Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun Svizra

Servizio delle attività informative della Confederazione SIC

LA SICUREZZA DELLA SVIZZERA

Rapporto sulla situazione del Servizio delle attività informative della Confederazione 2026

NESSUN CESSATO ALLARME!

Care lettrici, cari lettori,

nella sua Strategia in materia di politica di sicurezza 2026, il Consiglio federale constata che la situazione di sicurezza della Svizzera si è notevolmente deteriorata. Questa valutazione si basa essenzialmente sulle informazioni fornite dal Servizio informazioni della Confederazione (SIC). Nessun cessato allarme! – questa esclamazione è la sintesi più concisa del rapporto che avete tra le mani. Allo stesso tempo il rapporto mostra l'impegno attivo del SIC per la sicurezza del nostro Paese e le prestazioni che fornisce.

Per la Svizzera, la minaccia rappresentata dalla Russia è in primo piano. La Russia porta avanti la sua guerra di aggressione contro l'Ucraina. La sua strategia di conflitto ibrido nei confronti dell'Europa sta diventando più aggressiva e la Svizzera ne è direttamente colpita. A ciò si aggiungono rivalità e tensioni di politica egemonica, incertezza sull'impegno degli Stati Uniti per la sicurezza europea, crisi e conflitti riaccesi nelle aree periferiche del continente europeo da cui hanno origine minacce terroristiche ed estremiste violente. La politica di sicurezza svizzera deve tenere conto di questo contesto di sicurezza in tutte le sue sfaccettature per proteggere la società e lo Stato.

Nella prevenzione e nella difesa in ambito di minacce di politica di sicurezza, il SIC svolge un ruolo fondamentale. Il concetto di «prima linea di difesa» non è campato in aria. Affinché il SIC possa continuare a svolgere questa funzione, ha bisogno di competenze adeguate all'evoluzione della situazione di sicurezza. La Strategia in materia di politica di sicurezza 2026 mira quindi, con le sue misure, anche a migliorare le capacità di intelligence che permettono di individuare e impedire le minacce il più precocemente possibile. L'aggiornamento di queste competenze è l'obiettivo della revisione in corso della legge federale del 2017 sulle attività informative (LAIn) che dovrà garantire che la prima linea di difesa della Svizzera regga anche in futuro.

La valutazione della situazione da parte del SIC mette in evidenza che il prezzo della nostra sicurezza e della nostra autonomia sta aumentando. «La sicurezza della Svizzera» vuole essere un contributo approfondito e prezioso a questa consapevolezza.

Serge Bavaud
Direttore del Servizio delle attività informative della Confederazione

Illustrazione 1

IN BREVE

Il contesto della politica di sicurezza e la situazione della sicurezza in Svizzera si sono notevolmente deteriorati. La Russia rimane la minaccia più grave e immediata per la sicurezza, la stabilità e la pace in Europa. A livello globale, la tendenza strategica principale è la rivalità sistemica tra Stati Uniti e Cina, anche se gli Stati Uniti hanno dato una nuova impostazione alla loro politica estera e di sicurezza. Perseguono in modo più marcato come la Cina e la Russia la concezione delle sfere di influenza. Così facendo indeboliscono l'ordine mondiale basato su regole, che in particolare l'Europa continua a sostenere.

Nonostante le crescenti difficoltà economiche, il sistema Putin continua a dimostrarsi stabile. La **Russia** prosegue per il quinto anno la sua guerra di aggressione contro l'Ucraina, senza alcun accordo di cessate il fuoco stabile né alcun trattato di pace sostenibile all'orizzonte. Da quando la Russia ha aggredito l'Ucraina nel 2022, minaccia di ricorrere alle armi nucleari. Nel frattempo, in Europa ha intensificato notevolmente il suo conflitto ibrido, in particolare con attività di sabotaggio, ma anche di influenza, con l'intento di mettere alla prova l'articolo 5 del Trattato Nord Atlantico nonché di indebolire le democrazie occidentali e l'unità transatlantica. La NATO ritiene che un attacco a uno Stato membro da parte della Russia entro la fine di questo decennio sia una possibilità realistica e quindi sta orientando in tal senso l'ulteriore sviluppo delle proprie capacità di difesa. Il termine entro il quale l'Europa dovrà essere concretamente in grado di difendersi dalla Russia dipende in larga misura dalla credibilità della NATO in termini di deterrenza, dalla posizione degli Stati Uniti nei confronti della NATO e dall'ulteriore evoluzione della guerra contro l'Ucraina. I tempi di preavviso per una guerra contro un membro europeo della NATO si sono notevolmente ridotti.

La **Cina** sta lavorando a favore di un nuovo ordine mondiale incentrato sui propri interessi: in un contesto di crescenti tensioni, sfrutta le dipendenze occidentali quale strumento di pressione. La Cina ha fatto della Russia il suo primo partner politico e riveste un ruolo fondamentale nel proseguimento della guerra contro l'Ucraina. La Cina mira a diventare la maggiore potenza economica, tecnologica e militare del mondo. In questo contesto, essa rappresenta sempre più una minaccia ibrida. Nel frattempo, diversi Stati occidentali stanno perseguendo strategie volte a ridurre le vulnerabilità economiche nei confronti della Cina e a rafforzare la loro resilienza. L'UE vede la Cina non solo come partner commerciale, ma anche come rivale sistemico. Da entrambe le parti sussistono tuttavia dipendenze reciproche, motivo per cui le relazioni sino-europee sono relativamente stabili nonostante la situazione politica tesa.

La **Cina** punta a un nuovo ordine mondiale. Partendo dal rifiuto dell'ordine di stampo occidentale, si avvicina sempre più a **Russia, Iran e Corea del Nord**. Sebbene i quattro Stati non formino alcuna alleanza e le loro relazioni siano caratterizzate da divergenze e diffidenza reciproca, sul piano politico la Corea del Nord non è più così isolata come lo era anni fa. Ha acquisito infatti maggiore margine di manovra nei confronti del suo principale partner commerciale, la Cina, e ha ulteriormente intensificato la cooperazione con la Russia. Prosegue inoltre il suo programma nucleare e continua a produrre uranio arricchito e plutonio. Dal canto loro, la Cina, ma anche la Russia, cercano di conquistare gli Stati del Sud globale per i propri interessi.

La **guerra in Iran** e la conseguente escalation nella regione stanno portando a un ulteriore indebolimento del cosiddetto Asse della resistenza guidato dal Paese, ma anche a un'ulteriore destabilizzazione di quest'area. Durante

la guerra l'Iran non ha ricevuto alcun sostegno politico o militare decisivo né dalla Russia né dalla Cina. I recenti avvenimenti si inseriscono nel contesto di una serie di conflitti irrisolti nel Vicino e Medio Oriente, in particolare tra Israele e i Palestinesi, in Iraq, in Yemen, in Libano e in Siria. La guerra in Iran mina la stabilità degli Stati del Golfo e ha inoltre acuito le tensioni in materia di politica di sicurezza tra gli Stati Uniti e i loro alleati europei. A causa del blocco dello Stretto di Hormuz, la guerra avrà ripercussioni economiche e di sicurezza a livello mondiale che si protrarranno nel tempo. La guerra provocherà inoltre un'ulteriore scarsità di beni militari rari a livello globale, in particolare nel settore della difesa aerea e della difesa dai droni.

Gli **Stati Uniti**, come la Cina e la Russia, mirano a un cambiamento dell'ordine mondiale. L'amministrazione statunitense intende concentrare la propria attenzione sulla «patria» e sull'«emisfero occidentale», relativizzando nei propri documenti programmatici le rivalità strategiche con Cina e Russia. Nei confronti dell'Europa prevalgono in parte toni da guerra culturale. Nel complesso, però, al momento la politica estera e di sicurezza statunitense è fortemente influenzata dalla personalità del Presidente. A seconda delle circostanze, essa assume ripetutamente chiari tratti globalisti, egemonici e interventisti ma esige che l'Europa si assuma autonomamente la responsabilità della propria sicurezza.

Nei prossimi anni l'**Europa** intende ridurre la sua dipendenza non solo dalla Cina, come descritto sopra, ma anche dagli Stati Uniti. Gli investimenti dell'UE nel settore della difesa hanno fatto un balzo in avanti nel 2025, ma la strada verso un'Europa post-americana è ancora lunga. La capacità di difesa e di deterrenza dell'Europa continua a dipendere dalle competenze militari strategiche di alto livello degli Stati Uniti, mentre la ricerca in Europa in questo campo è molto indietro rispetto ad analoghi investimenti statunitensi. La frammentazione del mercato europeo degli armamenti riduce l'efficienza del riarmo militare annunciato.

Le tendenze globali comportano minacce per la Svizzera e attacchi contro di essa:

- le azioni di sabotaggio fanno parte del conflitto ibrido della Russia contro l'Europa. Anche contro la Svizzera vengono messi in atto spionaggio, ciberattacchi e attività di influenza. Tuttavia, finora non si sono ancora verificati atti di sabotaggio rivolti contro **infrastrutture critiche** svizzere. Ciononostante, il nostro Paese potrebbe subire danni collaterali causati da simili attacchi all'estero in qualsiasi momento, ad esempio con l'intento di colpire gli Stati o le alleanze che ne dipendono;

- la Svizzera è particolarmente colpita dagli **sforzi di proliferazione** della Russia. A ciò si aggiunge il fatto che la Cina sta cercando di ottenere un vantaggio in Svizzera nella lotta per la supremazia tecnologica: il polo di ricerca svizzero rappresenta infatti un obiettivo interessante per la Cina. Per quanto riguarda la lotta contro la proliferazione e lo spionaggio, la Svizzera garantisce le conoscenze e così facendo contribuisce anche a rafforzare la prontezza alla difesa dell'Occidente. Se la Svizzera non agisce, si rischia di subire pressioni o addirittura un intervento sanzionatorio diretto da parte degli Stati occidentali;

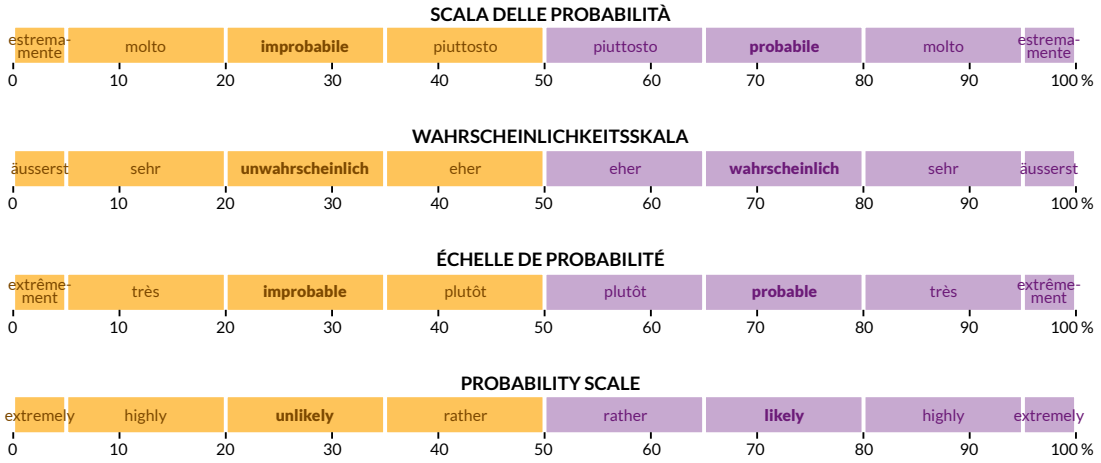
- i fattori che favoriscono lo **spionaggio** in Svizzera sono stabili: la minaccia generale di spionaggio è molto elevata. I servizi di intelligence esteri continuano a interessarsi a numerosi temi e settori, tra cui in via prioritaria la politica estera, commerciale e di sicurezza, ma anche le capacità dell'esercito, l'industria degli armamenti e la ricerca di punta nonché le organizzazioni, i gruppi

e le persone che vengono di volta in volta classificati come una minaccia. Istituzioni, organizzazioni e persone sono oggetto sia di spionaggio tradizionale sia attraverso ciberattacchi. La principale minaccia di spionaggio è rappresentata dalla Russia e dalla Cina.

- In Svizzera la **minaccia terroristica** continua a essere determinata principalmente dal movimento jihadista, soprattutto da persone che simpatizzano con lo «Stato Islamico» o che sono ispirate dalla propaganda jihadista. L'aggressione con coltello avvenuta a Winterthur il 28 maggio 2026, perpetrata da una persona radicalizzata dal jihadismo, conferma questa valutazione. La minaccia terroristica rimane elevata, il che significa che vi sono indizi della presenza di soggetti terroristici in Svizzera e/o di intenzioni terroristiche contro la Svizzera. La minaccia è sempre più diffusa. Il fenomeno della radicalizzazione jihadista online rimane virulento. La dinamica persistente dei conflitti in Vicino e Medio Oriente aumenta inoltre la probabilità di atti di violenza contro gli interessi ebraici, israeliani e americani in Europa. Ciò vale anche per la Svizzera. I luoghi di pubblico accesso difficili da proteggere, e in particolare le folle presenti in occasione di eventi sportivi e culturali, rimangono esposti come potenziali obiettivi di attentati. Inoltre, la guerra in Iran ha conseguenze dirette sulla minaccia terroristica in Europa e in Svizzera. A questo proposito, come potenziali autori di attentati vengono presi in considerazione principalmente attori al di fuori dello spettro jihadista. Tra questi figurano, ad esempio, sostenitori o simpatizzanti dell'Iran e attori vicini all'Iran, simpatizzanti di Hamas o anche criminali reclutati e pagati appositamente per compiere attentati.

- Anche l'**estremismo violento** rappresenta una minaccia per la Svizzera. Il potenziale di violenza degli ambienti dell'estremismo violento di sinistra rimane infatti elevato. La causa palestinese e quella curda costituiscono, insieme all'antifascismo, il suo impegno principale. Persiste anche la minaccia rappresentata dagli estremisti di destra violenti. Entrambi gli ambienti proseguono le loro attività e gli sviluppi osservati negli ultimi anni trovano conferma. Anche in futuro i due ambienti continueranno a orientarsi essenzialmente verso i temi prioritari perseguiti finora.

Panoramica delle indicazioni di probabilità menzionate in questo rapporto



RADAR DELLA SITUAZIONE

Per rappresentare le minacce rilevanti per la Svizzera il SIC utilizza uno strumento denominato radar della situazione. Il presente rapporto comprende una versione semplificata del radar della situazione, priva di dati confidenziali. In tale versione destinata al largo pubblico sono illustrate le minacce rientranti nella sfera di competenza del SIC e dell'Ufficio federale di polizia. Il rapporto non tratta temi di cui si occupano gli altri organi federali, ma fa riferimento ai lori rapporti.

