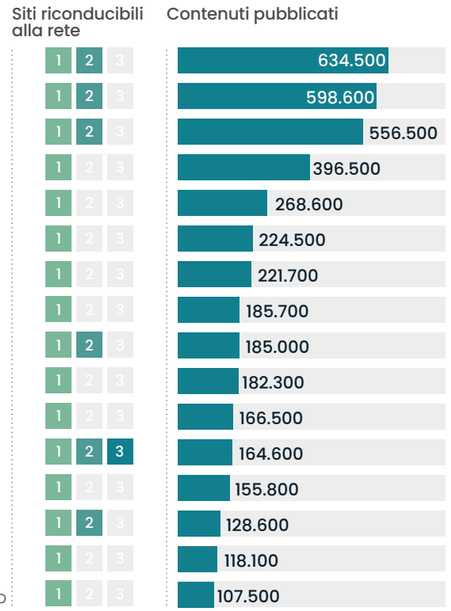


1. *"Hamilton 2.0"* è un progetto della Alliance for Securing Democracy presso il German Marshall Fund of the United States (GMFUS). La piattaforma raccoglie i contenuti pubblicati da canali statali ufficiali o media finanziati dallo stato di Russia, Cina e Iran su Telegram, Facebook, Instagram, YouTube, siti d'informazione online, dichiarazioni ufficiali e comunicati stampa.

2. *L'engagement rate* rapporta le interazioni attive (like e condivisioni) al volume totale delle visualizzazioni, permettendo di distinguere tra la mera esposizione passiva e la reale capacità di un messaggio di generare risonanza e partecipazione nell'audience. Il valore indica quante interazioni ogni contenuto ha mediamente ricevuto ogni 100 visualizzazioni.

I principali target della rete Pravda

dall'avvio delle rilevazioni della "Pravda Dashboard" (CheckFirst e DFRLab) al 31 gennaio 2026



Tra le principali campagne FIMI attribuite alla Russia, la rete Pravda propone nelle sue molteplici versioni nazionali articoli che riutilizzano contenuti provenienti da siti d'informazione e canali Telegram pro-Cremlino, amplificando le narrazioni russe.

Il livello di rischio della disinformazione

Nell'edizione 2026 del Global Risks Report, il World Economic Forum (WEF) ha collocato "misinformazione e disinformazione" al secondo posto tra i rischi globali più gravi nel breve termine (2 anni), dietro ai soli "conflitti geoeconomici" e davanti a "polarizzazione sociale" ed "eventi climatici estremi". Ad acuire il livello di rischio sono, secondo il WEF, l'accelerazione tecnologica e le opportunità offerte dall'IA alla creazione di contenuti ingannevoli e manipolativi.

Le Nazioni Unite, nel loro più recente Global Risk Report (basato su dati 2024), pongono invece "misinformazione e disinformazione" al terzo posto tra i rischi globali dopo "l'inazione rispetto al cambiamento climatico" e "l'inquinamento su larga scala". Il rischio in questione, accresciuto dall'innovazione tecnologica, è direttamente connesso al rischio di "collasso della coesione sociale" e, di conseguenza, alla "erosione della sovranità statale".

sentono la profilazione psicologica automatizzata dei destinatari della disinformazione, identificando vulnerabilità emotive e cognitive specifiche (es. tendenza al complottismo, polarizzazione politica, ansia sociale);

- gli **ecosistemi di bot e influencer sintetici**, ossia reti automatizzate di account, che possono essere gestite da IA, amplificano in modo massivo il contenuto disinformativo. Inoltre, gli influencer sintetici, creati interamente tramite IA, possono costruirsi una credibilità su nicchie specifiche, veicolando messaggi con una parvenza di autenticità;
- gli **attacchi coordinati cibernetici e cognitivi**, che, in futuro, potrebbero aumentare, creando una sinergia di shock e incertezza.

La costante iperconnessione e l'eccesso informativo (overload) che caratterizzano le moderne società democratiche rendono la mente umana sempre più vulnerabile. La disinformazione strategica sfrutta questo contesto saturando il canale informativo, rendendo difficile l'analisi critica e spingendo gli individui a delegare la propria decisione cognitiva a input esterni maggiormente caratterizzati da rapidità ed elevato impatto emotivo.

In definitiva, la necessità di difendere il dominio cognitivo richiederebbe lo sviluppo e l'adozione di contromisure tecnologiche che possano ripristinare la fiducia nell'informazione e garantire la sua integrità. Al riguardo, si potrebbe optare per strategie di contrasto in grado di muoversi sia sull'asse del

> *La tecnologia blockchain presenta delle caratteristiche fondamentali che la rendono una risorsa preziosa nel contrasto alla disinformazione*

rafforzamento della trasparenza e dell'immutabilità dell'origine dei contenuti, sia su quello dell'adozione di strumenti avanzati di verifica.

In questo scenario, la **tecnologia blockchain** presenta delle caratteristiche fondamentali (decentralizzazione, immutabilità, crittografia), che la rendono una **risorsa preziosa nel contrasto alla disinformazione**. Si pensi, in particolare:

- alla **tracciabilità dell'informazione**. La blockchain consente infatti di creare un registro cronologico, distribuito e protetto da meccanismi crittografici. Ne deriva che un contenuto (es. articolo di giornale, immagine, video) può essere registrato sulla blockchain al momento della sua creazione, ottenendo un "sigillo temporale" inalterabile. Qualsiasi modifica successiva risulterebbe immediatamente evidente. Tale caratteristica rafforza l'autenticità dei contenuti originali e responsabilizza gli editori e i giornalisti;
- all'**identità digitale sovrana (self-sovereign identity - SSI)**. L'applicazione della blockchain per l'identità digitale può limitare la diffusione massiva di bot e account falsi. Con account legati a un'identità digitale verificabile, le operazioni di

amplificazione non autentica risulterebbero significativamente più difficili e tracciabili.

Complementarmente alla blockchain esistono anche **altre tecnologie di verifica digitale che si concentrano sull'attribuzione e sulla protezione dei contenuti**, come:

- il **digital watermarking e i metadati protetti**. L'inserimento di watermark digitali nei contenuti multimediali, talvolta impercettibili all'occhio umano ma rilevabili da software specifici, fornisce una prova d'integrità. Analogamente, l'utilizzo di standard per metadati protetti permette di incorporare direttamente nel file l'intera cronologia di creazione, modifica e pubblicazione, rendendo immediatamente riconoscibile l'origine del contenuto e, di conseguenza, la sua eventuale alterazione;
- la **counter-AI**. Sistemi di machine learning addestrati per rilevare pattern di disinformazione su larga scala, identificare reti di bot e analizzare anomalie nella diffusione dei contenuti in tempo reale. Algoritmi specifici possono anche essere utilizzati per l'analisi forense dei deepfake.

La disinformazione è una sfida esistenziale per le democrazie. Se le tecnologie offensive (come l'IA generativa) ne hanno amplificato la portata, le tecnologie difensive (come la blockchain e la verifica digitale) dovranno essere in grado di offrire gli strumenti necessari per ricostruire un ambiente informativo affidabile, essenziale per la stabilità e la sicurezza nazionale.

UN CASO DI STUDIO: LA PREVENZIONE DEI SABOTAGGI SOTTOMARINI

La **prevenzione dei sabotaggi alle infrastrutture sottomarine** rappresenta, oggi, un tema operativo di sicurezza nazionale ed europea, in quanto incide direttamente sulla continuità dei servizi essenziali: connettività digitale, scambi economici, funzionamento di filiere critiche e, in parte crescente, integrazione energetica. Nel dominio subacqueo, infatti, la vulnerabilità non dipende soltanto dall'entità del danno materiale, ma dalla combinazione di scarsa osservabilità, difficoltà di attribuzione e tempi di ripristino. In questo contesto, la prevenzione non può essere letta come un insieme astratto di principi, ma come l'esito di un percorso già avviato e caratterizzato da assetti di governance, intese internazionali, investimenti in capacità di monitoraggio, meccanismi di cooperazione tra pubblico e privato, nonché sviluppo tecnologico applicato.

Le **infrastrutture sottomarine** costituiscono una **componente strutturale dell'economia contemporanea e della competizione geopolitica internazionale**. I cavi in fibra ottica trasportano la quasi totalità del traffico intercontinentale di dati e abilitano servizi che sostengono pagamenti, cloud, logistica, sanità digitale e operazioni industriali. Accanto alle dorsali di comunicazione, i collegamenti elettrici sottomarini e le infrastrutture energetiche offshore assumono un ruolo crescente per l'inte-

> *Il rischio di sabotaggio nel dominio underwater si caratterizza per l'ampiezza delle tratte, la presenza di punti di concentrazione (strozzature geografiche, approdi, corridoi obbligati), la profondità e la complessità dell'ambiente operativo*

grazione dei mercati e la transizione energetica. La dipendenza da tali asset definisce un profilo di rischio specifico, in quanto anche interruzioni circoscritte possono generare effetti a catena, con impatti economici e operativi non lineari.

In tale cornice, l'**Italia** presenta un profilo particolare. La collocazione al centro del Mediterraneo la rende uno **snodo fisico e digitale, esposto ai rischi, ma anche strategicamente rilevante per la continuità delle connessioni tra Europa, Nord Africa e Medio Oriente**.

Anche la dimensione industriale costituisce parte integrante della postura preventiva. A livello nazionale, ciò trova un concreto riflesso nei diversi attori e nelle competenze presenti lungo la catena del valore (es. cantieristica e sistemi integrati nel dominio underwater, produzione e progettazione di cavi sottomarini, capacità subsea e robotica per ispezione e intervento, operatori di rete e connettività con interessi diretti nella protezione delle dorsali).