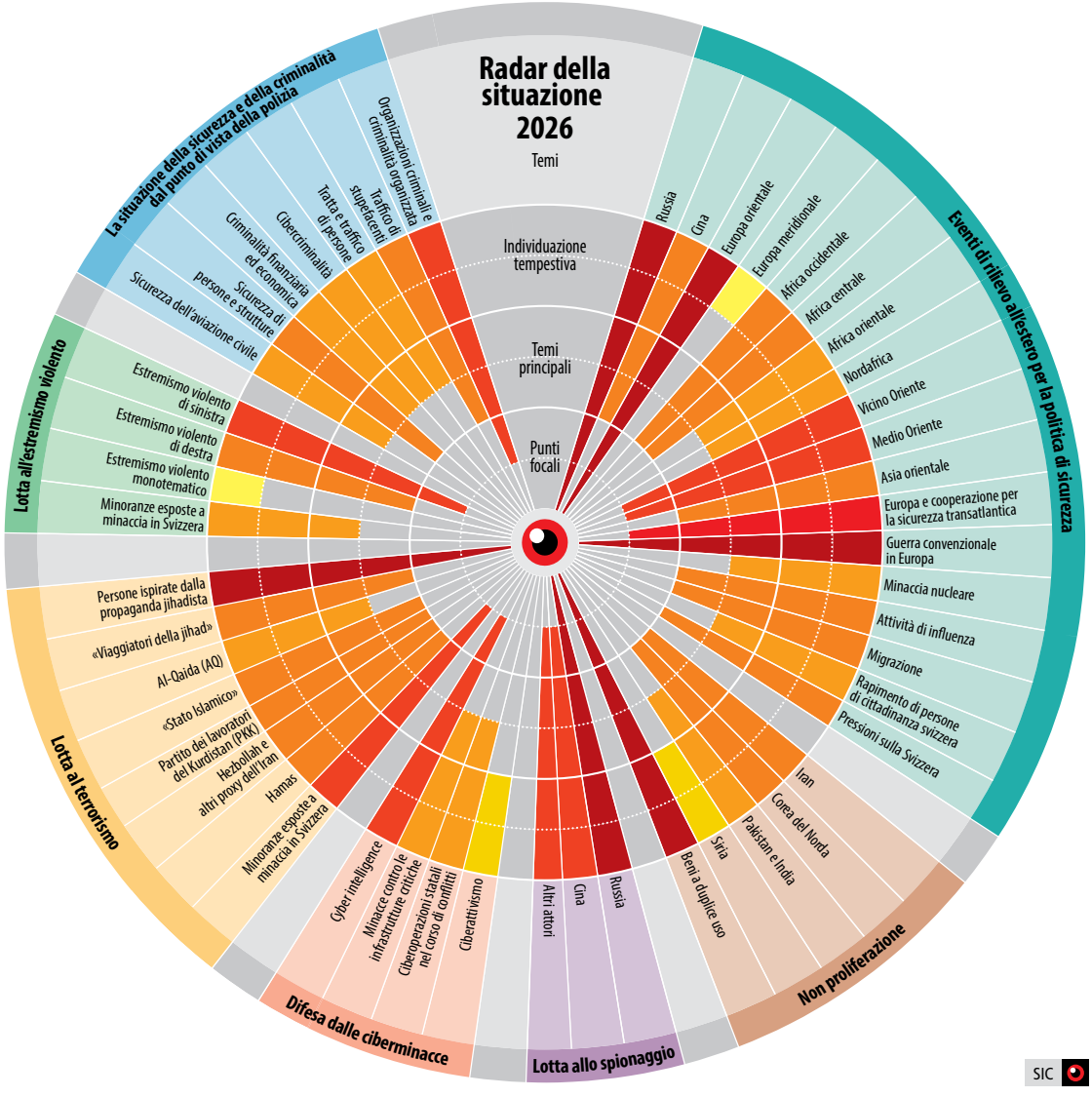


Illustrazione 2

CONTESTO STRATEGICO

TENDENZE GLOBALI

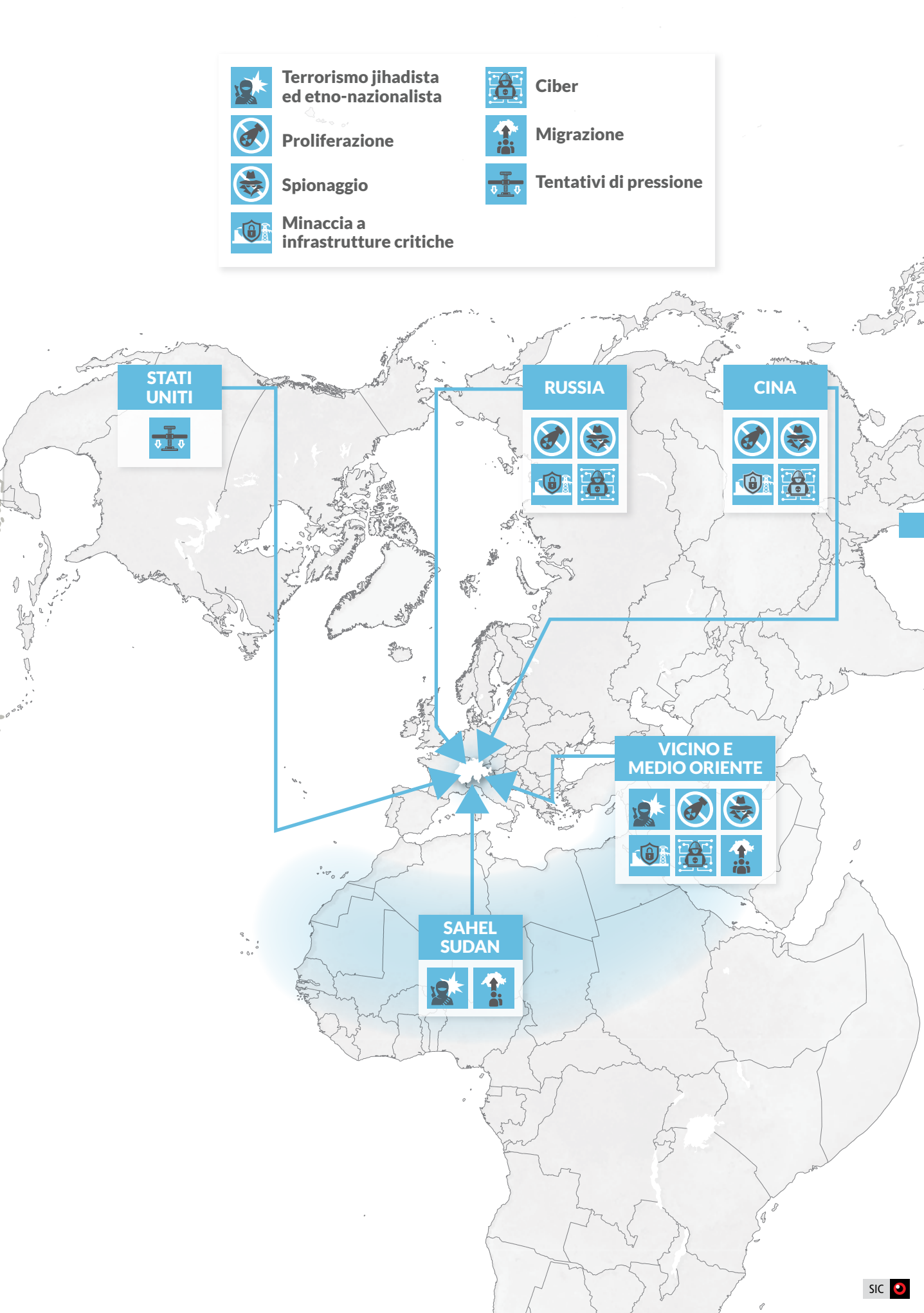
La Russia rimane la minaccia più grave e immediata per la sicurezza, la stabilità e la pace in Europa. Ha intensificato notevolmente il suo conflitto ibrido in Europa, come dimostrano i ciberattacchi, gli atti di sabotaggio, le violazioni dello spazio aereo e le attività di influenza nonché probabilmente anche misteriosi incidenti con i droni. La Svizzera è direttamente interessata dal conflitto ibrido *(cfr. al riguardo il capitolo «Russia», p. 22)*. La parziale conversione della Russia verso un'economia di guerra e il suo continuo riarmo, insieme alle mire russe note da tempo, rappresentano una minaccia per l'Europa che va oltre la guerra contro l'Ucraina. Questa guerra rimane la massima priorità per il regime russo, che ha sviluppato strategie complesse ed efficaci per continuare a rifornirsi di beni e tecnologie occidentali, aggirando a tal fine regole e sanzioni, anche in Svizzera.

La Russia ha intensificato notevolmente il suo conflitto ibrido in Europa. La Svizzera è direttamente interessata da questo conflitto ibrido.

La guerra contro l'Ucraina è una guerra di logoramento. Non si intravedono all'orizzonte né una decisione militare né accordo di cessate il fuoco stabile né un trattato di pace sostenibile: la Russia e l'Ucraina sembrano pronte a continuare rispettivamente la guerra di aggressione e quella di difesa. Nel frattempo, l'Europa si è ormai assunta la responsabilità principale del sostegno occidentale all'Ucraina, ma ha solo un'influenza indiretta sugli sforzi diplomatici per raggiungere la pace. Infatti, è soprattutto la Cina a svolgere un ruolo chiave affinché la guerra possa continuare.

Il 2022 ha anche segnato l'inizio di una nuova era nucleare. Le armi nucleari svolgono un ruolo di primo piano come strumento di potere, proprio come ai tempi della Guerra Fredda. Dall'inizio del conflitto la Russia ha ripetutamente minacciato di ricorrere alle armi nucleari e dopo decenni diverse potenze stanno valutando la possibilità di riprendere i propri test nucleari. A sua volta, la Cina sta ampliando il suo arsenale nucleare. La proliferazione nucleare è a un bivio e con la scadenza del trattato New Start nel febbraio 2026 è venuto meno l'ultimo accordo rimasto tra Stati Uniti e Russia in materia di controllo degli armamenti strategici. Ciò contribuisce a deteriorare il contesto in materia di politica di sicurezza della Svizzera in modo significativo e duraturo.

Anche la Cina rappresenta una minaccia ibrida crescente. La proiezione di potere cinese comprende strumenti militari, politici, istituzionali, ideologici, d'informazione, economici e tecnologici. La Cina intende mobilitare l'intero sistema per diventare una delle grandi potenze leader a livello economico, tecnologico e militare e in tal senso lavora alla creazione di un nuovo ordine mondiale: partendo dal rifiuto di quello di stampo occidentale, si è avvicinata sempre più a Russia, Iran e Corea del Nord. Tuttavia, questi Stati non formano alcuna alleanza. Tanto la Russia quanto la Cina in particolare, che non vuole esporsi alle rappresaglie statunitensi o compromettere le relazioni con gli Stati del Golfo, hanno reagito con molta cautela agli attacchi americano-israeliani contro l'Iran. Sebbene le relazioni tra i quattro Stati siano inoltre caratterizzate da divergenze e diffidenza reciproca, sono uniti in particolare dal fatto di rifiutare l'ordine mondiale di stampo occidentale e la democrazia liberale, puntando invece alla sovranità statale illimitata e a una forma di governo autocratica. È probabile che la loro unità sia destinata a durare nel tempo. Dal canto loro, la Cina, ma anche la Russia, cercano di conquistare gli Stati del Sud globale per i propri interessi. Le tensioni e i conflitti in Europa, in Africa e Asia, in particolare nel


Terrorismo jihadista ed etno-nazionalista
Proliferazione
Spionaggio
Minaccia a infrastrutture critiche
Ciber
Migrazione
Tentativi di pressione
STATI UNITI
RUSSIA
CINA
VICINO E MEDIO ORIENTE
SAHEL SUDAN

Vicino e Medio Oriente si moltiplicano e mettono alla prova la capacità di reazione degli Stati occidentali, soprattutto degli Stati Uniti. Dal Nord Africa e dalla regione del Sahel fino al Vicino e Medio Oriente, si estende sull'Europa un arco di crisi che comporta notevoli ripercussioni sulla sicurezza della Svizzera.

Gli Stati Uniti perseguono il proprio vantaggio geostrategico ed economico, anche se questo comporta tensioni con alleati e partner tradizionali. Dal 2025 l'Europa si trova in una posizione particolare, poiché si sforza di preservare un ordine che nemmeno gli Stati Uniti non sostengono più nella loro totalità. Per decenni questo ordine ha garantito sicurezza e benessere anche alla Svizzera.

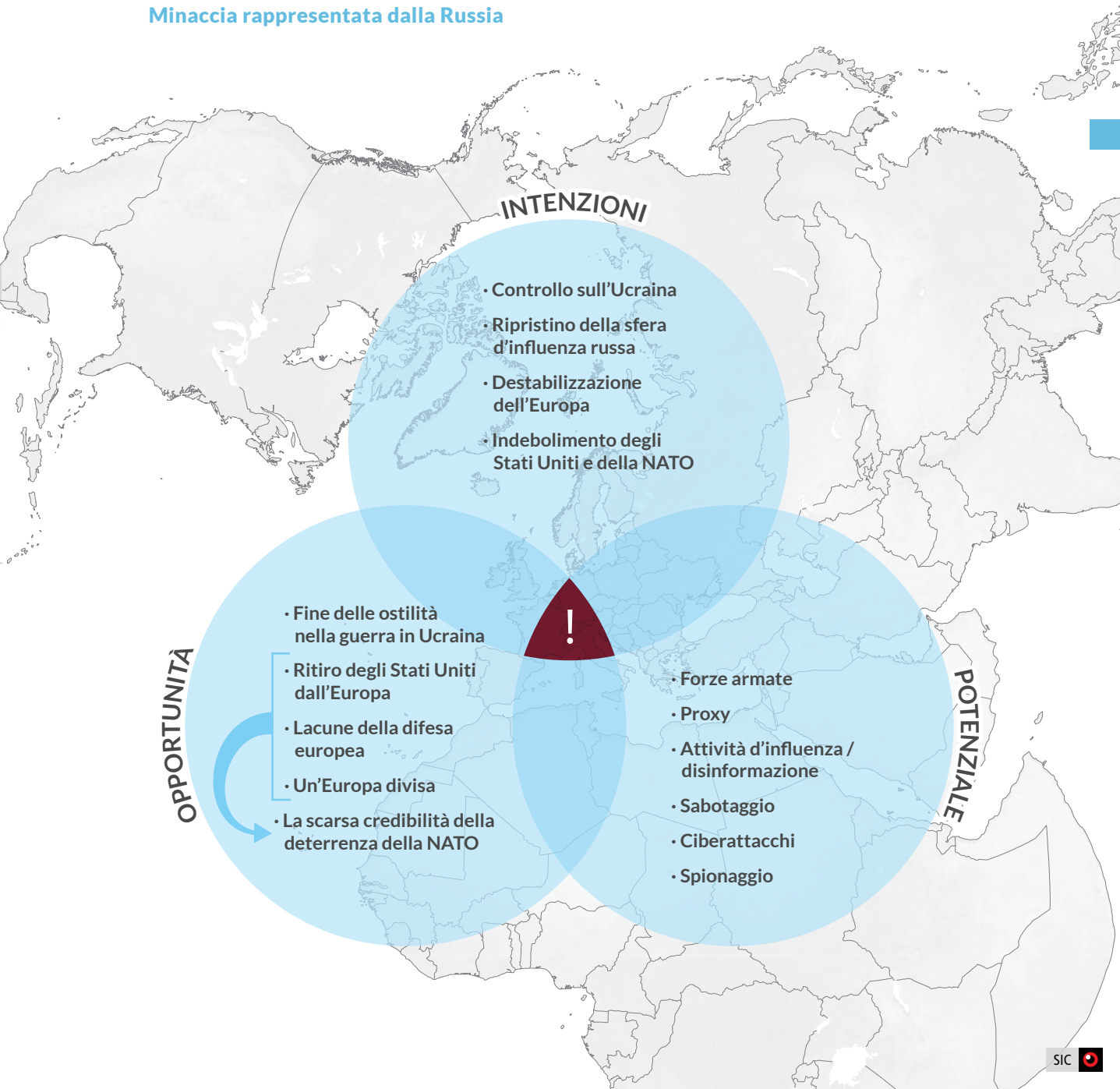
Le ambizioni di potere e i conflitti geopolitici rendono difficile risolvere in modo cooperativo le sfide globali e regionali in materia di politica di sicurezza. I principi dell'ordine globale e i forum internazionali sono messi sotto forte pressioni al fine di esercitare influenza e produrre effetti. Ciò vale in particolare per i regimi internazionali di non proliferazione delle armi di distruzione di massa o delle armi convenzionali, che le grandi potenze rivali non consentono di aggiornare.

L'ordine internazionale appare sovvertito e in fase di transizione. Si stanno delineando i contorni di un confronto globale, principalmente tra Stati Uniti e Cina, un mondo a due sfere di influenza caratterizzato dalla lotta strategica per la supremazia. Le grandi potenze ricorrono sempre più spesso a sanzioni, controlli sulle esportazioni, sovvenzioni, strumenti finanziari o altri strumenti di pressione, anche contro Paesi terzi, per impedire alla controparte di accedere a beni e tecnologie chiave e preservare nonché promuovere le proprie capacità. La potenziale rilevanza militare e civile di un numero crescente di settori e di categorie di beni fa sì che questi vengano classificati come critici o strategici: terre rare, semiconduttori, intelligenza artificiale, robotica, energie rinnovabili, tecnologia quantistica e biotecnologia, ma anche droni e dati in generale. Nel settore della difesa si tratta, ad esempio, della navigazione non satellitare, dei canali di comunicazione a prova di intercettazione o del cosiddetto campo di battaglia trasparente. Questo armamento geoeconomico ha ripercussioni sulla politica di sicurezza a livello globale, motivo per cui gli Stati integrano la sicurezza economica e tecnologica nei loro piani nazionali.

L'interdipendenza economica e l'interconnessione creano dipendenze. Queste vengono sempre più spesso utilizzate come strumenti di pressione e armi nei conflitti per raggiungere obiettivi politici e militari. Anche gli attori non

statali sfruttano le vulnerabilità altrui, come dimostrano gli attacchi degli Houthi yemeniti lungo una rotta marittima fondamentale per il commercio mondiale. Gli sviluppi nell'arco di crisi che si estende lungo la periferia meridionale continueranno a rappresentare una sfida per l'Europa: offrono margine di manovra a vari attori statali e non statali ostili «all'Occidente», e quindi anche alla Svizzera. L'Europa è minacciata e molto probabilmente tale minaccia non si attenuerà nei prossimi anni.