Il **rischio di sabotaggio nel dominio underwater** si caratterizza per l'ampiezza delle tratte, la presenza di punti di concentrazione (strozzature geografiche, approdi, corridoi obbligati), la profondità e la complessità dell'ambiente operativo. Ciò potrebbe favorire condotte collocabili nella c.d. "zona grigia", ossia azioni camuffabili come incidenti, interferenze accidentali o effetti collaterali di attività civili. La **prevenzione** deve quindi **misurarsi con il concetto di plausible deniability**, in modo da attribuire rilevanza non solo alla protezione fisica, ma anche alla capacità di rilevare anomalie, ricostruire la sequenza degli eventi e ridurre la finestra di incertezza decisionale.

Gli eventi degli ultimi anni (es. attacco ai gasdotti Nord Stream; danneggiamento del gasdotto Balticconnector e di collegamenti associati nel 2023; guasti di cavi e interconnessioni nel Baltico e in alcune aree dell'Indo-Pacifico) hanno consolidato il fatto che le **infrastrutture sottomarine** sono **vulnerabili non solo ad azioni "classiche", ma anche a interferenze intenzionali a basso costo**, capaci di generare interruzioni e, soprattutto, incertezza.

Su questa base, la **postura europea** si è progressivamente strutturata lungo **tre direttrici principali**:

- riconoscimento dei cavi e delle infrastrutture sottomarine come asset di rilevanza sistemica e, quindi, come priorità di resilienza;
- promozione della valutazione dei rischi e di procedure comuni per la segnalazione, la gestione dell'incidente e il relativo ripristino, con un maggiore coordinamento tra autorità competenti e operatori privati;

- orientamento di programmi e investimenti verso requisiti di sicurezza, affidabilità delle tecnologie impiegate e riduzione delle dipendenze critiche.

In parallelo, la postura della NATO, in stretta cooperazione con l'UE, ha contribuito a rendere il tema effettivamente operativo, riducendo frammentazioni e sovrapposizioni. L'Alleanza Atlantica, infatti, ha sviluppato iniziative dedicate alla protezione delle infrastrutture sottomarine critiche e al rafforzamento della consapevolezza situazionale integrata (dalla superficie al fondale, fino ai livelli informativi e di sorveglianza disponibili). La cooperazione con l'Unione europea, più in generale, si concentra su interoperabilità e scambio informativo, esercitazioni e procedure di crisi, coinvolgimento dell'industria e degli operatori, e raccordo tra capacità operative e leve non militari. L'obiettivo è quello di rendere più rapido e coerente il ciclo "rilevamento–attribuzione–decisione–ripristino", che nel dominio underwater costituisce una variabile determinante.

La **prevenzione**, tuttavia, **non è soltanto governance, ma anche capacità**. Al riguardo:

- **in superficie** la consapevolezza del dominio marittimo integra tracciamenti, dati di traffico navale e immagini satellitari, mentre piattaforme e reti di scambio informativo supportano la lettura dei pattern operativi e l'individuazione di comportamenti anomali in prossimità di aree sensibili;
- **sul fondale**, invece, la disponibilità di sensoristica acustica (sonar e idrofoni), ispezioni periodiche e capacità di intervento costituisce un fattore di riduzione del rischio. In questo ambito, tra l'altro, si sta consolidando anche l'uso della fibra ottica e dei sistemi associati come base per forme avanzate di rilevamento di perturbazioni e indicatori precoci, soprattutto in prossimità dei punti critici.

Le tecnologie autonome hanno già un ruolo concreto in questa traiettoria. I veicoli subacquei autonomi e quelli senza equipaggio consentono ispezioni, verifiche e, in alcuni casi, interventi su tratti e nodi critici, oltre a estendere persistenza e copertura sensoriale in aree di interesse. In parallelo, l'intelligenza artificiale svolge una funzione abilitante attraverso la fusione di dati multi-sorgente, la classificazione automatica di segnali, la correlazione tra eventi in superficie e sul fondale, nonché la riduzione dei falsi positivi e la prioritizzazione delle ispezioni.

Sul piano delle **tecnologie dual use**, robotica subacquea, sensoristica, piattaforme autonome e software di analisi risultano utili alla protezione ma, potenzialmente, anche all'offesa o alla ricognizione ostile. Nei sistemi democratici, la gestione di tali beni duali richiede un equilibrio che valorizzi cooperazione e innovazione come strumenti di sicurezza. Rilevano, nel senso, i programmi congiunti di sperimentazione pubblico-privata, gli standard tecnici condivisi, i requisiti di sicurezza verificabili e i meccanismi di scambio informativo che consentano agli operatori di segnalare tempestivamente anomalie e alle autorità di integrare rapidamente dati e valutazioni. In tale quadro, l'**innovazione** è una **componente della postura preventiva**, in quanto aumenta la proba-

bilità di rilevamento, riduce i tempi di reazione, migliora la qualità dell'attribuzione e rafforza la resilienza, purché accompagnata da adeguati criteri progettuali (security by design) e da una gestione ordinata delle filiere.

La prevenzione nel dominio underwater richiede, infine, un **contributo sistematico** anche da parte dell'**Intelligence**, specie per quanto attiene:

- al monitoraggio di registri pubblici, comunicazioni societarie, dati commerciali, tracciati di navigazione e indicatori logistici per individuare anomalie ricorrenti e profili di rischio;
- alla ricostruzione di contesti operativi e relazioni tra assetti, comunicazioni e attività in aree sensibili, in modo da rafforzare capacità di attribuzione e di allerta tempestiva;
- all'integrazione di ciò che non è direttamente osservabile: intenzioni, reti di supporto, intermediazioni e dinamiche locali nei porti, nelle filiere e nei servizi;
- all'analisi delle vulnerabilità di supply chain, catene di proprietà e controllo, acquisizioni e partnership sensibili, oltre che delle dipendenze tecnologiche e del rischio connesso al dual use.

In definitiva, attraverso l'esercizio di queste funzioni è possibile ridurre la "zona grigia" prima dell'evento, proteggere know-how e filiere nazionali, sostenere la decisione politico-amministrativa in tempi compatibili con la continuità dei servizi e, in caso di incidente, accelerare i tempi di attribuzione, risposta e ripristino in coordinamento con operatori e alleati.

CINQUE TEST GenAI

NOTA METODOLOGICA

Per la prima volta, la Relazione sulla politica dell'informazione per la sicurezza propone cinque esercizi di analisi previsionale condotti attraverso il ricorso alle tecnologie dell'intelligenza artificiale. Seppur presentati entro il perimetro di ciò che può essere reso pubblico, essi vogliono testimoniare la portata fortemente innovativa e l'elevato potenziale dell'applicazione di strumenti di intelligenza artificiale generativa (GenAI), ad esempio i large language model (LLM), all'analisi intelligence come sostegno all'analista e ai tradizionali metodi di analisi.

Per testare appieno le potenzialità dei LLM, gli esercizi sono stati condotti come casi-studio su fonti aperte, escludendo il ricorso a documenti classificati. Considerato l'enorme volume di dati potenzialmente utili alla sicurezza nazionale disponibile in tale ambito, l'OSINT si conferma una disciplina capace di generare valore aggiunto per i Servizi di informazione e sicurezza, sempre più legata all'innovazione tecnologica per gestire un simile bacino di informazioni e, dunque, naturale beneficiaria di applicazioni di GenAI.

Il filo conduttore è un approccio rigidamente antropocentrico: operatori OSINT, analisti esperti di materia e personale tecnico, riuniti in gruppi di lavoro multidisciplinari, hanno creato un "circuito di controllo qualità" applicato a ogni fase del processo, dalla definizione dell'obiettivo informativo, alla selezione accurata delle fonti, dal prompting dei modelli, alla revisione e ricalibratura dei risultati, sino alla rappresentazione infografica proposta in questa Relazione.

La stretta collaborazione tra analisti e tecnici ha consentito di sfruttare appieno le potenzialità dell'intelligenza artificiale, tenendo conto dei limiti, rifuggendo dalla cieca fiducia negli strumenti, garantendo una validazione continua al fine di mitigare il rischio di imprecisioni ed errori. La natura multidisciplinare dei gruppi di lavoro è stata altresì funzionale a seguire il passo dell'innovazione tecnologica, che procede a balzi prestazionali costanti. Le tecniche di analisi strutturate utilizzate nei casi-studio – brainstorming, scenari alternativi, scenario più probabile, avvocato del diavolo, futuri possibili – sono state potenziate da prompt specifici per i LLM, consentendo di generare rapidamente un ventaglio di idee, testare ipotesi contrarie e individuare il percorso più plausibile con coerenza logica.

Dal punto di vista metodologico, gli esperimenti hanno adottato diverse modalità operative. In alcuni casi, gli analisti hanno pre-validato un set ristretto di fonti, portando il large language model a lavorare su dati controllati; in altri, l'IA ha esplorato

il web aperto, ampliando il bacino informativo, accedendo a notizie aggiornate e riducendo i bias umani. L'approccio ibrido, che combina le due strategie, ha prodotto risultati di valore, dimostrando che la flessibilità è fondamentale per trarre il meglio da queste tecnologie. Inoltre, è stato sperimentato l'uso di LLM per rivedere e migliorare prodotti di analisi già completati, mettendo in discussione ogni passaggio, identificando lacune di ragionamento e contribuendo a una sintesi più accurata.

Un altro punto di forza è stato rappresentato dalla varietà dei modelli messi a confronto nello stesso esercizio, con più interazioni, verifiche incrociate e una successiva sintesi qualitativa dei dati. Alcuni risultati sono stati poi combinati con algoritmi statistici classici per fornire previsioni quantitative, creando soluzioni ibride che uniscono la capacità di sintesi dell'IA con la robustezza e la solidità dei metodi tradizionali.

Le sperimentazioni in esame si diversificano anche per gli orizzonti temporali considerati, muovendo dal breve periodo (6-12 mesi) per l'evoluzione della minaccia jihadista in Siria, sino al lungo termine per gli sviluppi che, al 2035, caratterizzeranno la competizione tra grandi potenze nello spazio extra-atmosferico. Alcuni esercizi hanno incluso poi lo sviluppo tramite la GenAI di indicatori utili alle attività di monitoraggio e ricalibratura degli scenari di crisi, in supporto ai processi decisionali.

In definitiva, l'attività svolta dimostra che le tecnologie di intelligenza artificiale, integrate in un processo antropocentrico e metodologicamente rigoroso, possono incrementare sensibilmente la qualità complessiva della produzione intelligence. L'IA consente di analizzare enormi quantità di dati in modo più rapido ed efficiente, di far emergere schemi e tendenze altrimenti invisibili e di comprendere meglio scenari complessi. Permangono tanto la complessità e il rigore del processo analitico, quanto la professionalità e la competenza specifica dell'analista, comunque destinato a evolvere verso un modello di lavoro sempre più sinergico con questi strumenti tecnologici, nel quale il suo maggior valore si esprimerà nell'addestramento dei sistemi, nel loro efficace impiego e nella validazione dei risultati.

SPAZIO 2035: LA COMPETIZIONE OLTRE L'ATMOSFERA

SPAZIO 2035: LA COMPETIZIONE OLTRE L'ATMOSFERA

Negli ultimi anni lo spazio extra-atmosferico ha acquisito un ruolo chiave nelle strategie di sicurezza e di sviluppo economico dei più importanti Paesi del mondo, alla ricerca di una sovranità tecnologica che include tecnologie e progettualità spaziali. Le aree di maggiore competizione si sostanziano, in particolare, nella ricerca e nello sviluppo di tecnologie avanzate per: osservazione della Terra, telecomunicazioni sicure, sistemi di navigazione, accesso allo spazio. Per questo motivo, il dominio spaziale sarà sempre più all'attenzione dell'analisi intelligence nel prossimo decennio.

NOTA METODOLOGICA

Individuati i quattro principali driver che caratterizzano lo spazio (le dinamiche di competizione tra i principali attori statuali, la commercializzazione dello spazio e l'affermazione dei grandi attori privati, la militarizzazione del settore e i rischi di sicurezza nell'orbita terrestre, e l'applicazione di tecnologie dirompenti) e messi a sistema con gli applicativi di intelligenza artificiale generativa (GenAI), sono stati tracciati gli sviluppi che, al 2035, in un futuro possibile, potranno caratterizzare la corsa allo spazio tra grandi potenze e il ruolo che il nostro Paese può riservarsi.

UN FUTURO POSSIBILE: LO SPAZIO NEL 2035

Immaginiamo di essere nel 2035. Il concetto di uno "Spazio Globale" unitario e regolato dal Trattato sullo Spazio Extra-atmosferico (1967) è collassato. Centrale per la sicurezza e la competitività economica degli Stati, nonché per la gestione delle crisi, l'ambiente spaziale è, al 2035, un terreno continuamente conteso.

L'orbita bassa (LEO) non è più un bene comune globale, ma una serie di "zone economiche esclusive" sovrapposte e altamente regolamentate. Esse non sono delimitate da confini fisici ma dal controllo di slot orbitali gestiti da tre blocchi spesso concorrenti: l'asse sino-russo, l'alleanza guidata dagli USA e una federazione commerciale europea ancora frammentata ma dotata di cospicue ri-

sorse economiche. Le due principali coalizioni, quella sino-russa e quella a guida americana, competono principalmente nell'infrastruttura cislunare e lunare attraverso le rispettive progettualità, ILRS e Artemis, fungendo da aggregatori per altri Paesi.
In tema di sicurezza orbitale, a seguito dei danni provocati da una collisione a catena in orbita bassa avvenuta nel 2032, innescata da una crisi geopolitica in un contesto di grave affollamento delle orbite, le principali potenze spaziali hanno siglato un Patto globale per la sicurezza orbitale che standardizza i tempi minimi di notifica delle manovre.
Il settore industriale si è consolidato attorno a un numero ristretto di integratori di "sistemi di sistemi": pochi operatori di mega-costellazioni, pochi operatori di servizi di lancio, aziende specializzate nella protezione cibernetica e di guerra elettronica e nella logistica in orbita. Gli Stati definiscono la direzione strategica delle politiche spaziali, ma gli attori privati dettano il ritmo delle innovazioni e del relativo uso commerciale. Le società capaci di produrre mega-costellazioni dispiegano risorse di "rimozione dei detriti", tecnologie con capacità dual-use e funzioni da sentinelle difensive.
Circa la militarizzazione dello spazio, prevalgono gli effetti reversibili: le azioni cinetiche generatrici di detriti sono rare, non perché i conflitti siano diminuiti ma perché sono strategicamente autolesioniste. Dominano lo scenario interferenze elettroniche, manovre di prossimità su assetti orbitali e sabotaggi nei confronti delle filiere spaziali. L'Europa esegue periodicamente stress test spaziali per convalidare la ridondanza tra le pipeline di comunicazione satellitare, navigazione e ISR.
Sulle tecnologie spaziali, l'intelligenza artificiale è onnipresente, mentre la tecnologia quantistica è selettiva e strategica. L'IA è integrata in tutte le operazioni spaziali, dall'assegnazione dei compiti all'autonomia di bordo, al rilevamento delle anomalie. Il progresso più prezioso è la resilienza abilitata dall'IA, in quanto le costellazioni riconfigurano orbite in pochi minuti in caso di necessità. La tecnologia quantistica, invece, è riservata a comunicazoni e crittografia ad alta sicurezza. Per l'esplorazione del sistema solare è la logistica cislunare a costituire lo snodo strategico delle missioni con e senza equipaggio.
In questo scenario, l'Italia può consolidare il proprio ruolo strategico nel settore spaziale in due modi paralleli e non confliggenti. Da un lato, rinunciando all'irraggiungibile obiettivo del controllo totale della catena di approvvigionamento e di una "piena sovranità tecnologica", il nostro Paese potrà

investire maggiori risorse e professionalità all'interno dell'Agenzia Spaziale Europea (ESA) e nelle sinergie con altre agenzie spaziali: NASA, JAXA (Agenzia spaziale giapponese) e CSA (Agenzia spaziale canadese). Dall'altro, potrebbe divenire un efficiente e indispensabile produttore di nodi di interoperabilità high-tech, sfruttando la specializzazione in moduli pressurizzati (compreso il supporto alla vita per la futura esplorazione umana della Luna), veicoli cargo per rifornimento delle stazioni spaziali e servizi/capacità di distribuzione quantistica delle chiavi (Quantum Key Distribution - QKD). In un'Europa non più strettamente dipendente dal supporto degli USA, l'approccio italiano "a doppio binario" evolverebbe in una "strategia ponte" che utilizza asset spaziali per connettere architetture tecniche e politiche tra Stati Uniti ed Europa.

LO SPAZIO VERSO IL 2035

Per ciascuno dei quattro principali driver che caratterizzano lo spazio e che disegnano il suo possibile sviluppo al 2035 sono stati identificati alcuni indicatori di tendenza. Si tratta di serie storiche, valutazioni e stime, tratte da fonti aperte, utilizzate nel processo analitico a supporto dell'attività di validazione dello scenario delineato con il ricorso alla GenAI.

DRIVER 1 Le dinamiche di competizione tra i principali attori statuali

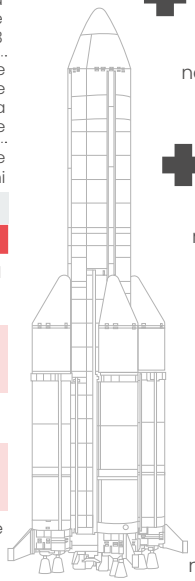
La nuova corsa alla luna

Artemis		International Lunar Research Station (ILRS)
STATI UNITI	Paese promotore	CINA
Programma lanciato nel 2017, aperto alla collaborazione internazionale attraverso gli "Artemis Accords"	Sintesi	Programma nato dalla collaborazione con la Russia; aperto alla collaborazione internazionale nel 2023
Presenza umana sostenibile sulla Luna con stazione orbitante e base sulla superficie, anche in vista dell'esplorazione umana di Marte	Obiettivo	Rete di infrastrutture nell'orbita e sulla superficie della Luna per la sua esplorazione multi-disciplinare, con la prospettiva una presenza umana stabile
61 Paesi	Adesione	17 Paesi e oltre 50 tra enti di ricerca e organizzazioni

Tabella di marcia

Missione	Data	Attività	Missione	Data	Attività
Artemis I	16 nov 2022	Test di volo senza equipaggio	Chang'e 7	2026	Esplorazione robotica del Polo Sud lunare per studiare ambiente e risorse
Artemis II	apr 2026	Flyby lunare con equipaggio	Chang'e 8	2029	Validazione di tecnologie per lo sfruttamento di risorse in superficie
Artemis III	entro il 2028	Allunaggio con equipaggio, al Polo Sud	n.a.	entro il 2030	Allunaggio con equipaggio, al Polo Sud
Artemis IV	n.a.	Realizzazione della stazione in orbita (Gateway) e attività umana sulla superfice	n.a.	2035	Costruzione di una stazione di base sulla superficie lunare, al Polo Sud
Artemis V	n.a.	Operazioni su stazione lunare e su stazione in orbita	n.a.	2050	Network lunare completo: stazione orbitante e sulla superficie per missioni di lunga durata