Minaccia rappresentata dalla Russia



STATI UNITI

Nel suo secondo mandato, il presidente Donald Trump sta perseguendo una politica estera e di sicurezza a più riprese sovversiva. Rispetto al suo primo mandato l'influenza stabilizzatrice degli internazionalisti tradizionali repubblicani all'interno del gabinetto è venuta meno e il presidente si è circondato principalmente di lealisti.

La politica degli Stati Uniti mira a ottenere i propri vantaggi economici, anche a scapito degli alleati tradizionali, che dovrebbero pagare di più per gli impegni in materia di sicurezza. Il focus strategico si concentra sulla «patria» e sull'«emisfero occidentale», relativizzando in maniera retorica le rivalità strategiche con Cina e Russia. Gli Stati Uniti hanno compiuto la più grande inversione di rotta in materia di politica di sicurezza esprimendo la volontà di riallacciare rapporti di cooperazione con la Russia, un'iniziativa finora fallita a causa della ferma intenzione del presidente Vladimir Putin di perseguire obiettivi massimi nella guerra contro l'Ucraina. Il presidente Trump continua a minimizzare la rivalità sistemica con la Cina. Già in occasione del vertice con il capo di Stato e di Partito Xi Jinping nell'autunno del 2025, aveva annunciato la nascita di un «G2», un gruppo esclusivo di due grandi potenze destinate a dominare il mondo in futuro. Tuttavia, anche se la retorica nei confronti della Cina si è notevolmente attenuata, la rivalità sistemica con la Cina e la regione Asia-Pacifico rimane una priorità strategica per gli Stati Uniti. Ciò avviene principalmente per ragioni economiche, ma ha conseguenze in termini di politica di sicurezza: gli Stati Uniti intendono infatti rafforzare le proprie forze armate e l'autonomia dei propri alleati militari nella regione, al fine di scoraggiare la Cina. Il potere deterrente riguarda soprattutto gli interventi militari della Cina nella regione, che potrebbero compromettere la stabilità delle catene di approvvigionamento, in particolare nel caso di un conflitto su Taiwan.

La politica estera e di sicurezza degli Stati Uniti è attualmente interventista, nonostante in campagna elettorale Donald Trump si fosse presentato come isolazionista, intenzionato a mettere gli Stati Uniti al primo posto e a tenerli fuori da ulteriori «guerre infinite». Sebbene tra i più stretti consiglieri del Presidente esistano diverse scuole di pensiero, la politica estera e di sicurezza americana è determinata innanzitutto dal Presidente: nella pratica assume, a seconda delle situazioni, tratti chiaramente globalisti, egemonici e interventisti, anche se nei documenti programmatici strategici vengono sostenuti principi fondamentali divergenti e specialmente la guerra contro l'Iran è controversa tra i repubblicani dell'«America First».

Le crisi, i conflitti e le guerre che si stanno verificando contemporaneamente in America Latina, Europa, Vicino e Medio Oriente e nell'Asia-Pacifico mettono a dura prova le forze degli Stati Uniti. A ciò si aggiunge l'indebolimento delle alleanze tradizionali provocato dal Paese stesso. Proprio le minacce proferite all'inizio del 2026 dal presidente statunitense nei confronti della Danimarca – membro della NATO – di annettere la Groenlandia, hanno indebolito la fiducia dell'Europa negli Stati Uniti.

Le crisi, i conflitti e le guerre che si stanno verificando contemporaneamente mettono a dura prova le forze degli Stati Uniti. A ciò si aggiunge l'indebolimento delle alleanze tradizionali provocato dal Paese stesso.

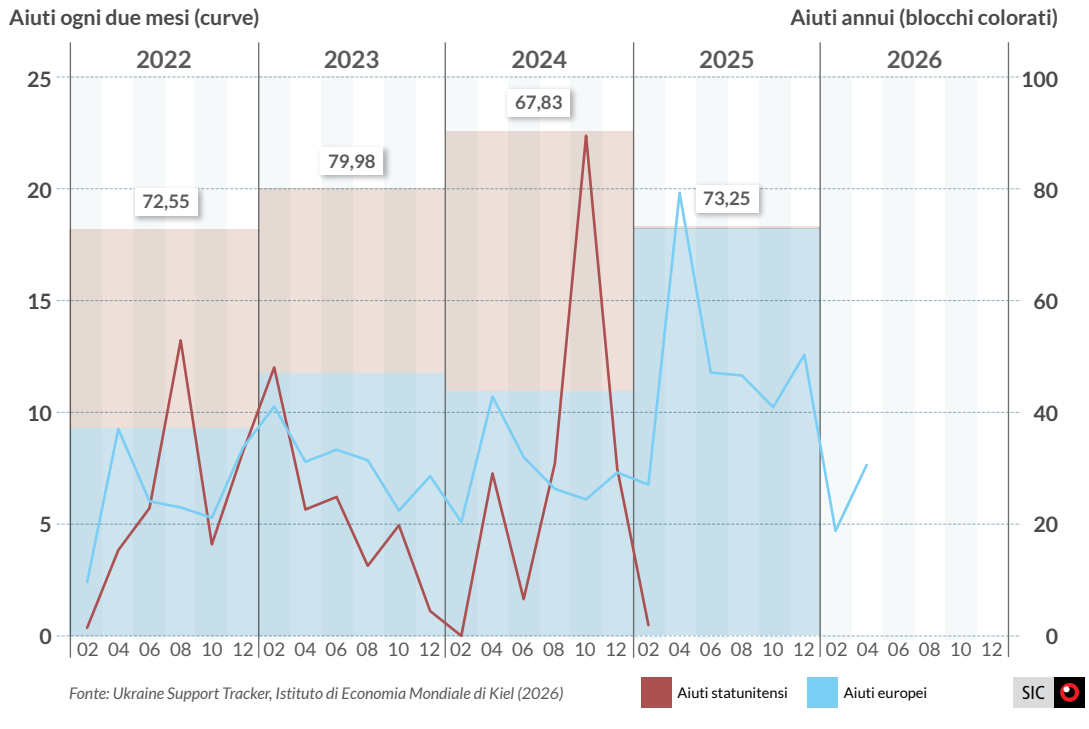
Il presidente Trump continuerà a cercare di porre fine alla guerra contro l'Ucraina. La possibilità che ciò avvenga nei prossimi mesi dipende da diversi fattori dinamici. A tal fine una tregua dovrebbe apparire più vantaggiosa per entrambe le parti in conflitto rispetto al proseguimento della guerra, il che dipende, tra l'altro, anche dal sostegno occidentale all'Ucraina, dalla situazione militare al fronte e dall'andamento dell'economia russa. Un cessate il fuoco stabile o un accordo di pace duraturo entro la fine del 2026 restano molto improbabili.

Gli Stati Uniti hanno avviato una nuova ripartizione degli oneri, secondo la quale l'Europa in futuro dovrà assumersi un maggiore carico degli impegni di deterrenza e di difesa nell'ambito della NATO. È probabile che la presenza militare americana in Europa sarà ridotta, anche se si prevede che ciò non avverrà in modo improvviso né significativo. Inoltre, per il momento gli Stati Uniti manterranno il loro scudo nucleare sull'Europa e non ritireranno bruscamente dall'Europa le loro capacità militari chiave attualmente indispensabili: in linea di principio, hanno bisogno di essere presenti in Europa, anche nell'ottica di una proiezione di potere militare a livello globale. Ciononostante, nei confronti dell'Europa prevale talvolta un tono aspro da scontro culturale, poiché parti dell'amministrazione statunitense guardano all'Europa attraverso la lente della propria politica interna, affermando che il vecchio continente rischia la cancellazione della sua civiltà.

La rivalità sistemica tra Stati Uniti e Cina si accentuerà e si manifesterà principalmente nei settori dell'economia, della politica doganale e della tecnologia, con ripercussioni dirette sull'Europa e sulla Svizzera *(cfr. «Cina: sicurezza economica», p. 28)*. A livello militare, entrambe le nazioni continueranno a potenziare i propri armamenti, cercando di superarsi a vicenda in termini di forza e potere.

Aiuti statunitensi ed europei all'Ucraina dal gennaio 2022

(in miliardi EUR)



Fonte: Ukraine Support Tracker, Istituto di Economia Mondiale di Kiel (2026)

EUROPA

Dopo il vertice inconcludente con gli Stati Uniti tenutosi in Alaska, dalla fine dell'estate 2025 la Russia ha intensificato il suo conflitto ibrido contro l'Europa. A differenza di quanto avvenuto dalla primavera all'autunno del 2024, la Russia ha puntato soprattutto sulle violazioni dello spazio aereo da parte dei suoi aerei da combattimento e presumibilmente sui voli di droni sugli aeroporti civili e militari. Ci sono stati però anche atti di sabotaggio (sia fisici sia informatici), tra l'altro contro infrastrutture ferroviarie ed energetiche polacche.

La continua minaccia russa e l'atteggiamento della nuova amministrazione statunitense hanno portato l'Europa ad assumersi una responsabilità nettamente maggiore per la propria difesa, la deterrenza nei confronti della Russia e il sostegno all'Ucraina. Nell'ambito dell'alleanza transatlantica, gli Stati Uniti avevano chiesto a più riprese una simile ridistribuzione degli oneri fin dall'inizio della Guerra Fredda. In occasione del vertice NATO tenutosi all'Aia nel giugno 2025, i membri si sono impegnati a raggiungere un nuovo obiettivo di spesa per la difesa, pari al cinque per cento del rispettivo prodotto interno lordo. La NATO ha inoltre lanciato tre nuove missioni: Baltic Sentry, Eastern Sentry e Arctic Sentry. Da gennaio 2025, Baltic Sentry sorveglia e protegge i cavi sottomarini nel Mar Baltico. Nel settembre 2025, la NATO ha inoltre reagito con Eastern Sentry alla serie di violazioni dello spazio aereo e ai misteriosi incidenti con droni sopra il proprio territorio. Questa nuova missione testa la Eastern Flank Deterrence Line annunciata dalla NATO nel luglio 2025, una rete di sensori a più livelli per il rilevamento e la difesa contro mezzi nemici. Nel febbraio 2026, sullo sfondo delle rivendicazioni territoriali del presidente Trump sulla Groenlandia, la NATO ha lanciato Arctic Sentry a dimostrazione del maggiore impegno degli Stati membri europei nell'estremo Nord. In concreto, sono stati intensificati i pattugliamenti nella regione.

Secondo l'Ukraine Support Tracker del Kiel Institute, tra gennaio 2022 e fine aprile 2026 l'Europa ha speso in totale 215 miliardi di euro a sostegno dell'Ucraina, una cifra nettamente superiore ai 115 miliardi di euro stanziati dagli Stati Uniti. I principali donatori sono la Germania e il Regno Unito. L'Ucraina continua tuttavia a dipendere dagli Stati Uniti, soprattutto per quanto riguarda i sistemi di difesa aerea e le informazioni di intelligence. Con la cosiddetta lista delle esigenze prioritarie per l'Ucraina (Prioritised Ukraine Requirements List), dal 2025 è in vigore un meccanismo con il quale l'Europa finanzia l'acquisto di armi americane a favore dell'Ucraina. Tra le altre cose, sono stati forniti sistemi di difesa terra-aria Patriot e sistemi di artiglieria a lunga gittata.

Nel complesso, gli Stati europei sono ormai i principali sostenitori dell'Ucraina. Il loro aiuto militare è stato superiore del 67 per cento rispetto alla media registrata tra il 2022 e il 2024. Ciononostante, nel 2025 l'Ucraina ha dovuto fare i conti con un sostegno internazionale ridotto, poiché gli Stati Uniti hanno drasticamente ridotto i propri aiuti in quell'anno. Gli Stati europei hanno inoltre dovuto reagire a più riprese a una dinamica in rapida evoluzione riguardo alle iniziative statunitensi volte a garantire la pace in Ucraina. Tuttavia, finora non si è giunti né a una normalizzazione delle relazioni tra Stati Uniti e Russia né a un accordo di pace negoziato da questi due Paesi.

I rapporti tra Europa e Cina rimangono tesi, anche se entrambe le parti si adoperano a favore di relazioni stabili e costruttive. L'UE

vede la Cina non solo come partner commerciale, ma anche come rivale sistemico. Il rifiuto dell'ordine mondiale di stampo occidentale da parte della Cina, il suo modello economico sostenuto dallo Stato, le distorsioni del mercato, i trasferimenti di tecnologia e le dipendenze strategiche rappresentano minacce e rischi per la concorrenza europea, il commercio equo, la sicurezza delle catene di approvvigionamento nonché la sovranità industriale e tecnologica. Nel 2025 l'UE ha ampliato in modo significativo la sua strategia di sicurezza economica, concentrandosi sulla gestione dei rischi derivanti dai cambiamenti geopolitici, dagli sviluppi tecnologici e dalle dipendenze da Paesi terzi, in particolare dalla Cina. Anche il continuo sostegno della Cina allo sforzo bellico russo rimane un motivo centrale di discordia. A causa della politica commerciale ed economica degli Stati Uniti, in parte conflittuale e maggiormente incentrata sugli interessi nazionali, alcuni Stati europei stanno cercando di compensare le perdite economiche attraverso una cooperazione più stretta con la Cina.

Nel 2025 gli investimenti dell'UE nel settore della difesa hanno fatto un balzo in avanti. Ma la principale iniziativa politico-militare degli europei del 2025, ad esempio, vale a dire la pianificazione di una missione militare sul territorio ucraino come possibile garanzia di sicurezza per l'Ucraina, non si è svolta nel quadro dell'UE, ma in un formato ad hoc sotto la guida della Gran Bretagna, Paese non membro.

La strada verso un'Europa autonoma nel settore della difesa è quindi ancora lunga: anche se ormai praticamente tutti gli Stati europei della NATO raggiungono il precedente obiettivo del due per cento del prodotto interno lordo per le spese di difesa, la capacità di difesa e di deterrenza dell'Europa continua a dipendere dalle competenze militari strategiche di alto livello degli Stati Uniti, oltre al fatto che la ricerca europea in questo campo è molto indietro rispetto agli investimenti statunitensi. Inoltre, in molte regioni si registrano problemi di reclutamento.

La strada verso un'Europa autonoma nel settore della difesa è ancora lunga. La capacità di difesa e di deterrenza dell'Europa continua a dipendere dalle competenze militari strategiche di alto livello degli Stati Uniti.

Il frammentato mercato europeo degli armamenti riduce l'efficienza del riarmo militare annunciato. Ma la tendenza per i prossimi anni è chiara: l'Europa vuole ridurre la sua dipendenza dagli Stati Uniti e costruire una propria capacità di deterrenza militare. A lungo termine gli sforzi volti ad armonizzare il mercato degli armamenti e l'approccio sempre più integrativo nella politica comune di sicurezza e di difesa dovrebbero dare i loro frutti. Resta tuttavia da vedere se l'attuale coesione in materia di politica di sicurezza in Europa, al momento sempre più forte, rimarrà tale o se in futuro subirà una nuova frammentazione.

Nel 2026 è probabile che l'UE contrasterà in modo più attivo la Cina e cercherà di ridurre ulteriormente i rischi: la strategia di sicurezza economica dell'UE comprende strumenti quali verifiche sugli investimenti, controlli sulle esportazioni di tecnologie critiche, misure antisovvenzione e dazi antidumping. In controtendenza rispetto a ciò, tuttavia, alcuni Stati europei continueranno ad aprirsi economicamente nei confronti della Cina. La Svizzera si trova a dover affrontare le stesse decisioni *(cfr. «Cina: sicurezza economica», p. 28)*.