Vent'anni di lanci spaziali
dal 2005 al 2025



+1.400%
lanci effettuati dagli Stati Uniti nel 2025 (180) rispetto al 2005 (12)

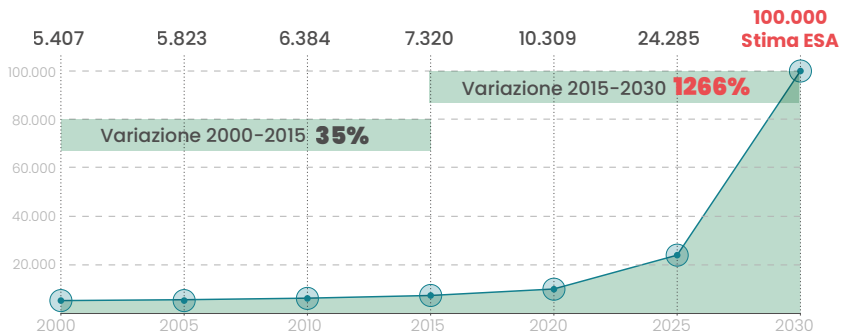
+1.760%
lanci effettuati dalla Cina nel 2025 (93) rispetto al 2005 (5)

+60%
lanci effettuali dall'Europa nel 2025 (8) rispetto al 2005 (5)

-35%
lanci effettuali dalla Russia nel 2025 (17) rispetto al 2005 (26)

DRIVER 2 La militarizzazione e i rischi di sicurezza nell'orbita terrestre

Trent'anni di satelliti lanciati nello spazio, dal 2000 alle stime per il 2030



La sicurezza delle orbite e la space debris

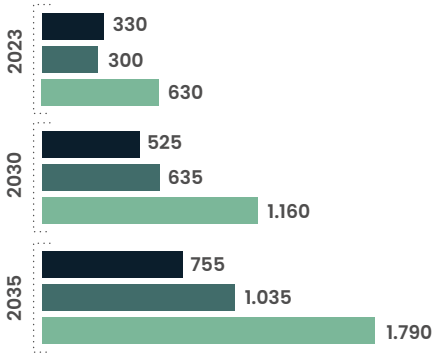
dati ESA aggiornati a ottobre 2025

7.070	razzi lanciati nello spazio dal 1957
43.510	oggetti nell'orbita terrestre monitorati dalle reti di sorveglianza spaziale
23.770	satelliti condotti in orbita dal 1957, di cui 15.860 ancora in orbita
54.000	oggetti nell'orbita terrestre più grandi di 10 centimetri (stima)
1,2 oltre mln	di oggetti nell'orbita terrestre tra 1 cm e 10 cm* (stima)

** Si tratta di oggetti in grado di causare danni "catastrofici"*

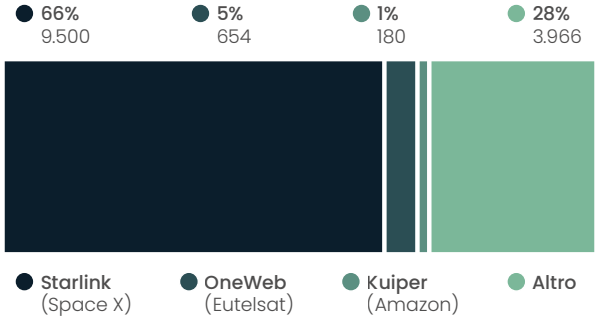
DRIVER 3 La commercializzazione dello spazio e l'affermazione dei grandi attori privati

Stime di crescita della Space Economy (in miliardi di dollari)



- **Applicazioni dirette**
  Si tratta di servizi che si applicano direttamente entro il perimetro del settore spaziale, ad esempio per i servizi lancio, la realizzazione o la gestione di satelliti, le infrastrutture di terra.
- **Applicazioni indirette**
  Si tratta dell'applicazione di tecnologie e servizi spaziali ad altri settori: logistica, trasporti, food & beverage, difesa, media e intrattenimento.
- Totale

I satelliti operativi nell'orbita terrestre per costellazione



DRIVER 4 L'applicazione delle tecnologie dirompenti

500 miliardi di dollari

il peso dell'adozione di tecnologie innovative sullo scenario base di crescita della Space Economy, pari a 1.790 miliardi di dollari nel 2035 (ricavi derivanti da applicazioni spaziali). Secondo le stime di McKinsey & Company, rispetto allo scenario in questione, la crescita può arrivare a 2.300 miliardi di dollari in caso di riduzione dei costi di accesso allo spazio e di migliore gestione dei dati spaziali grazie all'efficace adozione di tecnologie dirompenti, in primis intelligenza artificiale e cloud computing.

2027

l'anno previsto per il lancio dei primi due satelliti prototipali del Project Suncatcher, il progetto di Google per il lancio in orbita di data center dedicati all'intelligenza artificiale che sfrutterebbero l'energia solare. Altri grandi attori privati hanno annunciato progettualità simili, a testimonianza della concreta prospettiva di vedere, tra qualche anno, un ecosistema IT spaziale, riducendo latenza e dipendenza dalla Terra.

SCENARI DI CONFLITTO RUSSIA-NATO

SCENARI DI CONFLITTO RUSSIA-NATO

Nota metodologica

La base informativa è costituita da documenti selezionati dagli analisti e pubblicati da autorevoli centri di ricerca sulle capacità delle Forze Armate russe e su ulteriori fattori di tipo economico, politico e sociale della Federazione Russa. Gli analisti hanno fornito degli assunti sulla base dei quali il LLM ha proposto tre scenari alternativi e indipendenti di un attacco russo convenzionale verso uno o più Paesi NATO entro il 2030. Su ulteriore input degli analisti, il LLM ha altresì fornito: una finestra temporale di accadimento, i connessi fattori circostanziali abilitanti, le forze e gli assetti impiegati e gli obiettivi tattici perseguiti dalla Russia in ciascuno scenario.

SCENARIO 1
Intervento ibrido su Narva

PROBABILITÀ VALIDATA DAGLI ANALISTI

QUANDO 2028 | DOVE Narva (Estonia)

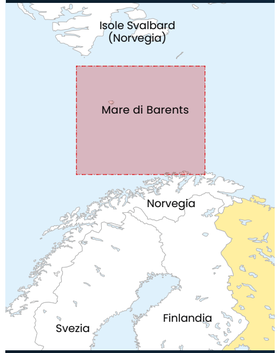
SCENARIO 2
Blitz nel corridoio Suwalki

PROBABILITÀ VALIDATA DAGLI ANALISTI

QUANDO 2029 | DOVE Corridoio di Suwalki

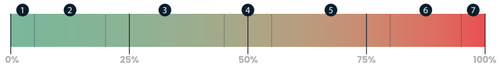
SCENARIO 3
Operazione marittima contro la Norvegia

PROBABILITÀ VALIDATA DAGLI ANALISTI



QUANDO 2030 | DOVE Mare di Barents

Scala delle probabilità usata



COME SI LEGGE

1. QUASI NESSUNA PROBABILITÀ *(almost no chance)*
2. MOLTO IMPROBABILE *(very unlikely)*
3. IMPROBABILE *(unlikely)*
4. QUASI EQUIPROBABILE *(roughly even chance)*
5. PROBABILE *(likely)*
6. MOLTO PROBABILE *(very likely)*
7. QUASI CERTO *(almost certain)*

SCENARIO 1 - Intervento ibrido su Narva

Fattori abilitanti: campagna presidenziale USA; possibile rimodulazione impegno truppe USA in Europa; cessate il fuoco in Ucraina molto fragile.

Pretesto: 1) Tentativo del Cremlino, poi fallito, di istituire un gruppo di mediazione internazionale per risolvere le violazioni contro "cittadini russi"; 2) Intervento russo a loro tutela.

Modalità di attacco
- attacchi preparatori cibernetici a infrastrutture critiche;
- campagne di propaganda su social media per creare disordini;
- restrizioni commerciali e dazi su residuo commercio bilaterale;
- infiltrazioni di forze speciali russe;
- intervento limitato di forze regolari russe.

Obiettivi: Instaurare una zona "grigia" sotto influenza russa a Narva senza provocare un'escalation con le forze NATO. Test di coesione della risposta NATO. Posizioni acquisite in Estonia sono utili a ottenere maggiori concessioni in Ucraina.

Possibili conclusioni: Il Cremlino prova a trasformare la città di Narva in "area contesa sotto mandato internazionale".

SCENARIO 2 - Blitz nel corridoio Suwalki

Fattori abilitanti: completata la ricostituzione militare russa; stimato vantaggio su modernizzazione Forze NATO; totale subordinazione delle Forze bielorusse agli obiettivi Russi.

Pretesto: Attivazione da parte di Minsk del trattato di difesa congiunta con la Russia sulla scorta di "presunte prossime aggressioni" da parte NATO.

Modalità di attacco
- impiego di mezzi meccanizzati da Kaliningrad e Grodno (Bielorussia);
- creazione di forze speciali congiunte russo-bielorusse;
- attacchi cibernetici contro snodi ferroviari;
- attacchi con missili a corto raggio e droni contro difese NATO posizionate in vicinanza.

Obiettivi: Creare un collegamento via terra e compromettere la connessione diretta dei Paesi Baltici con la Polonia.

Possibili conclusioni: Mosca si ritira in cambio di concessioni ulteriori sulla questione ucraina o con garanzie di ritiro di assetti NATO dal territorio baltico.

SCENARIO 3 - Operazione marittima contro la Norvegia

Fattori abilitanti: ammodernamento della Flotta del Nord russa; test della deterrenza USA sul fronte artico.

Pretesto: Operazione navale russa di interdizione marittima nel Mare di Barents. Disputa relativa alla delimitazione e ai diritti di sfruttamento delle zone marittime intorno alle isole Svalbard.

Modalità di attacco
- esercitazioni navali vicino a piattaforme petrolifere e cavi sottomarini norvegesi;
- interdizione attiva dell'area con sorvoli provocatori e blocco rotte commerciali chiave;
- manifestazioni a Murmansk e Arkhangelsk (Russia) per amplificare la narrazione di difesa dell'Artico.

Obiettivi: Cementare la supremazia russa nell'Artico e screditare la capacità di difesa della NATO sul fianco settentrionale.

Possibili conclusioni: Mosca congela la situazione con una dichiarazione unilaterale di controllo su alcune aree della ZEE norvegese. Tenta di rinegoziare il Trattato delle Svalbard, acquisendo anche il diritto a condurre esercitazioni militari.

Analisi del tono delle notizie relative ai rapporti bilaterali tra la Russia e quattro Paesi NATO (Estonia, Lituania, Norvegia e Polonia)

La sperimentazione integra l'esercizio sugli scenari di attacco convenzionale da parte della Russia alla NATO entro il 2030 con un'analisi delle notizie pubblicate nel periodo ottobre-dicembre 2025 riguardo le relazioni tra la Russia e ciascuno dei quattro Paesi potenzialmente vittima di incursioni russe, come rilevato nei tre scenari precedenti (Estonia, Lituania, Norvegia e Polonia).

A tale scopo, si è fatto ricorso a GDELT – un database pubblico che raccoglie e analizza migliaia di notizie da fonti aperte in oltre 100 lingue – selezionando le fonti con un valore pari o minore a -7 nel punteggio Goldstein (indicatore numerico che misura il livello di cooperazione/conflitto associato agli eventi riportati nelle notizie, con il valore minimo, ossia più conflittuale, pari a -10).

Mediante un'analisi quantitativa di articoli reperiti nel periodo in esame, sono stati identificati:

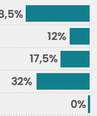
1. i principali temi che, agli occhi dei mezzi di informazione, sono connessi a narrazioni in cui dominano temi conflittuali (punteggio Goldstein uguale o minore a -7) tra la Russia ed i cinque Paesi presi in esame;
2. i principali temi che generano reazioni conflittuali in ogni singola relazione bilaterale.

Le risultanze potenziano l'attività degli analisti OSINT e gli esperti di materia tesa a identificare verso quali narrazioni focalizzare la ricerca informativa in questi Paesi, per individuare segnali di escalation nelle relazioni bilaterali, anche al fine di una più corretta costruzione di partenza e ricalibratura successiva di scenari previsionali.

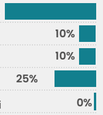
I cinque temi che alimentano di più la conflittualità retorica tra la Russia ed Estonia, Lituania, Norvegia e Polonia sono:

1. Incursioni di droni/violazioni spazio aereo;
2. Sabotaggi;
3. Incidenti di natura securitaria ai confini;
4. Escalation diplomatica (es. convocazione dell'Ambasciatore; proteste ufficiali);
5. Attacchi o minacce di attacchi cibernetici.

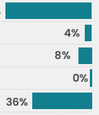
Principali temi che alimentano la conflittualità retorica tra la Russia e l'Estonia



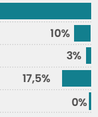
Principali temi che alimentano la conflittualità retorica tra la Russia e la Lituania



Principali temi che alimentano la conflittualità retorica tra la Russia e la Norvegia



Principali temi che alimentano la conflittualità retorica tra la Russia e la Polonia



SCENARI DI CONFLITTO RUSSIA-NATO

Il seguente test di GenAI è stato condotto tenuto conto della frequenza crescente di dichiarazioni pubbliche da parte di Autorità politiche e di Direttori di Servizi Intelligence occidentali su un possibile attacco convenzionale russo contro Paesi NATO nei prossimi anni.

Il supporto all'analisi previsionale si è materializzato nella "generazione" di tre scenari alternativi e indipendenti che includessero anche fattori abilitanti, pretesto, modalità di attacco, obiettivi e possibili conclusioni dell'azione russa.
Le probabilità di accadimento per ciascuno scenario sono state validate dagli analisti.

CRIPTOVALUTE: EFFETTI DI UN IPOTETICO SCENARIO DI CRISI

CRIPTOVALUTE: EFFETTI DI UN IPOTETICO SCENARIO DI CRISI

La simulazione è un esercizio sperimentale di applicazione di strumenti IA per identificare eventuali canali di trasmissione di una crisi nel mercato delle criptovalute al resto del sistema finanziario, con particolare attenzione ai titoli di Stato dei Paesi europei. La simulazione parte dall'assunto di una crisi nel settore delle criptovalute.

Trigger: eventi che innescano il meccanismo di trasmissione della crisi delle criptovalute al sistema finanziario tradizionale.

TRIGGER A — Shock di mercato

PROBABILITÀ VALIDATA DAGLI ANALISTI: ALTA

A fronte dell'aumento dei costi di finanziamento sui mercati, i fondi d'investimento ricevono richieste di fornire ulteriori garanzie delle proprie posizioni in criptovalute e devono trovare liquidità nell'immediato. Conseguentemente, i fondi iniziano a vendere i titoli di Stato in portafoglio.

TRIGGER B — Crisi di fiducia

PROBABILITÀ VALIDATA DAGLI ANALISTI: MEDIA

A seguito di una «crisi di fiducia» verso il mondo delle criptovalute (ad es. dopo il fallimento di una stablecoin affermata), si diffonde sui mercati un sentimento di panico che aumenta l'avversione al rischio degli investitori. In tale contesto, i titoli di Stato dei Paesi della periferia dell'eurozona vengono percepiti come più rischiosi, facendo crescere il premio per detenerli.

TRIGGER C — Shock regolatorio

PROBABILITÀ VALIDATA DAGLI ANALISTI: BASSA

Dopo che un Paese/Organizzazione di Stati economicamente rilevante introduce divieti di detenzione o di transazione in criptovalute, verso queste ultime si riduce la fiducia degli investitori, determinando un "effetto panico" che porta i fondi di investimento a liquidare i titoli di Stato in portafoglio.

Time-Lapse (12 mesi). Fasi e meccanismo di trasmissione

AVVIENE ALMENO UNO DEI TRIGGER (A, B o C)

FASE 1 — 1 SETTIMANA

- I fondi iniziano a vendere titoli di Stato

FASE 2 — 2-4 SETTIMANE

- I compratori di titoli di Stato si fanno più cauti e gli intermediari non riescono ad assorbire tutto il flusso.
- Le aste del Tesoro diventano più delicate e prende forma il rischio di un "buyers' strike" (pochi partecipanti o domanda debole).

FASE 3 — MESE 2

- Lo shock si trasferisce ai risparmiatori: le perdite sulle criptovalute riducono la ricchezza percepita e cresce il bisogno di liquidità.
- Una parte delle famiglie inizia a vendere anche titoli di Stato per fare cassa.

FASE 4 — MESI 3-6

- La tensione entra nei sistemi bancari: con i titoli di Stato in calo, le banche diventano più prudenti e restringono il credito, soprattutto verso le PMI.
- Ne deriva un credit crunch che frena investimenti e consumi, aumentando il rischio di recessione e peggiorando la percezione di sostenibilità del debito pubblico.

FASE 5 — MESI 6-9

- La crisi arriva al picco: le ipotesi di downgrade diventano centrali perché potrebbero innescare ulteriori vendite da parte dei fondi.
- Lo spread si amplia, cresce la pressione politica in Europa e si apre un confronto su condizioni e strumenti di sostegno.

FASE 6 — MESE 9-12

- La BCE interviene con acquisti mirati dei titoli di Stato. L'intervento stabilizza il mercato e riporta fiducia, riducendo lo spread.
- La fase acuta lascia un'eredità: rendimenti strutturalmente più alti, banche conservative e una crescita più debole.

PROIEZIONI FUTURE DEI FLUSSI MIGRATORI

PROIEZIONI FUTURE DEI FLUSSI MIGRATORI

Nel corso del 2026, l'evoluzione dei flussi di migrazione irregolare verso l'Italia può essere delineata attraverso quattro possibili scenari, differenziati per intensità, origine dei flussi e tenuta dei sistemi di controllo nei Paesi di partenza e transito.

NOTA METODOLOGICA

Al modello dell'IA sono stati forniti dati ufficiali relativi ai flussi migratori irregolari verso l'Italia nel periodo gennaio 2020 – dicembre 2025, comprendenti i volumi di sbarco registrati e la composizione per nazionalità dei migranti giunti sul territorio nazionale. Inoltre, documenti ufficiali di fonti istituzionali, nazionali e internazionali, hanno contribuito a contestualizzare il fenomeno. L'intero processo è stato sottoposto a supervisione e validazione da parte degli analisti. L'output consiste in quattro scenari alternativi, ciascuno con una percentuale di probabilità di inveramento. L'applicazione di algoritmi statistici classici su serie storiche ha permesso l'elaborazione di una previsione per il 2026, che risulta compatibile con lo scenario più probabile.