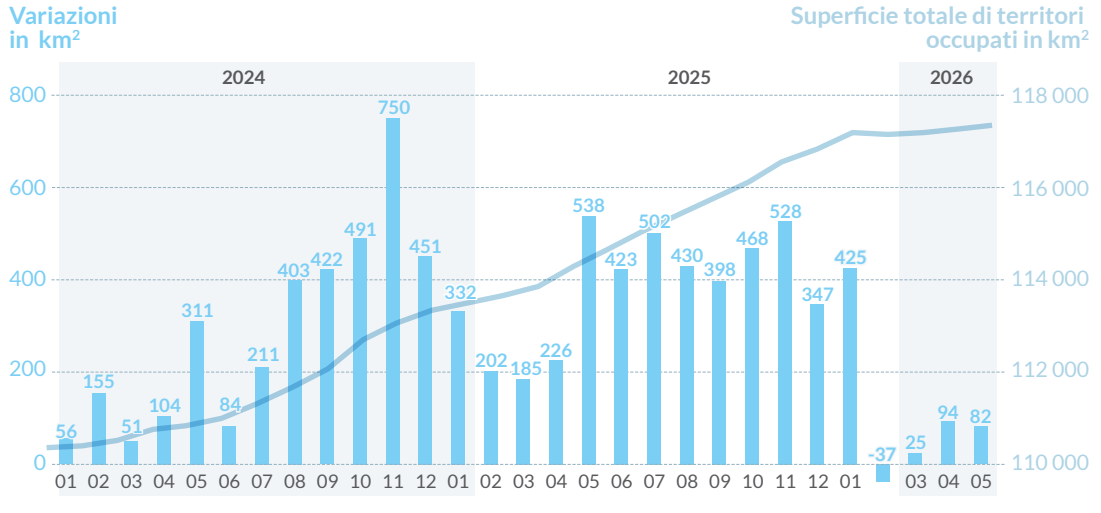
RUSSIA

Nonostante le crescenti difficoltà economiche, il sistema Putin continua a dimostrarsi stabile. Le persone chiave gli rimangono fedeli; sebbene molte di loro abbiano già superato i 70 anni, il presidente Putin non intende sostituirle, tanto meno durante la guerra in corso, puntando invece alla stabilità. Ciononostante, da diversi anni la dirigenza sta formando una nuova generazione, composta in parte da figli di stretti alleati del Presidente, ma anche da tecnocrati che gli hanno dimostrato una lealtà incondizionata. In Russia l'opposizione è sempre più repressa; ciò va di pari passo con una propaganda più aggressiva nei media e nel settore dell'istruzione, come pure con una crescente sorveglianza, repressione e militarizzazione della società.

I problemi economici si sono aggravati. Nel 2025 il prodotto interno lordo è cresciuto solo dell'uno per cento circa. A risentire in particolare dell'inflazione elevata, degli alti costi degli interessi e della carenza di manodopera sono i settori civili. Dal canto loro, le spese pubbliche hanno continuato ad aumentare. Il calo del prezzo del petrolio e le nuove sanzioni hanno determinato al contempo una riduzione relativamente significativa delle entrate provenienti dal settore energetico. Ciò ha contribuito a far sì che il bilancio russo del 2025 si chiudesse con un deficit di almeno 50 miliardi di franchi, ma probabilmente superiore. Il finanziamento delle spese di guerra è stato comunque garantito. L'aumento dei prezzi del petrolio e del gas a livello mondiale causato dalla guerra in Iran sta generando entrate supplementari per le casse dello Stato russo. Affinché la Russia possa finanziare il proprio deficit di bilancio grazie alle maggiori entrate provenienti dal settore energetico, il prezzo del petrolio dovrebbe però rimanere per oltre un anno al di sopra dei 100 dollari al barile.

In questa guerra, la Russia è superiore all'Ucraina, sia in termini di risorse materiali che di effettivi. Sul versante ucraino, la mancanza di personale indebolisce la difesa, con conseguenti perdite territoriali. Sebbene la situazione delle forze armate ucraine sia leggermente migliorata dall'inizio del 2026, le forze armate russe avan-

Avanzate mensili delle truppe russe



SIC

zano, anche se molto lentamente. L'Ucraina si è dimostrata molto innovativa nella produzione e nell'impiego dei droni. Ormai produce autonomamente la maggior parte dei droni utilizzati e li impiega con successo nella difesa aerea, al fronte e contro obiettivi strategici sul territorio russo. L'Ucraina condivide le competenze in materia non solo con la NATO, ma anche con i Paesi del Golfo. L'Ucraina continua però a dipendere dal sostegno estero, soprattutto per quanto riguarda le finanze, la difesa aerea, l'artiglieria e i mezzi a lunga gittata, oltre che per le informazioni di intelligence. Di recente tale sostegno è diminuito, mentre la Russia recluta un numero sufficiente di nuovi soldati per compensare le perdite e rifornire nuove formazioni.

La Russia intende indebolire le democrazie occidentali e l'unità transatlantica. La sua strategia di conflitto ibrido riguarda anche la Svizzera o la minaccia:

- La Russia prende direttamente di mira la Svizzera con disinformazione e propaganda. Ad esempio, la filiale di lingua tedesca dell'emittente statale russa RT 2025 ha diffuso circa un quarto in più di notizie sulla Svizzera rispetto all'anno precedente.
- I ciberattacchi contro obiettivi all'estero passano anche attraverso infrastrutture svizzere.
- Presumibilmente la Russia sfrutta la Svizzera anche dal punto di vista logistico e per preparare azioni di sabotaggio e destabilizzazione in altre parti d'Europa.
- La Russia cerca di ottenere informazioni confidenziali dalle autorità svizzere tramite attività di spionaggio.
- La Russia sfrutta la Svizzera per l'approvvigionamento segreto di beni e tecnologie soggetti a sanzioni, al fine di aumentare la propria capacità produttiva di materiale bellico e munizioni.

La popolazione russa avverte sempre più gli effetti della guerra, il che sta alimentando un crescente malcontento. Lo Stato russo riesce tuttavia attraverso la sorveglianza e la repressione a gestire questo malcontento e a soffocare sul nascere ogni forma di resistenza. In vista delle elezioni della Duma di Stato del settembre 2026, sono in corso preparativi per garantire una vittoria incontrastata del partito di governo «Russia Unita», al fine di assicurare una stabilità interna a lungo termine.

Il 2026 sarà ancora un anno difficile per la Russia dal punto di vista economico, con crescenti ripercussioni sulla popolazione. Il Cremlino continuerà tuttavia a dare priorità al finanziamento della guerra, in modo da mantenere le spese per la difesa e la sicurezza a un livello elevato. Le entrate del budget statale provenienti dal settore petrolifero e del gas sono diminuite in termini percentuali negli ultimi anni. Da gennaio 2026 il Cremlino ha invece aumentato l'IVA e punta a regolamentare la zona grigia dell'economia. Nonostante la situazione economica più difficile, nulla lascia presupporre che ciò possa compromettere la capacità della Russia di resistere nella guerra contro l'Ucraina.

È estremamente probabile che la Russia intensifichi la sua strategia di conflitto ibrido in Europa. In questo contesto, anche le infrastrutture critiche svizzere potrebbero diventare un obiettivo appetibile: la Russia potrebbe sabotarle o distruggerle, non tanto per danneggiare la Svizzera, in primo luogo, quanto piuttosto per colpire i Paesi dell'UE e della NATO.

È estremamente probabile che la Russia intensifichi la sua strategia di conflitto ibrido in Europa. In questo contesto, anche le infrastrutture critiche svizzere potrebbero diventare un obiettivo appetibile.

Le forze armate russe potranno probabilmente continuare a combattere fino alla fine del 2026, seppure a un costo maggiore per l'economia del Paese. Considerato il ritmo attuale con cui l'esercito guadagna terreno, gli ci vorranno ancora anni per conquistare completamente il Donbass. È estremamente probabile che le forze armate russe mantengano l'iniziativa fino alla fine del 2026; tuttavia, è estremamente improbabile che le forze armate ucraine subiscano un crollo entro la fine del 2026.

La Russia può continuare a insistere pubblicamente sulle proprie pretese massimaliste, a ritardare i negoziati in modo mirato e a puntare sulla carta militare fino a quando non riuscirà a ottenere concessioni o vantaggi concreti. L'intenzione a lungo termine della Russia di ottenere il controllo sull'Ucraina rimane immutata, anche se per ragioni tattiche il Cremlino potrebbe accettare una tregua o un «accordo» a suo vantaggio, fiducioso nel fatto che la situazione politica interna, militare e diplomatica dell'Ucraina continuerà a deteriorarsi e che il sostegno occidentale non durerà.

La posizione dell'Ucraina nel «processo di pace» dipende dagli sviluppi della politica interna. Il presidente Volodymyr Zelensky è indebolito dagli scandali legati alla corruzione. Accetterà di fare concessioni territoriali nel Donbass solo in cambio di garanzie di sicurezza internazionali. Senza un cessate il fuoco con la Russia, è improbabile che in Ucraina si tengano elezioni presidenziali o un referendum sui negoziati di pace. Ciò è subordinato al fatto che il presidente Trump aumenti la pressione sull'Ucraina al punto che essa debba cedere alle condizioni russe.

Le concezioni radicalmente diverse di Russia e Ucraina in merito alla pace, e in particolare la posizione intransigente della Russia quanto alle sue massime pretese, impediranno anche nel 2026 una soluzione del conflitto, almeno finché la situazione generale sul fronte militare non peggiori in modo determinante per una delle due parti *(Per quanto riguarda le conseguenze per la Svizzera, si veda il riquadro «Una guerra tra la NATO e la Russia in Europa entro il 2030?» nella pagina successiva).*

UNA GUERRA TRA LA NATO E LA RUSSIA IN EUROPA ENTRO IL 2030?

Dal 2022 le autorità di sicurezza degli Stati occidentali hanno messo pubblicamente in guardia dalla possibilità di un attacco militare russo alla NATO. La NATO si sta preparando a un attacco russo che, secondo diversi servizi di intelligence europei, potrebbe avvenire prima della fine del decennio in corso. I tempi di preavviso in caso di guerra in Europa si sono notevolmente ridotti, anche per la Svizzera: se prima erano almeno di dieci anni, ora sono solo pochi anni. È quindi ancora più importante ridurre al minimo le possibilità della Russia in Europa, Svizzera compresa.

Non è possibile sapere con precisione entro quando l'Europa dovrà essere in grado di difendersi dalla Russia, poiché occorre tenere conto di molte variabili e incognite, tra cui l'ulteriore andamento della guerra contro l'Ucraina e la posizione degli Stati Uniti nei confronti della NATO:

- La Russia sta maturando una preziosa esperienza bellica in Ucraina. Al momento, tuttavia, il suo potenziale militare rimane in gran parte assorbito da questo conflitto; solo alla fine di esso si potrebbe accelerare la ricostituzione delle forze armate russe, compreso il loro corpo di ufficiali, fortemente ridotto. La Russia sta inoltre sviluppando strategie complesse per dotarsi di armamenti attraverso beni e tecnologie occidentali.

- Gli Stati Uniti non hanno ridotto la loro presenza in Europa né in modo improvviso né significativo, ma hanno comunque annunciato dei cambiamenti. Resta da chiedersi quanto siano affidabili le loro garanzie di sicurezza, quanto sia stabile l'Unione europea in termini di politica interna e di sicurezza e quanto a lungo Stati chiave come Francia e Germania manterranno la loro linea a favore dell'Ucraina e della NATO. Gli attacchi ibridi della Russia mirano a dividere le società occidentali per indebolirne la coesione politica e la capacità decisionale.

La chiusura a livello di politica interna dell'Europa, degli Stati Uniti e della NATO, oltre alle capacità della Russia attualmente ancora impegnate in Ucraina, costituiscono variabili importanti per valutare la probabilità di una guerra tra la Russia e la NATO. In questo contesto è anche importante il livello di credibilità che il presidente russo Putin e la sua cerchia di potere attribuiscono alla capacità di deterrenza e alla difesa della NATO.

Finché le forze armate russe saranno impegnate in Ucraina e gli Stati Uniti continueranno a garantire la difesa dell'Europa, si applicano le seguenti probabilità d'insorgenza:

- È estremamente probabile un ulteriore inasprimento della strategia di conflitto ibrido della Russia in Europa, anche al fine di mettere alla prova l'articolo 5 del Patto Atlantico. Un'escalation potrebbe verificarsi in qualsiasi momento e in modo repentino.

Un'escalation potrebbe verificarsi in qualsiasi momento e in modo repentino.

- Un attacco militare della Russia contro uno Stato europeo è molto improbabile.

- Una guerra su vasta scala tra la Russia e la NATO è estremamente improbabile.

CINA

Con il 15° piano quinquennale, la Cina punta a una crescita economica a lungo termine e al dominio tecnologico attraverso l'innovazione e il controllo delle catene di approvvigionamento critiche. Allo stesso tempo, si prevede di modernizzare le forze armate e di approfondire ulteriormente la fusione tra settore militare e civile. La Cina sta espandendo la propria influenza a livello globale. Il suo intento è quello di sovvertire gli equilibri di potere a suo favore e così facendo rivaleggia principalmente con gli Stati Uniti. Tali ambizioni, la competizione tra le grandi potenze e il conseguente potenziamento di strumenti economici quali mezzi di pressione e armamenti stanno accelerando la frammentazione geoeconomica. Tutti questi fattori comportano minacce e rischi per la sicurezza economica, anche per la Svizzera.

Nel 2025, ad esempio, ha sfruttato le dipendenze dell'Occidente come mezzo per esercitare una contropressione mai vista prima, ad esempio in risposta ai dazi commerciali statunitensi. Fino a ottobre 2025 la Cina aveva limitato l'esportazione di 12 delle 17 terre rare totali, causando così interruzioni nell'approvvigionamento. Inoltre, propone un nuovo ordine mondiale e sta cercando di convincere gli Stati del Sud globale ad aderirvi.

La Cina ha fatto della Russia il suo primo partner politico. Svolge un ruolo chiave nel proseguimento della guerra contro l'Ucraina, acquistando petrolio e gas dalla Russia. Inoltre, la Cina vende alla Russia beni a duplice impiego, sostenendo di fatto l'azione militare della Russia, anche se respinge tale accusa. La Cina esporta poi in Russia beni acquistati in Svizzera, ad esempio macchine utensili, oppure le utilizza in loco per la produzione a favore della Russia. La Cina non vuole che la Russia venga indebolita da una sconfitta in Ucraina, soprattutto per l'importanza politica della sua partnership. Una tale sconfitta sposterebbe gli equilibri strategici a sfavore della Cina. Con il crollo del potere statale in Russia, si creerebbe inoltre un grave rischio per la sicurezza lungo i propri confini.

La Cina sta lavorando a favore di un nuovo ordine mondiale. Ha fatto della Russia il suo primo partner politico.

L'ascesa della Cina come potenza mondiale è evidente soprattutto nell'area dell'Asia-Pacifico, dove coniuga sempre più spesso gli strumenti economici e diplomatici utilizzati anche in altre parti del mondo con mezzi militari e paramilitari. Le forze armate cinesi proseguono nel loro processo di ammodernamento e di potenziamento: si stima che oggi il 12 per cento della spesa militare mondiale sia attribuibile alla Cina. Le forti tensioni causate dalla Cina nel Mar Cinese Meridionale e Orientale e intorno a Taiwan continuano ad aumentare. La Cina viola regolarmente il diritto internazionale con le sue attività militari in parte aggressive ed esercita pressioni sui suoi vicini per affermare le proprie rivendicazioni territoriali.

Gli Stati Uniti stanno cercando di controbilanciare la proiezione di potere della Cina nell'Asia-Pacifico, oltre che di rafforzare in linea di principio le loro alleanze in quell'area. Tuttavia, alcuni Stati non sono sicuri di quale sia la posizione dell'amministrazione Trump nella regione e nei confronti della Cina, né riescono a fare fronte comune con la Cina. Piuttosto, molti di essi stanno perseguendo sempre più approcci pragmatici basati sui propri interessi nazionali, senza posizionarsi chiaramente come partner della Cina o degli Stati Uniti.

La Cina continuerà a perseguire le proprie ambizioni. Questo perpetuerà la rivalità sistemica con gli Stati Uniti.

In Europa, la Cina continuerà a sostenere la Russia sul piano politico, economico e con beni a duplice impiego. Ne trae però vantaggio anche grazie ai rapporti di forza e paga alla Russia per il petrolio e il gas prezzi molto bassi La Russia rappresenta un asso nella manica per la Cina lungo il percorso verso un nuovo ordine mondiale. La Cina continuerà ad adoperarsi per sottrarre gli Stati del Sud globale dalla sfera di influenza degli Stati Uniti o per tenerli lontani, cercando al contempo di svolgere un ruolo di leader nei confronti di questi Stati senza esporsi troppo.

La Cina sotto Xi Jinping continuerà ad ampliare la propria influenza nell'area dell'Asia-Pacifico, cercando di ridurre l'influenza degli Stati Uniti nella regione. Intende aumentare, tramite investimenti, le dipendenze esistenti. Si presenta come un partner affidabile e sfrutta le incertezze causate dagli Stati Uniti, ad esempio con la loro politica doganale, la sospensione degli aiuti allo sviluppo o il rigoroso riorientamento della politica di sicurezza. Interverrà anche a livello politico per influenzare i Governi della regione e reprimere le critiche.