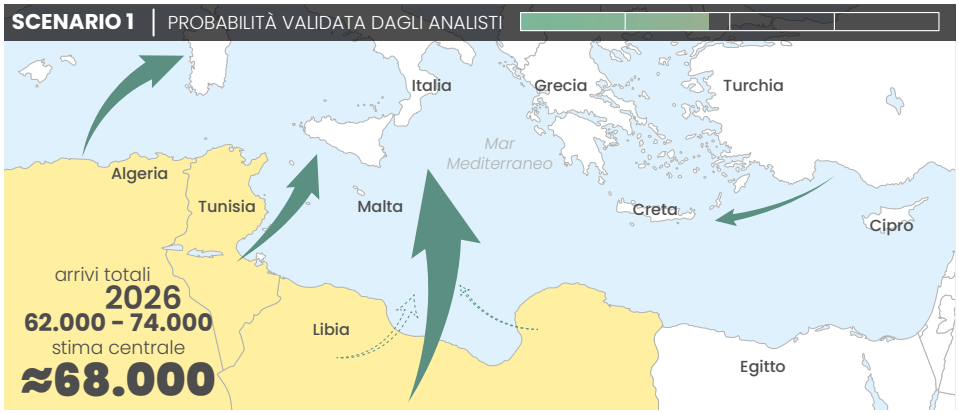
PRIMO SCENARIO

Nel primo scenario, riconducibile a una situazione di "pressione gestita", si prevede una sostanziale continuità con le dinamiche osservate nel biennio 2024–2025.

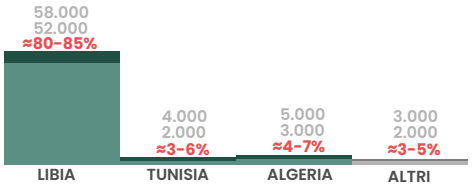
La Libia rimane il principale punto di origine delle partenze, con un ruolo predominante della Tripolitania sotto il Governo di Unità Nazionale (GNU) e una partecipazione più limitata della Cirenaica. L'assetto libico resta frammentato ma funzionale: il Memorandum Italia–Libia, rinnovato nel novembre 2025, sostiene operazioni di intercettazione della Guardia Costiera libica, mantenute intorno al 60–65%. Tale equilibrio è tuttavia precario, poiché riallineamenti tra milizie o tensioni tra GNU e Cirenaica potrebbero rapidamente ridurre la capacità operativa di quella Guardia Costiera, rappresentando il principale rischio geopolitico verso scenari di maggiore pressione.

La Tunisia mantiene un profilo contenuto

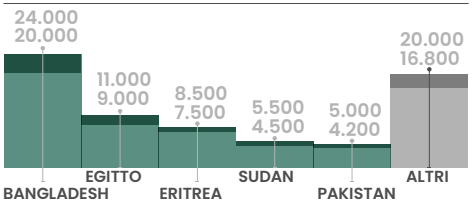
Scenario base - "pressione gestita"



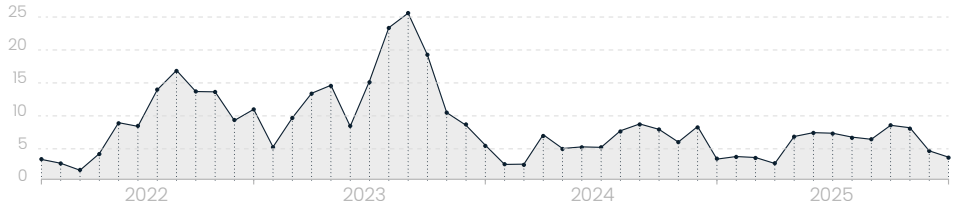
Volumi per paese di partenza



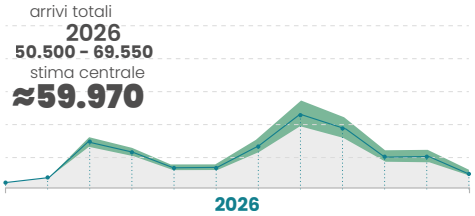
Arrivi per nazionalità



Andamento migratorio dal 2022 al 2025

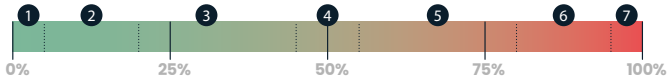


Previsione statistica 2026



È stata fatta una previsione dei flussi migratori mensili utilizzando algoritmi statistici classici a cui sono state fornite le serie temporali storiche degli arrivi dal gennaio 2022 al dicembre 2025. Le risultanze tracciano un andamento degli arrivi degli immigrati irregolari in Italia nel corso del 2026 marcatamente compatibile con il "primo scenario – pressione gestita" delineato dall'IA.

Scala delle probabilità usata



COME SI LEGGE

1. QUASI NESSUNA PROBABILITÀ *(almost no chance)*
2. MOLTO IMPROBABILE *(very unlikely)*
3. IMPROBABILE *(unlikely)*
4. QUASI EQUIPROBABILE *(roughly even chance)*
5. PROBABILE *(likely)*
6. MOLTO PROBABILE *(very likely)*
7. QUASI CERTO *(almost certain)*

grazie al rafforzamento dell'enforcement securitario e alla cooperazione formalizzata nel Memorandum UE–Tunisia, che riduce sensibilmente i flussi rispetto al 2023 senza chiudere completamente la rotta. Questa contenzione resta vulnerabile a shock economici: un deterioramento finanziario potrebbe compromettere rapidamente i meccanismi di controllo.

L'Algeria emerge come corridoio di transito secondario, senza configurarsi come rotta autonoma di rilievo. In assenza di accordi strutturati con l'UE nel 2026, il transito, nella forma di traversate dirette e movimenti verso le aree di partenza tunisine, è tollerato informalmente, distinguendosi da modelli di controllo più espliciti.

L'Egitto opera principalmente come paese di origine e transito. La crisi macroeconomica resta grave ma cronica; il Partenariato Strategico UE–Egitto del 2024 contribuisce a una stabilizzazione parziale, limitando impennate

improvvise senza eliminare i fattori di spinta. I Paesi di origine mostrano dinamiche geopolitiche differenziate: la guerra in Sudan prosegue senza regionalizzarsi, mantenendo alti livelli di sfollamento ma con incrementi migratori graduali nel 2026; Bangladesh e Pakistan affrontano pressioni significative, ma in assenza di shock sistemici si prevede una continuità dei flussi.

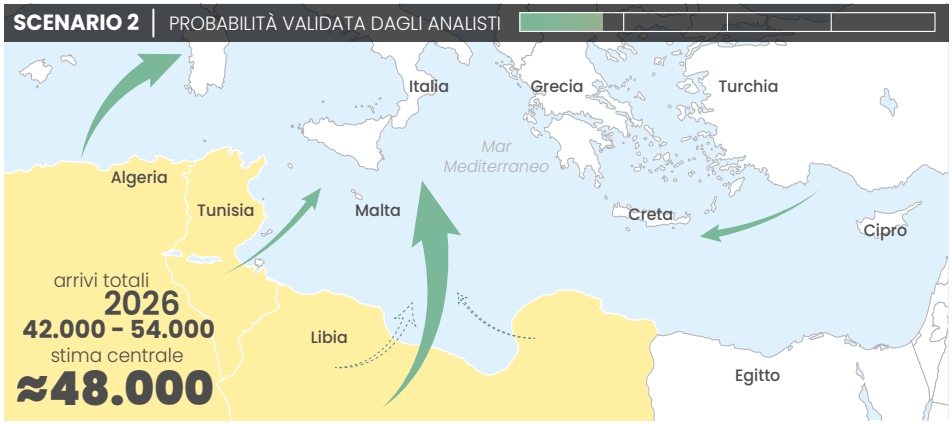
A livello europeo, l'avvio dell'implementazione del Patto UE sulla migrazione e l'asilo introduce elementi di maggiore coordinamento procedurale, ma non determina nell'immediato una trasformazione strutturale delle dinamiche di flusso. Gli strumenti di esternalizzazione e di gestione avanzata delle frontiere, inclusi i meccanismi bilaterali di supporto e rimpatrio, rappresentano più fattori di contenimento incrementale che di deterrenza. Nel complesso, la pressione migratoria resta significativa ma gestibile, pur in un contesto di vulnerabilità geopolitiche suscettibili di rapidi mutamenti.

SECONDO SCENARIO

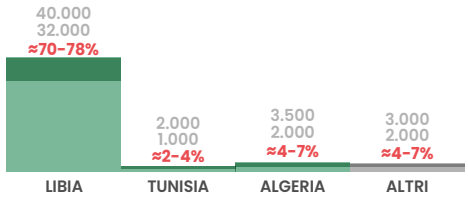
Il secondo scenario, definito "di flussi contenuti", delinea un contesto di rafforzamento complessivo delle capacità di controllo degli attori statali in un quadro regionale relativamente stabile, sostenuto da un'architettura geopolitica più complessa rispetto allo scenario base.

In Libia, il Memorandum Italia–Libia viene potenziato politicamente e operativamente, con un aumento dei mezzi e un miglior coordinamento che innalza i tassi di intercettazione fino al 70–80%. Parallelamente, prende forma un assetto trilaterale Turchia–Italia–Libia che estende il controllo lungo l'intera catena del traffico, interrompendo le reti

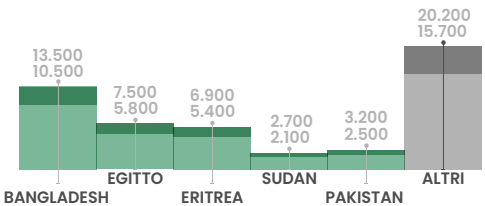
Scenario di bassa pressione migratoria - "flussi contenuti"



Volumi per paese di partenza



Arrivi per nazionalità

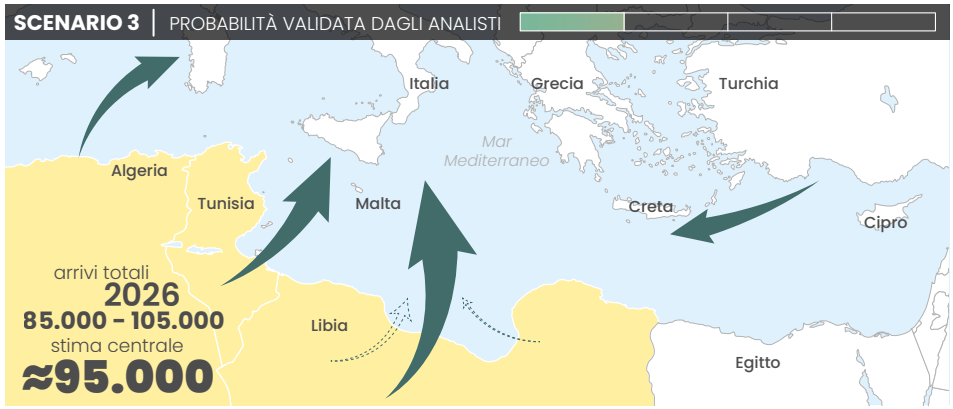


"verticalmente integrate" dai Paesi asiatici. Questo segna un passaggio da un contenimento "gestito" a uno più attivo e sistemico.
La Tunisia scende a minimi storici in termini di partenze grazie a un enforcement securitario credibile sostenuto da una stabilizzazione macroeconomica supportata da UE e FMI, che rafforza la legittimità interna delle politiche di controllo e riduce la tolleranza tacita delle partenze.
L'Egitto beneficia di un analogo ancoraggio macroeconomico tramite il Partenariato Strategico UE, che rafforza la capacità di controllo e riduce gli incentivi al transito informale verso la Libia.
L'Algeria non evolve verso un ruolo di rilievo, con flussi che rimangono di limitata entità: pur in assenza di accordi formali, il rafforzamento dei controlli regionali riduce l'attrattività del transito.
Sul piano regionale, il contesto è segnato da una stabilizzazione deliberata dei conflitti: una de-escalation parziale in Sudan attenua le spinte migratorie verso Egitto e Libia, pur senza risolvere il conflitto.
A livello UE, l'applicazione del Patto sulla migrazione e l'asilo comporta ricollocamenti e finanziamenti che alleviano la pressione sull'Italia. Il protocollo Italia-Albania supera i contenziosi legali e opera su scala significativa, funzionando come deterrente credibile.Nel complesso, le altre rotte restano marginali e il quadro migratorio si configura come moderato, con una pressione sensibilmente ridotta.

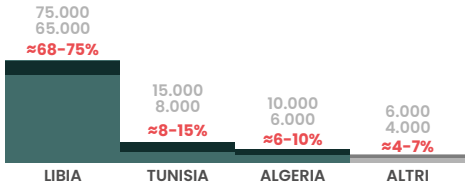
TERZO SCENARIO

Il terzo scenario, definito "di crisi convergenti", delinea un netto peggioramento del contesto regionale, determinato dalla sovrapposizione di sviluppi geopolitici negativi.
In Libia si registra un indebolimento strutturale delle capacità di controllo, con un'accentuata frammentazione politica tra Tripolitania e Cirenaica che compromette la gestione delle frontiere marittime. I tassi di intercettazione crollano dal 70-80% al 40-50% a causa della riduzione del supporto europeo, dei vincoli politici alla cooperazione e della competizione tra milizie costiere. Entrambe le aree diventano così generatori di flussi consistenti, con un rischio concreto di perdita del controllo costiero e di collasso statale. Nel Sudan e nel Corno d'Africa l'intensificazione dei conflitti produce nuovi grandi spostamenti forzati, alimentando un forte aumento dei flussi verso la Libia e, in parte, attraverso l'Algeria. Il conflitto diventa il principale driver della mobilità forzata verso nord.
La Tunisia riemerge come rotta alternativa a seguito di un deterioramento economico

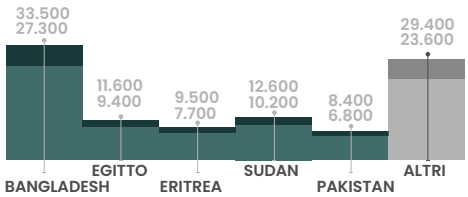
Scenario di alta pressione migratoria - "crisi convergenti"



Volumi per paese di partenza



Arrivi per nazionalità

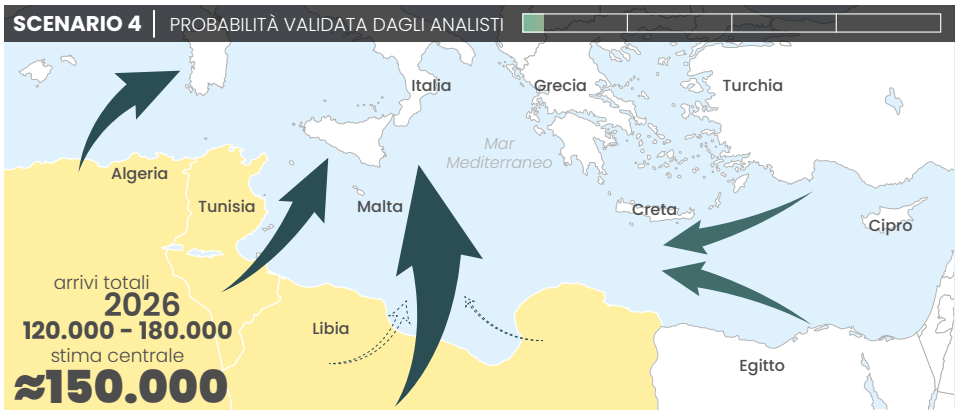


acuto, con lo stallo del programma FMI e disordini sociali che erodono la sostenibilità dell'enforcement securitario e riattivano la rotta. L'Algeria evolve da corridoio tollerato a rotta autonoma emergente, utilizzando una maggiore fuoriuscita come leva di pressione geopolitica verso UE e Italia.
L'Egitto affronta un aggravamento della crisi interna, con inflazione e tagli ai sussidi che rafforzano il suo ruolo di area di partenza verso la Libia e, marginalmente, verso il Mediterraneo centrale. In Asia, shock politici ed economici in Bangladesh e Pakistan alimentano un'impennata delle partenze lungo filiere di traffico integrate.
A livello UE, il Patto sulla migrazione e l'asilo perde coesione: gli impegni di solidarietà si riducono e l'Italia resta in larga parte isolata. Il protocollo Italia-Albania non raggiunge la scala prevista, indebolendone l'effetto deterrente. Le rotte orientali generano spillover aggiuntivi verso le zone SAR italiane. Nel complesso, la pressione migratoria risulta nettamente superiore rispetto agli altri scenari.

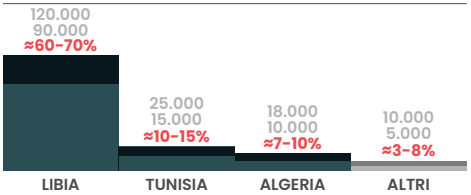
QUARTO SCENARIO

Il quarto scenario, configurato come "stress test di sistema", prospetta una fase di forte instabilità regionale segnata dal collasso simultaneo dei meccanismi di controllo e dalla co-occorrenza di eventi estremi.
In Libia, il deterioramento assume caratteri catastrofici: la ripresa della guerra civile o un'ulteriore frammentazione statale porta alla disgregazione della Guardia Costiera e al ritiro delle missioni internazionali, lasciando ampio spazio alle reti di traffico. Lo stock di oltre 800 mila migranti presenti nel Paese viene mobilitato simultaneamente da molteplici aree costiere, con un crollo quasi totale dell'interdizione alle par-

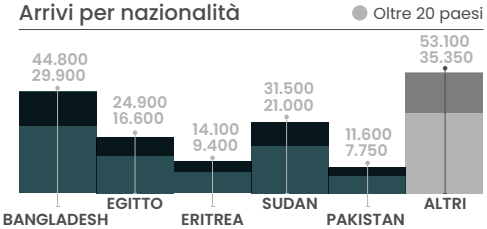
Scenario di shock - "stress test di sistema"



Volumi per paese di partenza



Arrivi per nazionalità



tenze e una situazione di vera e propria "anarchia costiera".

Nel Sudan e nel Corno d'Africa, il conflitto si regionalizza coinvolgendo paesi limitrofi, con effetti destabilizzanti anche sull'Egitto. Gli spostamenti forzati superano ampiamente le proiezioni, rendendo il 2026 una fase acuta di crisi multiterritoriale.

L'Egitto diventa epicentro di una crisi sistemica: proteste di massa e shock economici, aggravati dall'aumento dei prezzi alimentari, generano una forte emigrazione e indeboliscono il controllo delle frontiere. Il Paese rischia di trasformarsi in un'area di partenza autonoma verso l'Italia, con l'attivazione di nuove rotte.

La Tunisia registra il collasso dell'enforcement securitario, con partenze su larga scala dalle aree costiere, mentre l'Algeria evolve in una rotta strutturata e autonoma di rilievo. A questi fattori si sommano shock climatici estremi nel Sahel, nel Corno d'Africa e in Asia meridionale, che accelerano la mobilità in modo sincronizzato con i driver politici e conflittuali.