Questa politica va di pari passo con l'ulteriore potenziamento dell'Esercito popolare di liberazione. Entro il 2049 la Cina intende diventare la più grande potenza militare a livello mondiale. La riduzione dei poteri di alcuni quadri potrebbe, tuttavia, indebolire l'Esercito popolare, almeno temporaneamente. Ciononostante, le attività militari della Cina nella regione Asia-Pacifico sono destinate ad aumentare. L'integrazione di Taiwan rimane la priorità, anche se è probabile che la Cina non eserciti ancora pressioni per giungere a una decisione al riguardo. Al momento i rischi politici, militari ed economici sono troppo elevati, ma l'integrazione con Taiwan resta la priorità. Il rischio di un'escalation rimane tuttavia considerevole. La politica estera e di sicurezza imprevedibile degli Stati Uniti continua a rappresentare una sfida anche per la Cina.

CINA: SICUREZZA ECONOMICA

La sicurezza economica e tecnologica fa ormai parte del piano di sicurezza nazionale di molti Stati. Questi ultimi intendono ridurre la propria vulnerabilità economica e rafforzare la propria resilienza, in particolare nei confronti della Cina.

Come per altri Stati, anche la Svizzera è fortemente dipendente dalle catene di approvvigionamento cinesi. La Cina sovvenziona e favorisce le proprie aziende. È il principale produttore di tecnologie fondamentali e domina la produzione e la lavorazione di materie prime critiche. Controlla, ad esempio, l'80-90 per cento della produzione mondiale di terre rare. Dal 2025 i nuovi meccanismi cinesi di controllo delle esportazioni generano incertezze e ritardi nelle consegne, mentre a lungo termine mettono a rischio la sicurezza dell'approvvigionamento di prodotti importanti. Per autorizzare l'esportazione di terre rare, la Cina richiede la divulgazione dettagliata della destinazione d'uso. Grazie a queste informazioni, può identificare le dipendenze e potrebbe sfruttare queste informazioni in modo mirato per applicare sanzioni o adottare misure coercitive.

D'altra parte, la Cina dipende dall'Europa in alcuni ambiti. Le aziende europee forniscono importanti materiali all'avanguardia, prodotti chimici e tecnologie di punta. Tra queste figurano in particolare la tecnologia aerospaziale, le macchine di precisione e le attrezzature per la produzione di semiconduttori. A ciò si aggiungono investimenti e competenze tecnologiche. L'orientamento all'esportazione della sua economia rende la Cina vulnerabile rispetto alla politica commerciale europea. Queste dipendenze limitate, e probabilmente anche la politica doganale americana, hanno portato nel 2025 a relazioni euro-cinesi relativamente stabili.

La Cina è interessata ai risultati conseguiti dalla ricerca e dallo sviluppo della Svizzera. Per consentire trasferimenti di tecnologia verso il proprio Paese, la Cina investe in aziende innovative, recluta talenti e promuove la collaborazione con le istituzioni scientifiche occidentali, ad esempio finanziando borse di ricerca e di studio. Il trasferimento di tecnologia avviene però anche attraverso lo spionaggio. Dal punto di vista della politica di sicurezza, rivestono particolare rilevanza i beni a duplice impiego.

Le tensioni tra Cina ed Europa sono di natura strutturale e, di conseguenza, destinate a perdurare. La Cina non modificherà i propri obiettivi con il 15° piano quinquennale. Continuerà a sfruttare i Paesi esteri come fattore essenziale di supporto all'ammodernamento della propria economia e del proprio esercito nonché per ampliare la propria influenza internazionale. La ricerca e lo sviluppo di Europa e Svizzera restano obiettivi interessanti. La Cina rafforzerà il proprio dominio su beni e materie prime di importanza strategica e grazie alla sua sovraccapacità continuerà a riversare merci sul mercato europeo, mettendo sotto pressione la base industriale europea.

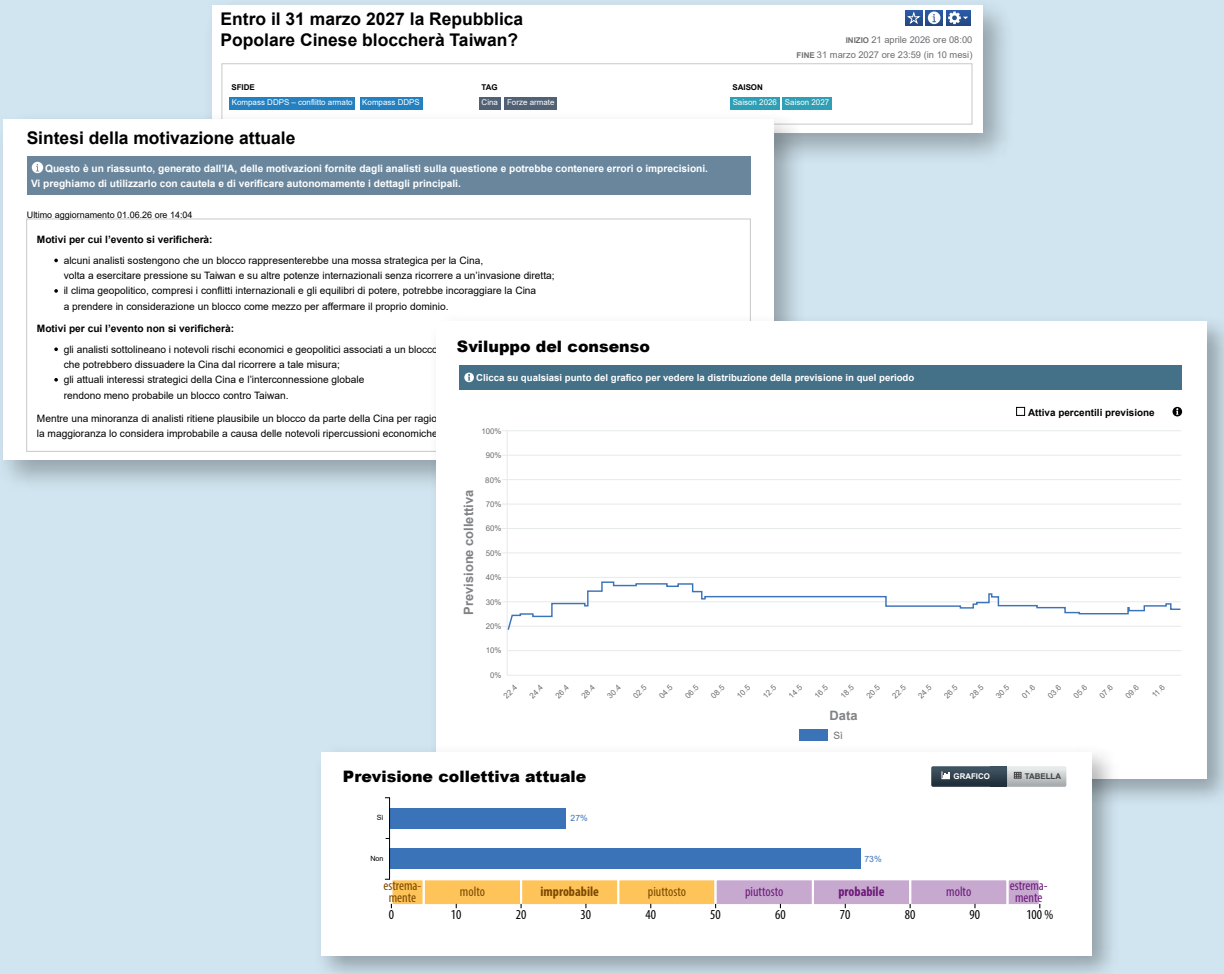
Le tensioni tra Cina ed Europa sono di natura strutturale e, di conseguenza, destinate a perdurare.

Oltre a ciò, la sicurezza economica europea e svizzera continua a dipendere dalle relazioni tra Stati Uniti e Cina. Da un lato, perché le decisioni cinesi, pur essendo rivolte principalmente agli Stati Uniti, hanno ripercussioni anche sull'Europa. Dall'altro lato, è molto probabile che gli Stati Uniti continuino a esercitare pressioni sugli Stati- europei affinché riducano la collaborazione con attori considerati problematici, in particolare le aziende cinesi.

KOMPASS
VBS / DDPS

Dal 2024 il SIC gestisce il «Kompass DDPS», una piattaforma di crowdsourcing. L'obiettivo è quello d'individuare tempestivamente gli sviluppi rilevanti in materia di politica di sicurezza e valutarli. La piattaforma è aperta a tutti i collaboratori dell'Amministrazione federale. Ciò permette di sfruttare la diversità cognitiva, la molteplicità di prospettive e le conoscenze in senso all'Amministrazione. Studi empirici hanno più volte dimostrato l'efficacia di tale approccio. Le previsioni del «Kompass DDPS» vengono elaborate graficamente in modo automatizzato e in parte valutate con l'aiuto dell'intelligenza artificiale (IA). L'IA riassume le motivazioni addotte dagli utenti per la previsione.

L'anno prossimo la Cina implementerà un blocco navale nei confronti di Taiwan? Nel maggio 2026, gli utenti della piattaforma di crowdsourcing ritenevano improbabile questo evento. Secondo loro, i costi economici e politici dissuadono la Cina da tale passo.



VICINO E MEDIO ORIENTE

I conflitti irrisolti continuano a caratterizzare la situazione nel Vicino e Medio Oriente. Al centro di questi conflitti vi è lo scontro tra Israele e gli Stati Uniti da una parte, e l'Iran con i suoi alleati e proxy regionali dall'altra, che si sta svolgendo su diversi fronti.

Nella loro Strategia di Sicurezza Nazionale 2025, gli Stati Uniti hanno dichiarato di voler ridurre il loro focus sul Vicino e Medio Oriente in futuro. Ciononostante, nel febbraio 2026, il presidente Trump ha deciso di sferrare un attacco militare su larga scala contro l'Iran insieme a Israele, puntando a limitarne la capacità di influenza nella regione come obiettivo minimo e a creare le condizioni per un cambio di regime come obiettivo massimo.

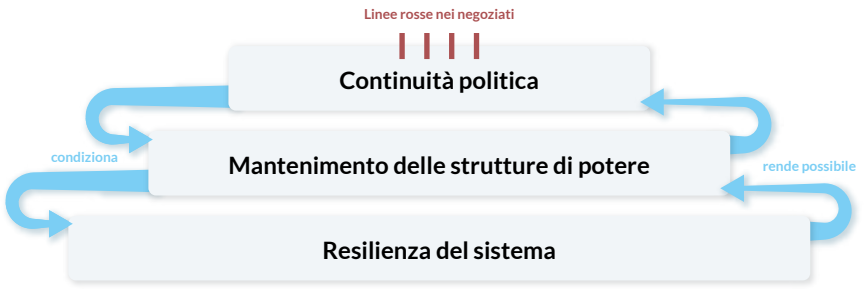
I vertici iraniani hanno reagito in modo sempre più aggressivo, ordinando attacchi mirati in oltre una decina di Stati e determinando di fatto la chiusura dello Stretto di Hormuz. Il coinvolgimento di attori del cosiddetto Asse della resistenza a guida iraniana ha contribuito all'ulteriore regionalizzazione del conflitto. Da parte sua, Israele ha reagito al ripetuto attacco di Hezbollah riprendendo la sua offensiva in Libano su larga scala. L'obiettivo rimane l'annientamento di Hezbollah.

Grazie all'aumento dei prezzi dell'energia e all'allentamento delle sanzioni nel settore petrolifero, la guerra in Iran appare vantaggiosa per la Russia nel breve termine. Sebbene i due Paesi siano legati da un accordo di partenariato strategico dal 2025, il sostegno politico e militare russo all'Iran è rimasto limitato. La Cina vede compromessi i propri interessi, ma modulerà il proprio sostegno in modo tale da poter evitare un deterioramento delle relazioni bilaterali con gli Stati Uniti e gli Stati del Golfo.

A Gaza, nel gennaio 2026 gli Stati Uniti hanno annunciato l'inizio della seconda fase del piano Trump e la nomina del cosiddetto Consiglio di pace (Board of Peace) nonché degli altri organismi preposti alla futura amministrazione della Striscia di Gaza. L'attuazione di tale piano, tuttavia, procede con estrema lentezza. Nonostante l'indebolimento e l'isolamento, Hamas continua a essere la forza palestinese più potente nella Striscia di Gaza.

Il fatto che gli Stati Uniti rimangano l'attore esterno più influente della regione è evidente anche in Siria, dove sostengono il Governo di transizione guidato da Ahmed al-Sharaa, anche a scapito dei loro alleati curdi di lunga data. Sebbene tale governo goda ormai di ampio riconoscimento e legittimità sul piano internazionale, a livello nazionale la sua pretesa di potere continua a essere contestata.

La stabilità del regime in Iran si articola su più livelli



SIC

La guerra contro l'Iran e il suo esito condizioneranno la regione nei prossimi anni. Di particolare importanza è il futuro del regime iraniano: non solo deve contrastare la minaccia militare di Stati Uniti e Israele, ma anche garantire il controllo della propria popolazione, anche alla luce della sanguinosa repressione delle proteste nel gennaio 2026, che ne ha accelerato la perdita di legittimità. Il fattore decisivo sarà la composizione del regime dopo la fine della guerra. La Guida Suprema a lungo al potere, Ali Khamenei, come pure numerosi esponenti politici e militari di spicco sono morti. Se il regime dovesse continuare a esistere, è probabile che cresceranno il potere e l'influenza dei Guardiani della Rivoluzione, che ne sono il pilastro fondamentale. Sebbene abbia dato prova di resilienza durante la guerra in Iran, la sopravvivenza del regime non è garantita a lungo termine. L'obiettivo primario del regime rimarrà quello di garantire la propria sopravvivenza e di conseguenza si porrà inevitabilmente la questione se debba puntare all'armamento nucleare. Nel caso di un colpo di Stato in Iran, è molto probabile che non avverrà in modo pacifico. Se il programma missilistico dovesse proseguire, è prevedibile che nel giro di pochi anni vaste aree dell'Europa, comprese le basi statunitensi presenti sul territorio, rientrino nel raggio d'azione dei sistemi d'arma iraniani.

Se il programma missilistico dovesse proseguire, è prevedibile che nel giro di pochi anni vaste aree dell'Europa, comprese le basi statunitensi presenti sul territorio, rientrino nel raggio d'azione dei sistemi d'arma iraniani.

Israele continuerà a perseguire il suo obiettivo strategico di un cambio di regime in Iran e cercherà di indebolire ulteriormente l'Asse della resistenza, in special modo Hezbollah in Libano, già fortemente minato sul piano militare e politicamente isolato. In tal senso, è probabile che anche in futuro Israele punti anzitutto sulla sua forza militare e finché il presidente Trump sarà in carica, potrà contare su un ampio sostegno statunitense. Tuttavia, poiché sul piano militare, politico ed economico Israele dipende dagli Stati Uniti, è possibile che questi gli impongano dei limiti, come ha dimostrato il presidente Trump durante la guerra a Gaza

Per gli Stati del Golfo, il conflitto nel Vicino e Medio Oriente rappresenta una sfida importante. La guerra mina il loro modello economico, che presuppone stabilità nella regione. Anziché concentrarsi sul proprio sviluppo economico, devono affrontare il problema di come gestire in futuro l'Iran e la minaccia che rappresenta. Molto probabilmente manterranno lo stretto legame con gli Stati Uniti sotto la presidenza Trump. Altrettanto probabile è che gli Stati del Golfo potenzino le loro capacità difensive, il che si tradurrà in un'ulteriore scarsità di beni militari a livello mondiale, in particolare nel settore della difesa aerea e della difesa dai droni. È improbabile che il processo di normalizzazione dei rapporti tra Stati del Golfo e Israele prosegua rapidamente, ad eccezione degli attuali membri degli Accordi di Abramo, poiché Israele è percepito in molti ambienti come una potenza destabilizzante nella regione e non sembra essere disposto a fare concessioni nella sua politica verso i Palestinesi.

Dopo la tregua provvisoria della guerra a Gaza, il suo futuro dipende in larga misura dall'impegno degli Stati Uniti e dalla disponibilità di Hamas a fare concessioni in merito al proprio disarmo. In caso di fallimento, Israele manterrà verosimilmente l'occupazione permanente di parti della Striscia di Gaza, perpetuandone così la divisione in due. Anche la situazione in Cisgiordania, dove le condizioni di vita della popolazione palestinese continuano a peggio-

rare e il controllo israeliano viene esteso fino all'annessione, presenta un rischio di escalation, e un'inversione di tendenza appare molto improbabile.

In Siria, il processo di transizione rimane fragile. Oltre al sostegno internazionale, sarà determinante il successo del Governo di transizione nel raggiungere un equilibrio con le minoranze presenti nel Paese. Se la creazione di una nuova statualità dovesse fallire, c'è il rischio di un'ulteriore frammentazione della Siria o addirittura di una nuova guerra civile. A loro volta, i terroristi cercano di sfruttare gli spazi di manovra che si presentano.

AFRICA

Terrorismo, guerre civili e governi instabili rappresentano una sfida per l'Africa sul piano della di politica di sicurezza. Il terrorismo rimane la principale minaccia. Proviene in particolare da gruppi jihadisti, come Jamaat Nusrat al-Islam wal-Muslimin, affiliato ad Al Qaïda, e dalle province dello «Stato Islamico». Le loro mire espansionistiche esercitano una pressione sempre maggiore su vari Paesi. Dal punto di vista europeo, attualmente la minaccia per i propri cittadini sul posto è in primo piano, poiché né i ripetuti appelli dello «Stato Islamico» a recarsi in Africa né, in alternativa, a compiere attentati nel Paese d'origine trovano riscontro.

La rivalità tra le grandi potenze in Africa si sta intensificando, come dimostrano gli investimenti economici, la presenza militare, le iniziative diplomatiche e l'influenza tecnologica. Gli Stati Uniti stanno rafforzando la loro presenza per contrastare la crescente influenza di Cina e Russia e hanno annunciato un ampio sostegno economico e militare, ad esempio con l'African Growth and Opportunity Act, che garantisce ai Paesi africani un accesso preferenziale al mercato americano. Anche la Cina continua a espandere la propria presenza, in particolare attraverso progetti infrastrutturali. Inoltre, ha concluso accordi commerciali e di investimento di ampia portata con diversi Paesi africani. La Russia aveva in programma di espandere la propria presenza militare in Africa con una base militare in Sudan, destinata a fungere da caposaldo strategico per le operazioni nella regione, ma alla fine del 2025 il progetto è stato «temporaneamente sospeso». La Russia mantiene stretti rapporti con Stati come il Sudafrica, l'Egitto e la Nigeria. Nella regione del Sahel, a seguito di un colpo di Stato, le giunte militari hanno sostituito la presenza militare occidentale con truppe russe e le società minerarie occidentali con aziende russe o cinesi.

Numerosi Stati africani sono afflitti da instabilità politica, se non addirittura da una guerra civile. Conflitti come quelli in Sudan, nella Repubblica Democratica del Congo e nella Repubblica Centrafricana si traducono in crisi umanitarie e sfollamenti e possono portare a un'ulteriore destabilizzazione delle regioni africane, favorire il proliferare di gruppi terroristici e reti criminali come pure contribuire a un aumento dei flussi migratori verso l'Europa. In questo contesto, anche gli sviluppi nei Paesi nordafricani come la Libia, l'Algeria o il Marocco rivestono un ruolo importante.

Tra il 2020 e il 2050 la popolazione africana raddoppierà fino a raggiungere i due miliardi di persone. Oltre al terro-

rismo e ai conflitti, il progressivo cambiamento climatico e le catastrofi ambientali correlate rappresentano una minaccia crescente. Siccità e inondazioni sono causa di insicurezza alimentare, carenza idrica e sfollamenti. Gli eventi meteorologici estremi possono contribuire a disordini e conflitti sociali.

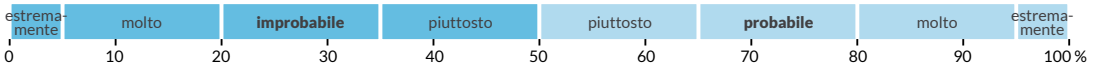
L'Africa rimane un importante teatro della politica di potere globale. Le grandi potenze e le potenze regionali emergenti difendono i loro interessi nella regione attraverso iniziative economiche, diplomatiche e militari. Nei prossimi anni la Cina potrebbe mostrare interesse per basi militari in Tanzania, Madagascar e possibilmente in Guinea equatoriale, sulla costa atlantica. Da parte sua, la Russia punta a potenziare la propria presenza militare, mentre la Turchia ha inviato truppe in Somalia e in Libia. In generale, tuttavia, nel continente si è imposto nuovamente il «non allineamento» quale strategia privilegiata, la quale consente di evitare dipendenze nonché di contendersi aiuti economici e concessioni politiche tra le grandi potenze.

L'Africa rimane un importante teatro della politica di potere globale.

Con la crescente digitalizzazione, le ciberminacce aumentano anche in Africa. I ciberattacchi possono danneggiare infrastrutture critiche come l'approvvigionamento energetico e le comunicazioni. La proliferazione dei droni è un'altra tendenza che rischia di aggravare i conflitti e di destabilizzare ulteriormente l'Africa. La mancanza di infrastrutture come pure le risorse limitate rendono l'Africa particolarmente vulnerabile ai rischi sanitari. I fattori già menzionati, quali gli effetti dei cambiamenti climatici, le carestie, l'aumento degli sfollati interni, i conflitti per le materie prime e le campagne di disinformazione contro l'Europa condotte da attori esterni, aggravano ulteriormente la situazione della sicurezza in diversi Stati africani. Le organizzazioni terroristiche ne trarranno vantaggio, cercando di espandersi territorialmente e di soppiantare le istituzioni statali.

Questi sviluppi e tendenze in Africa non rappresentano una minaccia diretta per la Svizzera, ma nel tempo hanno un impatto sul contesto della politica di sicurezza del nostro Paese. Stanno già gettando le prime ombre sull'Europa e potrebbero trasformarsi in gravi minacce nei prossimi decenni.

Scala delle probabilità



Situazione rilevata dal SIC
Previsioni del SIC

Illustrazione 3

TERRORISMO

LA MINACCIA TERRORISTICA IN SVIZZERA E IN EUROPA

La minaccia terroristica in Svizzera è elevata, il che significa che vi sono indizi della presenza di soggetti terroristi in Svizzera e/o di intenzioni terroristiche nei confronti della Svizzera. La minaccia continua a essere caratterizzata principalmente dal movimento jihadista, soprattutto da persone che simpatizzano con lo «Stato islamico» o che si ispirano alla propaganda jihadista. L'aggressione con coltello avvenuta a Winterthur il 28 maggio 2026, perpetrata da una persona radicalizzata dal jihadismo, conferma questa valutazione.

Il fenomeno della radicalizzazione online è diffuso in Svizzera come in tutta Europa. Nel ciberspazio sono soprattutto i giovani a finire nel vortice dei movimenti estremisti violenti. Contemporaneamente, è sempre più raro che l'influenza di gruppi estremisti violenti e delle loro ideologie sia il motore principale della radicalizzazione online. Altre cause risiedono ad esempio nel fascino diffuso per la violenza, nonché in situazioni personali di crisi e in contesti sociali che incidono in modo particolare sui giovani. Nondimeno, tali processi di radicalizzazione possono sfociare in atti di violenza di ispirazione jihadista.

Nel ciberspazio sono soprattutto i giovani a finire nel vortice dei movimenti estremisti violenti.

Nell'ambito del jihadismo, la propaganda dello «Stato islamico» continua a essere determinante in Svizzera e in Europa. Tuttavia, la maggior parte dei contenuti jihadisti che circolano nel ciberspazio non è più generata da organi mediatici centralizzati dello «Stato islamico», bensì da individui o piccoli gruppi simpatizzanti dello «Stato islamico», che operano in modo autonomo e decentrato.

Dalla metà di maggio 2025 il SIC ha registrato dodici attentati a livello europeo in relazione al terrorismo jihadista. La maggior parte degli attacchi ha coinvolto passanti o assembramenti di persone. Tutti gli attentati sono stati perpetrati con mezzi rudimentali. La maggior parte degli attentatori non era nota alle autorità di sicurezza prima del loro gesto, ma tutti hanno agito in modo autonomo, senza alcun legame diretto con lo «Stato islamico» o con un'altra organizzazione terroristica jihadista. Nessun gruppo jihadista ha rivendicato la responsabilità di questi attentati.

Neanche dopo il vasto attacco terroristico di Hamas del 7 ottobre 2023 il conflitto nel Vicino Oriente rappresenta un motivo conduttore per gli individui radicalizzati dal jihadismo in Svizzera e in Europa. Alimenta tuttavia azioni antisemite che all'estero sono sfociate occasionalmente anche in atti di violenza jihadista, come i recenti attentati del 2 ottobre 2025 contro una comunità ebraica a Manchester (Regno Unito) e del 14 dicembre 2025 durante una celebrazione di Hanukkah a Sydney (Australia). In seguito al conflitto nel Vicino Oriente, più volte sono stati manifestati propositi di attentati in tutta Europa e in diverse occasioni sono stati sventati attacchi pianificati contro obiettivi ebraici o israeliani. Nel contesto di questo conflitto, tanto lo «Stato islamico» quando Al-Qaïda hanno ripetutamente incitato a compiere attentati contro tali obiettivi: è il caso, ad esempio, dello «Stato Islamico», che il 18 settembre 2025 ha esortato esplicitamente i propri giovani seguaci a colpire obiettivi ebraici e cristiani in Europa. L'ultimo appello dello «Stato Islamico» a compiere attentati contro obiettivi ebraici risale al 2 aprile 2026.

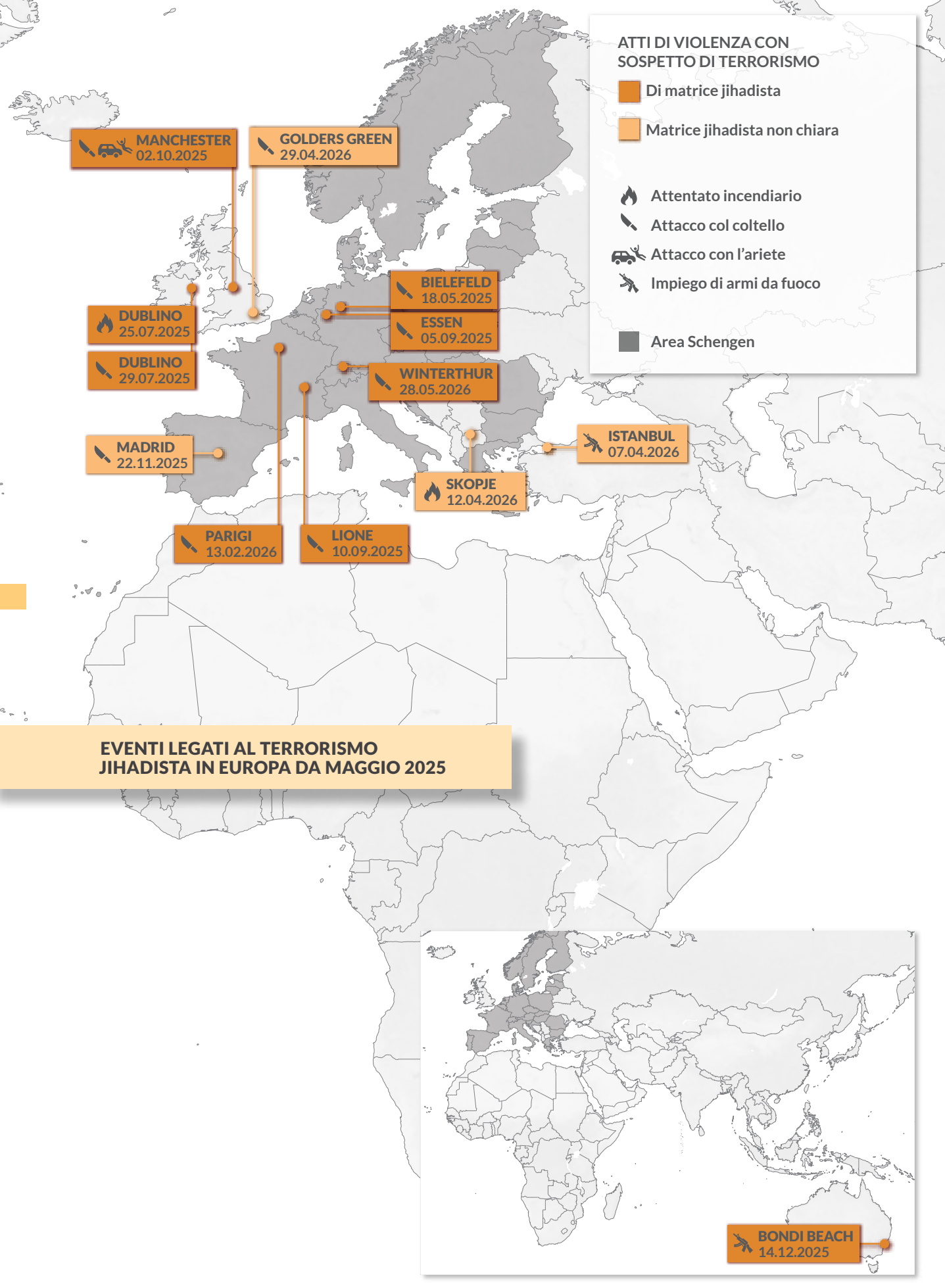
Dal 2022 si registra nuovamente un leggero aumento di «viaggiatori della jihad» provenienti dall'Europa: sono stati individuate diverse decine di casi di persone il cui proposito era di unirsi a un gruppo dello «Stato Islamico» in Africa, Vicino Oriente o Asia. I loro piani sono tuttavia falliti in gran parte a causa delle difficili condizioni generali o dell'intervento delle autorità di sicurezza. In Svizzera l'ultimo caso risale al luglio 2024, quando è stato arrestato un ventunenne svizzero che intendeva aderire allo «Stato islamico» in Somalia. Nel frattempo, decine di persone provenienti dall'Europa, che dal 2014 si sono unite allo «Stato islamico» in Siria e in Iraq come «viaggiatori della jihad», non si trovano più nei campi e nelle prigioni curde del Nord-Est della Siria, ma sono detenute dalle autorità irachene. Tra loro figurano tre cittadini svizzeri. Una cittadina svizzera si trova ancora con la figlia in un campo curdo nel nord-est della Siria.

Il fenomeno della radicalizzazione jihadista online continuerà a influenzare la minaccia terroristica in Svizzera. Tale minaccia rimane diffusa soprattutto nel ciberspazio, poiché nelle persone sospettate sono sempre più spesso il fascino esercitato dalla violenza o i problemi personali o psicologici a fungere da fattori trainanti, mentre le motivazioni ideologiche assumono un'importanza minore. È difficile, inoltre, valutare la gravità delle minacce di violenza, soprattutto quando si tratta di dichiarazioni rilasciate da giovani nel ciberspazio. Inoltre, in Europa sempre più spesso un sospetto iniziale di terrorismo per atti di violenza si rivela falso oppure i motivi non risultano chiaramente di matrice jihadista. Questa tendenza è destinata probabilmente a proseguire.

In Svizzera, la principale minaccia terroristica continua a provenire da singoli individui o piccoli gruppi ispirati al jihadismo, i quali compiono spontaneamente atti di violenza con mezzi semplici. Tali atti tendono a colpire soprattutto obiettivi difficili da proteggere. Le grandi manifestazioni e gli eventi con una forte affluenza negli spazi pubblici rimangono per i jihadisti occasioni ideali attuare i loro piani terroristici.

Il protrarsi dei conflitti nel Vicino e Medio Oriente in cui è coinvolto Israele continua ad aumentare la probabilità di atti di violenza di matrice jihadista contro interessi ebraici o israeliani in Europa. Questo vale anche per la Svizzera.

I jihadisti liberati dal carcere, così come gli individui radicalizzatisi durante la detenzione, rappresentano un fattore di rischio costante. Rimane anche il problema di eventuali ritorni di «viaggiatori della Jihad» che hanno legami con la Svizzera, tanto più che non è chiaro come evolverà la situazione delle persone precedentemente detenute nel Nord-Est della Siria.



EVENTI LEGATI AL TERRORISMO JIHADISTA IN EUROPA DA MAGGIO 2025

LE NUOVE TECNOLOGIE STANNO CAMBIANDO IL VOLTO DELLA MINACCIA TERRORISTICA

Spesso i terroristi reagiscono in modo rapido alle nuove tecnologie, accessibili pubblicamente, poco regolamentate e convenienti o addirittura gratuite. Lo «Stato islamico», ad esempio, ha deciso fin dall'inizio di optare per quelli che al tempo erano i social media e le applicazioni di comunicazione gratuite di ultima generazione, come Telegram, il che si è rivelato un fattore determinante per il successo dell'organizzazione terroristica, in quanto ne ha aumentato in modo significativo le capacità a livello di propaganda, reclutamento e sicurezza delle comunicazioni. Un altro esempio è rappresentato dalle criptovalute, sempre più utilizzate anche dai terroristi.