Sul piano internazionale, l'architettura di cooperazione si disgrega: la crisi UE-Turchia indebolisce il coordinamento, il Patto UE sulla migrazione e l'asilo fallisce e gli Stati membri rinazionalizzano le risposte, fino alla possibile reintroduzione di controlli interni all'area Schengen. Nel complesso, la pressione migratoria diventa eccezionalmente elevata e multidirezionale, trasformando la crisi migratoria in una crisi sistemica geopolitica, umanitaria e politica per l'Europa e il Mediterraneo.

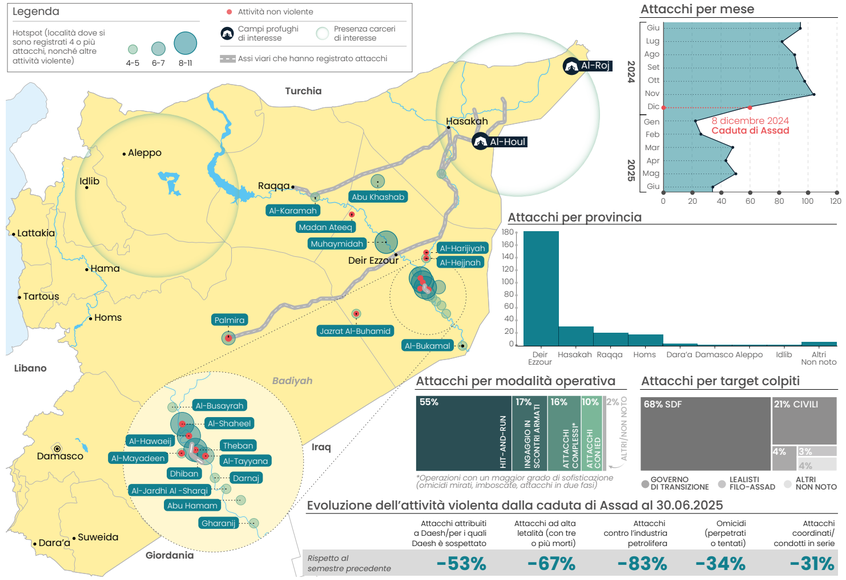
DAESH IN SIRIA DALLA CADUTA DI ASSAD

DAESH IN SIRIA DALLA CADUTA DI ASSAD

Nota metodologica

La sperimentazione ha consentito l'elaborazione di un'infografica sulla minaccia al giugno 2025 (in questa pagina) e di uno scenario previsionale a 12 mesi - luglio 2026 - corredato da indicatori strategici e tattico-operativi (esempi tratti da scenario e indicatori riportati nella pagina a destra). L'infografica si basa su dati estrapolati da fonti aperte selezionate. Il numero delle attività violente è speculativo, viste le diverse metodologie adottate nella raccolta dati e la tendenza di Daesh a rivendicare meno attacchi rispetto a quelli perpetrati. L'infografica riporta anche attacchi dei quali Daesh è solo sospettata.

Stato della minaccia posta da Daesh al giugno 2025 (periodo di riferimento 08 dicembre 2024- 30 giugno 2025)



Attacchi per mese

Attacchi per provincia

Attacchi per modalità operativa

*Operazioni con un maggior grado di sofisticazione (omicidi mirati, imboscate, attacchi in due fasi)

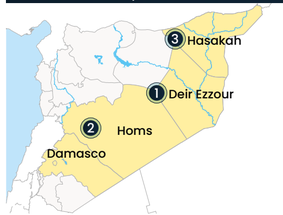
Attacchi per target colpiti

Evoluzione dell'attività violenta dalla caduta di Assad al 30.06.2025

	Attacchi attribuiti a Daesh/per i quali Daesh è sospettato	Attacchi ad alta letalità (con tre o più morti)	Attacchi contro l'industria petrolifera	Omicidi (perpetrati o tentati)	Attacchi coordinati/ condotti in serie
Rispetto al semestre precedente	**-53%**	**-67%**	**-83%**	**-34%**	**-31%**

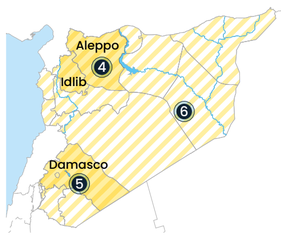
Esempi tratti dallo Scenario previsionale a 12 mesi (luglio 2026)

Vettore 1: Minaccia posta da Daesh



1. Attacchi opportunistici e attività non violente rimangono proiettate su Deir Ezzour.
2. Tentativi di espansione oltre le tradizionali aree di influenza, incluso verso la Capitale.
3. Probabili azioni di disturbo dall'esterno nei confronti dei campi profughi e delle carceri di Hasakah, dove sono detenuti affiliati Daesh, con possibili fughe opportunistiche; poco probabili assalti ad alto impatto.

Vettore 2: Minaccia posta da gruppi jihadisti diversi da Daesh



4. La componente dei Foreign Terrorist Fighters più estremista, nel prendere le distanze da Al-Sharaa, tenta di imporsi su base locale come autorità di governance.
5. Defezioni dalle strutture statali centrali che fanno capo a Damasco da parte dei miliziani di fazioni jihadiste formalmente disciolte.
6. Panorama filo-qaedista frammentato, con profili organizzativi e logistici deboli.

Vettore 3: Proiezione della minaccia verso l'Europa e l'Italia

7. Fughe di militanti Daesh da prigioni e campi profughi, facilitate dall'abbandono dei siti da parte del personale di sorveglianza o da fenomeni corruttivi.
8. Attivazione di reti di supporto logistico nei Paesi di transito verso l'Europa.
9. Sostegno alla facilitazione (ma non alla direzione) da remoto di attacchi compiuti da individui o reti già presenti in Europa.

Esempi tratti dagli Indicatori strategici e tattico-operativi

La Tabella Indicatori consente di accertare se l'attuale decorso della minaccia terroristica stia confermando lo "Scenario Previsionale a luglio 2026" (livello 0), oppure si stia discostando dallo stesso in senso peggiorativo (livello 1 e livello 2).

Vettore 1

Piano strategico

Livello di attività violenta di Daesh

MACRO INDICATORE

Piano tattico-operativo

INDICATORI DI CONFERMA — LIVELLO 0

Il numero di attacchi resta nell'intervallo di riferimento osservato nei primi mesi post-Assad con aumenti temporanei e circostanziati dei livelli di attività violenta. Gli attacchi complessi rimangono il 20% circa del totale, e in netta minoranza rispetto a quelli *hit-and-run*.

INDICATORI DI ESCALATION — LIVELLO 1

Il numero di attacchi aumenta con costanza rispetto all'intervallo di riferimento. Gli attacchi complessi aumentano. Emergono tentativi di coordinamento tra cellule per operazioni da compiere in più di una provincia.

INDICATORI DI GRAVE ESCALATION — LIVELLO 2

Il numero di attacchi aumenta in modo rilevante rispetto all'intervallo di riferimento. Gli attacchi complessi sono frequenti e coordinati. Emergono pianificazioni di una o più campagne offensive coordinate in più di una provincia.

Vettore 2

Piano strategico

Rapporto fra Governo di Transizione (GT) e altre fazioni jihadiste precedentemente anti Assad

MACRO INDICATORE

Piano tattico-operativo

INDICATORI DI CONFERMA — LIVELLO 0

Evidenze di discriminazione verso le minoranze etnico-religiose nel reclutamento e nella gestione degli apparati di sicurezza da parte dei Ministeri della Difesa e dell'Interno siriani.

INDICATORI DI ESCALATION — LIVELLO 1

Esclusione ripetuta e diffusa di specifiche etnie/confessioni religiose da unità militari o di sicurezza del GT o da posizioni amministrative di rilievo.

INDICATORI DI GRAVE ESCALATION — LIVELLO 2

Esclusione sistematica di specifiche etnie/confessioni religiose da unità militari o di sicurezza del GT o da posizioni amministrative di rilievo.

Vettore 3

Piano strategico

Tracciabilità dei miliziani jihadisti

MACRO INDICATORE

Piano tattico-operativo

INDICATORI DI CONFERMA — LIVELLO 0

Evidenze di combattenti attivi in possesso di documenti autentici ma riportanti generalità false.

INDICATORI DI ESCALATION — LIVELLO 1

Segnalazioni di discrepanze tra identità note alle intelligence occidentali e nuove generalità dichiarate da soggetti sospettati di aver condotto operazioni in Siria.

INDICATORI DI GRAVE ESCALATION — LIVELLO 2

Assunzione di posizioni di leadership da parte di individui noti alle intelligence occidentali con generalità differenti da quelle rivendicate.

SCENARIO PREVISIONALE A LUGLIO 2026

La sperimentazione sull'utilizzo della GenAI ha in questo caso riguardato lo stato e l'evoluzione della minaccia jihadista in Siria e le possibili proiezioni verso l'Europa e l'Italia.

Tre i prodotti elaborati:

1. Un'Infografica, che dà conto dell'attivismo di Daesh dalla caduta di Assad al 30 giugno 2025 e della proiezione della minaccia terroristica verso l'Italia e l'Europa.
2. Uno scenario previsionale a 12 mesi (luglio 2025 – luglio 2026), che delinea l'evoluzione ritenuta più probabile della minaccia jihadista in Siria e della sua proiezione verso l'Europa.
3. Una Tabella Indicatori, che supporta gli analisti dell'intelligence nell'individuazione dei fattori di rischio e dei segnali di escalation della minaccia rispetto a quanto ipotizzato nello scenario previsionale.