Lo sviluppo esponenziale dell'intelligenza artificiale, in particolare, può intensificare considerevolmente la minaccia jihadista in futuro. Non è solo il suo uso quotidiano da parte dei jihadisti a essere problematico, ma anche da parte delle aziende tecnologiche nel settore dei social media. L'esperienza dimostra che l'uso dell'intelligenza artificiale negli algoritmi di piattaforme come TikTok favorisce i processi di radicalizzazione.

Lo sviluppo esponenziale dell'intelligenza artificiale, in particolare, può intensificare considerevolmente la minaccia jihadista in futuro.

In futuro l'intelligenza artificiale avrà un impatto su numerosi settori e, soprattutto in combinazione con altre tecnologie, potrebbe comportare nuove sfide nella lotta al terrorismo – ad esempio nel campo della tecnologia dei droni a fini offensivi. Questa tecnologia ha registrato uno sviluppo vertiginoso dall'inizio della guerra contro l'Ucraina ed è in parte liberamente accessibile. Dal 2023 anche gli attori islamisti violenti nel Vicino Oriente, Africa e Asia utilizzano sempre più spesso droni armati. Le capacità di tali attori sono in costante aumento grazie al rapido sviluppo della tecnologia dei droni e all'elevato trasferimento di conoscenze.

A livello internazionale si cerca di contrastare l'abuso delle nuove tecnologie da parte dei terroristi attraverso normative di legge e misure di protezione adottate dalle aziende private. Negli ultimi anni, ad esempio, la regolamentazione statale delle grandi piattaforme online ha compiuto progressi significativi. Di conseguenza, i gestori delle piattaforme hanno adeguato le proprie linee guida e intensificato la lotta contro i contenuti jihadisti. Finora, però, queste misure sono riuscite a contenere appena il fenomeno della radicalizzazione online e questo per vari motivi, non ultimo il fatto che il rapido sviluppo della tecnologia e del mercato in questo settore consente ai jihadisti di ripiegare su prodotti alternativi o di utilizzare nuove tecnologie per dissimulare le loro attività online. Inoltre, le generazioni più giovani acquisiscono più presto e più facilmente nuove competenze tecnologiche.

ATTORI JIHADISTI FUORI DALL'EUROPA

I gruppi terroristici legati allo «Stato islamico» o ad Al-Qaïda influenzano direttamente la situazione di minaccia in Europa attraverso le loro attività di propaganda e di reclutamento. Allo stesso tempo, però, è difficile che siano in grado di preparare o compiere autonomamente attentati in Europa, anzi, poiché dipendono in larga misura dalla possibilità di trovare seguaci che vivano in Europa e che possano essere istigati nonché eventualmente istruiti a compiere atti di violenza.

Lo «Stato islamico» in Siria sta sfruttando il vuoto di potere creatosi dopo la caduta del regime di Bashar al-Assad e la persistente situazione di scarsa sicurezza in ampie zone del Paese per riorganizzarsi e rafforzarsi, in particolare intensificando il reclutamento. L'avanzata dell'esercito siriano nei territori curdi ha provocato ondate di fuga dai campi e dalle prigioni del Nord-Est della Siria. È però piuttosto probabile che lo «Stato islamico» non disponga di risorse sufficienti per accogliere tutte le persone in fuga. I fuggitivi potrebbero anche tentare di tornare in patria, ma per ora non vi è il minimo segnale di un'ondata di rientri.

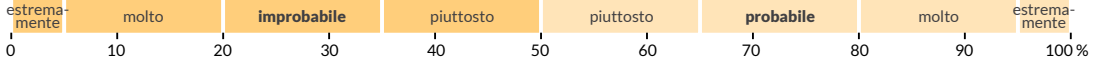
I fuggitivi potrebbero tentare di tornare in patria, ma per ora non vi è il minimo segnale di un'ondata di rientri.

Sebbene il Governo di transizione siriano stia cercando di contrastare i gruppi radicali o di matrice jihadista, come comunicato ufficialmente, la mancanza di controllo in vaste aree della Siria, nonché la carenza di risorse umane e finanziarie, rendono difficile un intervento efficace. Se è presumibile che lo «Stato islamico» possa ancora sferrare attacchi a sorpresa in gran parte facilmente attuabili, ciò non toglie che continuerà a tentare di compiere attentati contro obiettivi sensibili. Tra questi, oltre a rappresentanti del Governo di transizione siriano, figurano in particolare anche cittadini di Paesi occidentali e interessi occidentali in Siria.

In seguito alla forte pressione repressiva esercitata a livello internazionale, le capacità dello «Stato islamico» della Provincia del Khorasan (ISKP), con base in Afghanistan e Pakistan, di realizzare attentati contro obiettivi in Europa hanno toccato il minimo storico nel 2025. Con l'arresto del suo membro Özgür Altun in Pakistan nell'aprile 2025, anche la sua rivista online in lingua inglese «Voice of Khurasan» ha sospeso le pubblicazioni fino a gennaio 2026. Questa rivista offre agli individui radicalizzatisi in Europa con indirizzi di contatto un punto di riferimento diretto. In Europa l'ISKP continua a dipendere dalla capacità di trovare seguaci sul posto che possono essere motivati a compiere atti di violenza. Le sue reti internazionali presentano solo legami marginali con la Svizzera.

In Africa le province dello «Stato islamico» si sono propagate e consolidate a vista d'occhio: nonostante le perdite di personale e materiali dovute a operazioni antiterrorismo, le loro strutture rimangono funzionali e la loro rete praticamente intatta. Le strutture statali, deboli tanto in termini di legittimità quanto di garanzia della sicurezza, offrono condizioni favorevoli alle mire espansionistiche dei gruppi jihadisti. Altri fattori – come gli effetti del cambiamento climatico, le carestie, i flussi migratori, i conflitti etnici, la scarsità di risorse, la crescita demografica, l'influenza militare ed economica nonché le campagne di disinforma-

Scala delle probabilità



zione antieuropea condotte da attori esterni – si rafforzano a vicenda e peggiorano ulteriormente la situazione della sicurezza in diversi Stati africani.

Negli ultimi anni il nucleo di Al-Qaïda e le sue propaggini si sono concentrati principalmente su questioni regionali. Le piattaforme mediatiche di Al-Qaïda e i portali mediatici vicini all'organizzazione diffondono con regolarità appelli a mettere in atto azioni violente negli Stati Uniti e in Europa nonché contro interessi israeliani in tutto il mondo. Rispetto alla propaganda dello «Stato islamico», quella di Al-Qaïda continua tuttavia a suscitare scarso interesse in Europa.

La situazione non subirà cambiamenti significativi fino alla fine del 2026 : è probabile che organizzazioni terroristiche jihadiste nel Vicino Oriente, Africa e Asia continueranno a perseguire anzitutto una strategia regionale. È tuttavia piuttosto probabile che acquisiscano al contempo nuove risorse e potenzino le loro capacità operative, aumentando così la minaccia per gli interessi occidentali nella regione.

È molto probabile che lo «Stato islamico» in Siria sfrutti la situazione di instabilità e le crescenti animosità tra i diversi gruppi di popolazione per favorire la propria ripresa e che così rafforzato riesca a motivare all'adesione individui radicalizzati, non solo in Siria. I contatti a livello nazionale con le sue province gli facilitano il trasferimento di combattenti, competenze e risorse finanziarie. Sussistono contatti sporadici con l'Europa, i quali potrebbero sempre aumentare in futuro e accrescere così il potenziale di minaccia per la Svizzera e l'Europa. Gli individui rientrati da aree a presenza jihadista rappresentano una minaccia anche per la sicurezza dell'Europa, compresa quella della Svizzera.

Si moltiplicano gli indizi che lasciano presupporre che l'ISKP sia in fase di riorganizzazione e che l'indebolimento delle sue reti internazionali sia stato solo temporaneo, ma anche qualora dovesse riuscire a ricostruire tali reti nonché il suo apparato di propaganda, avrà comunque bisogno di tempo per tornare ai livelli del 2024.

È probabile che le province africane dello «Stato islamico» e le propaggini africane di Al-Qaïda continueranno a trarre vantaggio dal miglioramento delle condizioni generali, intensificando così il reclutamento e l'approvvigionamento di risorse finanziarie e materiali.

LOTTA AL TERRORISMO

Due volte all'anno il SIC pubblica sulla propria pagina Internet i dati inerenti alla lotta al terrorismo (persone che rappresentano un rischio, viaggiatori con finalità jihadiste, monitoraggio di siti Internet dal contenuto jihadista).

www.sic.admin.ch
> Sicurezza > Attività informative > Terrorismo

PKK

Nel maggio 2025 il Partito dei lavoratori del Kurdistan (PKK) ha annunciato il suo scioglimento, cui ha fatto seguito una serie di gesti simbolici di grande risonanza mediatica. Tuttavia, le sue strutture continuano a esistere e rimangono attive. Il PKK, quale rappresentante autoproclamato delle donne e degli uomini curdi in Europa, mira al riconoscimento dell'identità curda in Turchia, Siria, Iraq e Iran. In Svizzera, così come in altre parti d'Europa, continua a raccogliere fondi in segreto, a fare propaganda e a organizzare campi per la formazione ideologica e i reclutamenti.

Il PKK continua a perseguire l'obiettivo di essere rimosso dall'elenco dei soggetti terroristici dell'UE. Continuerà molto probabilmente a mantenere un approccio non violento in Europa, pur proseguendo le sue attività, in parte segrete. Cerca al contempo di evitare lotte di potere interne e spaccature a seguito dell'annunciato scioglimento. A seconda delle pressioni esercitate dal Governo turco e dell'evoluzione della situazione, in particolare nei territori curdi della Siria settentrionale, sono attese tensioni e proteste anche in Svizzera.

TERRORISMO DI PROVENIENZA ETNO-NAZIONALISTA E DI ALTRA PROVENIENZA

HAMAS

Il 15 maggio 2025 è entrata in vigore la legge federale che vieta Hamas e le organizzazioni associate, la quale fornisce alle autorità federali gli strumenti necessari per contrastare le attività di Hamas o il sostegno all'organizzazione – in particolare attraverso finanziamenti e propaganda – sul territorio svizzero. Ufficialmente Hamas non contempla atti terroristici in Europa, tali azioni non rientrano nella sua dottrina. La rete internazionale di Hamas si concentra principalmente su questioni politiche e finanziarie. Ci sono rapporti relativi a preparazione di attentati in Europa alla fine del 2023 e nel 2025, ma i collegamenti tra questi individui e Hamas non sono ancora chiari. Negli ultimi anni, tuttavia, alcuni dirigenti di Hamas hanno esortato ad attaccare israeliani ed ebrei al di fuori di Israele e dei territori palestinesi.

Qualora vi fosse la conferma di attentati pianificati da Hamas in Europa, ciò significherebbe una nuova minaccia per gli interessi ebraici e israeliani anche nel nostro Paese. Al momento è piuttosto improbabile che Hamas o una parte di tale organizzazione compia un attentato terroristico in Europa.

Situazione rilevata dal SIC
Previsioni del SIC

IRAN

Negli ultimi anni i servizi di intelligence iraniani e diversi proxy iraniani sono stati coinvolti nella preparazione di attività terroristiche in Europa.

L'Iran potrebbe reagire in modo asimmetrico agli attacchi israeliani e americani. Tra i metodi asimmetrici rientrano gli attacchi terroristici, ad esempio contro obiettivi israeliani, ebraici o americani, che potrebbero essere perpetrati dai servizi iraniani, dai proxy o da reti criminali incaricate. È inoltre probabile che i servizi di intelligence iraniani intensifichino la sorveglianza sui membri dell'opposizione iraniana residenti in Svizzera e adottino un approccio più aggressivo nei loro confronti, come minacce o anche lesioni personali.

Inoltre, individui radicalizzati che condividono l'ideologia del regime iraniano, ma che non sono collegati a esso a livello organizzativo, potrebbero compiere azioni spontanee, dirette principalmente contro obiettivi opportunistici.

HEZBOLLAH

Nella comunità sciita della diaspora libanese in Svizzera, Hezbollah dispone di una rete di persone che sostengono l'organizzazione sul piano comunitario e politico. Alcuni di questi individui potrebbero essere mobilitati anche per fornire supporto a Hezbollah in caso di azioni terroristiche. Nel dicembre 2024 entrambe le Camere federali hanno approvato una mozione volta a vietare Hezbollah in Svizzera, incaricando il Consiglio federale di attuarla.

La minaccia per l'Europa rappresentata dagli Hezbollah libanesi continua a dipendere dall'intensità dei conflitti, da un lato tra Israele e Hezbollah, dall'altro tra l'Iran e gli Stati che esso considera suoi nemici. Sebbene Hezbollah potrebbe estendere il conflitto con attentati al di fuori del Vicino Oriente, è più probabile che si concentri su operazioni sul territorio libanese e contro l'esercito israeliano.

Situazione rilevata dal SIC
Previsioni del SIC

Illustrazione 4

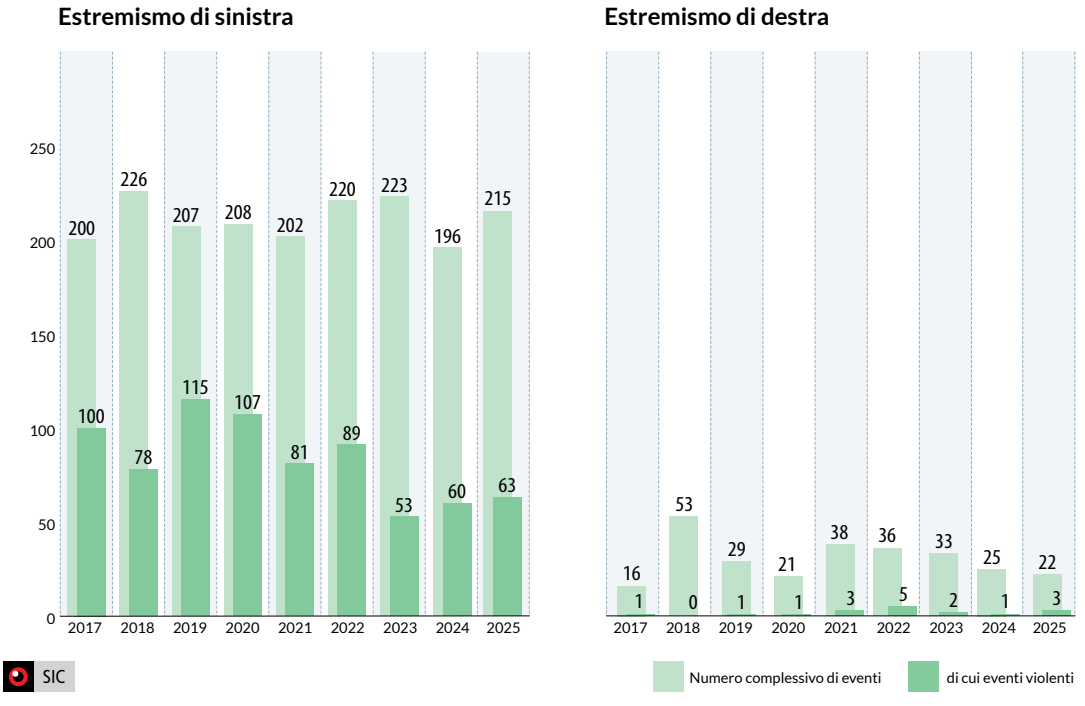
ESTREMISMO VIOLENTO

IL POTENZIALE DI VIOLENZA RIMANE ELEVATO

Gli estremisti violenti di sinistra e di destra proseguono le loro attività, confermando gli sviluppi osservati negli ultimi anni: entrambi gli ambienti si concentrano in linea di principio sulle tematiche affrontate da anni e a utilizzare le loro tipiche modalità d'azione per attirare l'attenzione sulle loro rivendicazioni. La violenza visibile pubblicamente proviene prevalentemente da esponenti degli ambienti estremisti di sinistra. Nessuno dei due ambienti dell'estremismo violento sembra in grado di indebolire in modo evidente la democrazia e i principi dello Stato di diritto, né di influenzare in modo significativo i processi politici. In entrambe le fazioni, i rappresentanti frequentano corsi di arti marziali.

Il potenziale di violenza negli ambienti dell'estremismo violento di sinistra è elevato. Attualmente il tema dominante è quello del conflitto in Vicino e Medio Oriente con le sue molteplici sfaccettature come la causa palestinese o curda nonché l'antiimperialismo e l'anticapitalismo. Questi temi si prestano bene anche per mobilitare diverse persone non violente a partecipare a manifestazioni di protesta. Gli ambienti dell'estremismo violento di sinistra strumentalizzano queste manifestazioni quali piattaforme per esercitare violenza. Gli atti di violenza si rivolgono soprattutto contro istituzioni che vengono associate agli Stati Uniti o a Israele oppure alla fornitura di armi e al finanziamento di questi Stati. Ad esempio, il gruppo Palestine Action, vietato nel Regno Unito, incita in tutto il mondo ad azioni violente contro le aziende produttrici di armi e i ministeri della difesa. Oltre a ciò, la lotta contro il fascismo continua ad avere la massima

Eventi di matrice estremista violenta notificati al SIC dal 2017
(senza gli imbrattamenti)



priorità. Gli eventi che si stanno attualmente verificando sulla scena mondiale influenzano le attività degli ambienti dell'estremismo violento di sinistra in misura maggiore rispetto a quelle degli ambienti dell'estremismo violento di destra. Proprio i grandi eventi a forte connotazione economica, come il World Economic Forum (WEF) o un vertice del G7, richiedono ripetutamente l'impiego di ingenti risorse da parte delle autorità di sicurezza, compresa la rete informativa integrata del SIC *(cfr. «indicatori 2025», p. 73)*, al fine di garantire la sicurezza contro questo potenziale di violenza.

Singoli gruppi dell'estremismo violento di destra guadagnano spesso visibilità con le loro azioni e diffondono videoregistrazioni di tali attività su canali online liberamente accessibili. Alcuni individui appartenenti agli ambienti violenti di estrema destra ricorrono alla violenza contro uomini che accusano di pedofilia.

In Svizzera vi sono alcuni obiettori dello Stato che non rispettano né riconoscono le autorità statali e rifiutano in linea di principio la legittimità dello Stato di diritto democratico. Alcune di esse sono di estrema destra e violente, e si oppongono con la forza agli atti di sovranità compiuti dagli organi statali.

L'evoluzione della situazione nel campo dell'estremismo violento ha indotto il Consiglio federale, nell'ambito della revisione in corso della legge sulle attività informative, a introdurre le cosiddette misure di acquisizione soggette ad autorizzazione, quali ad esempio la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, l'impiego di apparecchi di localizzazione e di altri apparecchi di sorveglianza anche in luoghi privati o non accessibili al pubblico, o l'infiltrazione in sistemi e reti informatiche, anche al fine di individuare o scongiurare minacce derivanti da attività dell'estremismo violento.

Entrambi gli ambienti dell'estremismo violento presenti in Svizzera proseguiranno le loro attività. Sostanzialmente si orienteranno verso i temi prioritari finora perseguiti.

I temi legati al conflitto nel Vicino e Medio Oriente, e in particolare la causa palestinese, continuano ad acquisire rilevanza per gli ambienti dell'estremismo violento di sinistra dando loro nuovo slancio. Se il conflitto nel Vicino e Medio Oriente non si attenuerà in modo significativo, rimarranno attivi gruppi che non esitano a impiegare la violenza durante le manifestazioni. Lo hanno dimostrato chiaramente gli scontri violenti durante la manifestazione a favore della Palestina a Berna nell'ottobre 2025, che hanno causato numerosi feriti e ingenti danni materiali: gli autori delle violenze, tra cui molti provenienti dalla Svizzera romanda, non hanno esitato a sferrare attacchi diretti contro le persone, aggredendo le forze di sicurezza e mettendo in pericolo i passanti. Resta da vedere se le voci che condannano gli atti di violenza acquisiranno un peso rilevante all'interno degli ambienti estremisti di sinistra; questo dibattito evidenzia tuttavia che questi ultimi sono ampi e diversificati.

I temi legati al conflitto nel Vicino e Medio Oriente, e in particolare la causa palestinese, continuano ad acquisire rilevanza per gli ambienti dell'estremismo violento di sinistra dando loro nuovo slancio.

Anche nelle azioni contro aziende economiche e infrastrutture ferroviarie o fornitori di servizi di telecomunicazione in Svizzera e in altri Paesi europei, la violenza e il sabotaggio sono considerati mezzi efficaci, come ha dimostrato l'attacco incendiario di un gruppo anarchico a una centrale elettrica di Berlino nel gennaio 2026. Nonostante la causa curda sia meno presente, per la frangia estremista violenta di sinistra rimane importante.

Gli estremisti violenti di sinistra limitano ripetutamente e direttamente i processi democratici, disturbando o addirittura impedendo le apparizioni di magistrati e imprenditori. I cambiamenti della situazione internazionale sono un'occasione di mobilitazione.

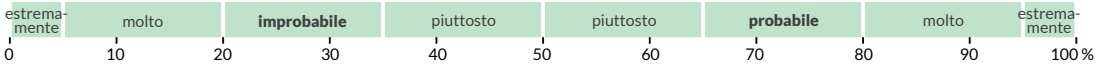
Rispetto agli anni precedenti, gli esponenti degli ambienti dell'estremismo violento di destra si presentano spesso in modo più discreto e sono più ponderati nel modo di esprimersi; questo attira nuovi adepti verso i singoli gruppi. La minaccia rappresentata dagli estremisti violenti di destra rimane, gli individui che operano al di fuori delle strutture organizzate dell'estremismo violento di destra rappresentano una minaccia più importante rispetto a singoli gruppi nel loro insieme. Continuano ad aumentare in particolare i casi di giovani adulti o minorenni che si radicalizzano online, ad esempio attraverso i social media e nelle piattaforme di gioco. Lo spazio digitale rimane centrale per la diffusione della propaganda.

Nei gruppi di discussione chiusi legati all'accelerazionismo continuano a essere condivise rappresentazioni estreme della violenza nonché espresse intenzioni di ricorrere ad azioni violente. I sostenitori dell'accelerazionismo ritengono che la società democratica sia destinata al declino e che il suo crollo debba essere accelerato con la forza per instaurare un nuovo ordine autoritario. La tendenza va tuttavia verso reti online che mescolano elementi ideologici con la rappresentazione di occultismo e crudeltà. L'aspetto ideologico passa sempre più in secondo piano e serve solo a legittimare la violenza.

L'interesse già elevato da parte degli estremisti di destra violenti per gli allenamenti negli sport di combattimento dovrebbe rimanere invariato o addirittura aumentare.

Singoli obiettori dello Stato continueranno a opporsi agli atti di sovranità, ricorrendo in alcuni casi anche alla violenza.

Scala delle probabilità



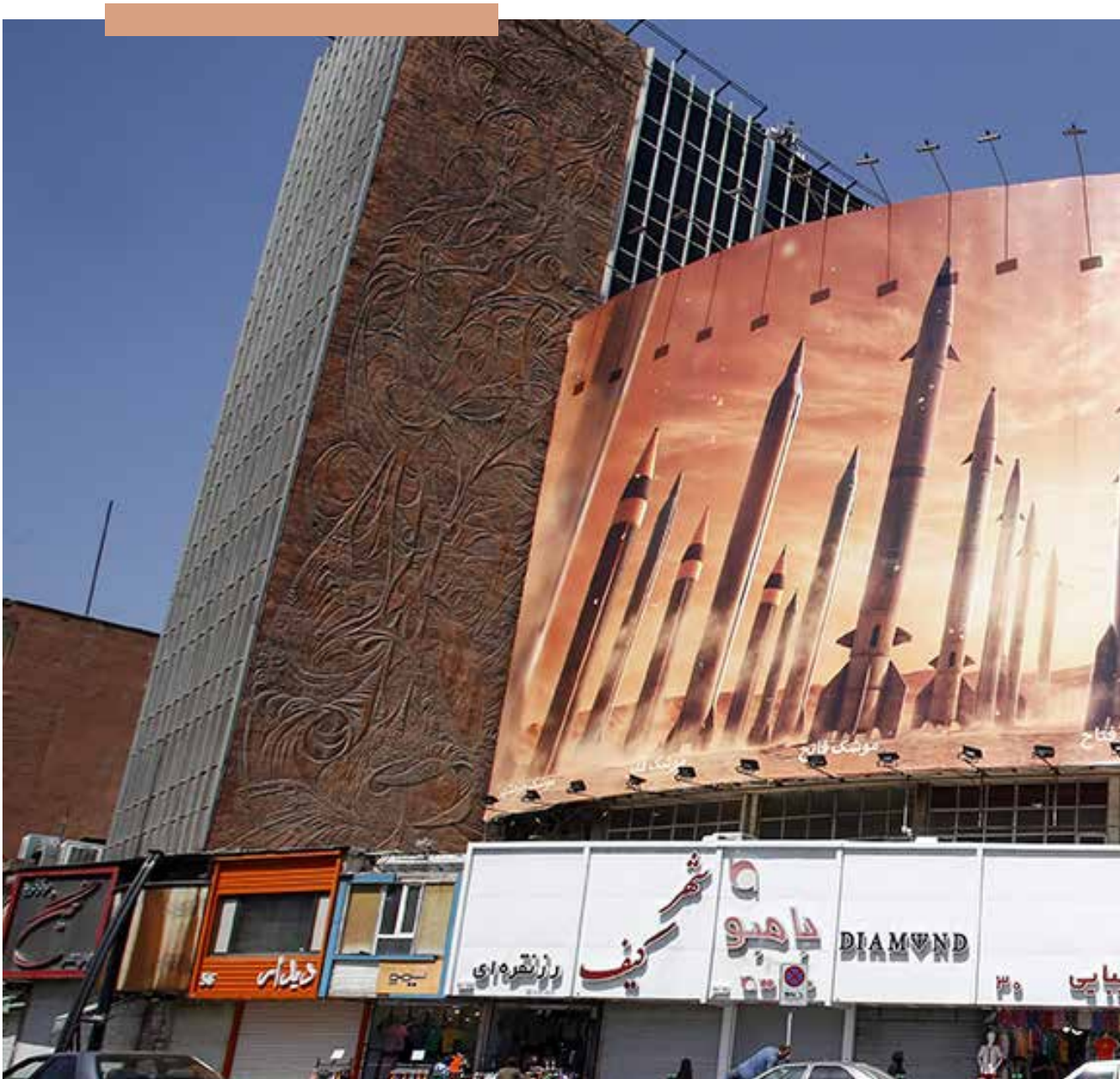


Illustrazione 5

PROLIFERAZIONE

SITUAZIONE GENERALE

La tendenza globale al riarmo si manifesta sia nel campo delle armi convenzionali sia in quello delle armi nucleari, biologiche e chimiche e dei relativi vettori. Gli Stati investono somme ingenti nel potenziamento e nell'ammodernamento di tali armi, accentuando così anche l'importanza strategica delle tecnologie chiave: diversi attori statali cercano di accedere ad esempio alla tecnologia quantistica, all'intelligenza artificiale, alla robotica, alla biotecnologia e alla tecnologia spaziale e vogliono impedire tale accesso ad altri attori statali.

In quanto polo industriale e di ricerca ad alto grado di specializzazione, la Svizzera è particolarmente coinvolta da questi processi. Ad esempio, la Russia fa in modo di aggirare le sanzioni e di acquistare macchine utensili in Svizzera a favore del suo complesso militare-industriale. A sua volta, la Cina cerca nel nostro Paese conoscenze e tecnologie con potenziale strategico e militare. Anche l'Iran e la Corea del Nord sono interessati ai beni svizzeri per i loro programmi di armamento strategico.

Le reti e le modalità di approvvigionamento diventano sempre più complesse e difficili da individuare. I meccanismi e gli strumenti per la lotta contro la proliferazione si sono indeboliti a livello internazionale, poiché il multilateralismo è stato messo in discussione. La Russia e gli interessi sempre più divergenti dei vari Paesi impediscono di sviluppare adeguatamente i regimi di controllo delle esportazioni. Inoltre, lo sviluppo di diverse tecnologie potenzialmente rivoluzionarie rende la lotta contro la proliferazione notevolmente più complessa, come risulta evidente in diversi ambiti: gli elenchi di beni a duplice impiego stanno diventando sempre più lunghi e complessi e si crea un conflitto tra la ricerca scientifica internazionale e la tutela degli interessi nazionali. In questo scenario gli interessi economici sono sempre più esposti ai rischi della proliferazione.

A livello globale, la concorrenza industriale e tecnologica è destinata a persistere: gran parte degli Stati occidentali continuerà a cercare di impedire alla Russia di acquisire nuove capacità militari e di ostacolare la Cina nell'ottenere vantaggi tecnologici decisivi. Tutte le parti eserciteranno ancora una forte pressione sulla Svizzera, rendendo sempre più complesso mantenere la sovranità nella lotta contro la proliferazione e nel controllo delle esportazioni. Gli strumenti tradizionali del controllo degli armamenti perderanno ulteriore importanza. In Svizzera le reti di approvvigionamento restano attive.

Tutte le parti eserciteranno ancora una forte pressione sulla Svizzera.

RUSSIA

La Russia continua ad ammodernare il proprio arsenale nucleare, in particolare i vettori; i problemi relativi allo sviluppo di un missile balistico intercontinentale pesante non sono però ancora risolti. Anche l'ultimo test del 2025 è fallito.

I droni svolgono un ruolo decisivo nella guerra contro l'Ucraina, ma non sostituiscono completamente le armi a distanza tradizionali come l'artiglieria, i missili balistici e i missili da crociera, con conseguente accelerazione dello sviluppo di questi sistemi d'arma come pure della guerra elettronica. Ne deriva una forte domanda di beni industriali, che la Russia deve in parte procurarsi anche negli Stati occidentali.

La Russia ha elaborato strategie complesse per promuovere i suoi sforzi bellici anche avvalendosi di beni e tecnologie svizzeri, tra cui l'impiego dei propri servizi di intelligence o di reti di approvvigionamento specifiche in Svizzera e all'estero. Si osserva un aumento della frequenza di trasmissione di merci svizzere da Paesi terzi verso la Russia. Lo stesso vale per l'utilizzo di prodotti svizzeri per fabbricare merci destinate alla Russia in Paesi terzi. I Paesi che non hanno adottato le sanzioni contro la Russia, come la Turchia, gli Emirati Arabi Uniti e la Cina, vengono utilizzati per aggirare sanzioni e misure di controllo all'esportazione di beni a duplice impiego. Particolarmente coinvolti sono l'industria delle macchine utensili, il materiale da laboratorio e anche settori come la microtecnica.

La Russia non dichiara più i voli di prova di missili balistici, contrariamente a quanto previsto dal Codice di condotta dell'Aia, e in Ucraina ha utilizzato a più riprese l'arma chimica cloropicrina. Tali violazioni del diritto internazionale e di altre normative hanno un effetto destabilizzate e testimoniano l'erosione degli accordi multilaterali.

La Russia continuerà ad adoperarsi per rifornire il proprio complesso militare-industriale con beni e tecnologie svizzeri. È probabile che incrementerà ulteriormente il ricorso a Paesi terzi per aggirare le sanzioni e le disposizioni riguardanti i beni a duplice impiego. I beni svizzeri possono essere riesportati da tali Paesi terzi oppure possono essere prodotti in loco con l'ausilio di beni e tecnologie svizzeri per poi essere consegnati alla Russia.

La Russia continuerà ad adoperarsi per rifornire il proprio complesso militare-industriale con beni e tecnologie svizzeri.

Gli Stati che sostengono militarmente l'Ucraina e lavorano per indebolire la Russia potrebbero considerare insufficiente l'attuazione delle sanzioni contro la Russia da parte della Svizzera, con possibili conseguenze negative per l'economia e la cooperazione in materia di politica di sicurezza.

La Russia non tornerà a rispettare gli accordi internazionali in tempi brevi. Il trattato New Start che ha sottoscritto con gli Stati Uniti sulla limitazione delle armi nucleari strategiche, ad esempio, è scaduto nel febbraio 2026. La Russia continuerà invece a lavorare all'ammodernamento del proprio arsenale di missili balistici intercontinentali e utilizzerà i test riusciti di questi sistemi vettori a fini propagandistici.

Situazione rilevata dal SIC
Previsioni del SIC

CINA

La Cina sfrutta i propri vantaggi economici come leva geopolitica. La strategia di fusione civile-militare elaborata dal capo di Stato e di Partito Xi Jinping promuove l'utilizzo di tecnologie potenzialmente rivoluzionarie per scopi militari. Di conseguenza, i controlli sulle esportazioni armonizzati a livello internazionale di beni a duplice impiego e la sicurezza delle conoscenze acquisiscono maggiore importanza, mentre il blocco e l'indebolimento del regime tradizionale multilaterale di controllo delle esportazioni favorisce la strategia cinese.

Per molti Paesi, Svizzera compresa, la Cina rappresenta un partner commerciale e tecnologico importante se non addirittura indispensabile. La cooperazione in ambito commerciale e scientifico è proficua sotto molti aspetti, ma non priva di rischi. Grazie all'elevato grado di specializzazione, l'industria e il potenziale innovativo del nostro Paese offrono opportunità particolarmente interessanti per le acquisizioni tecnologiche.

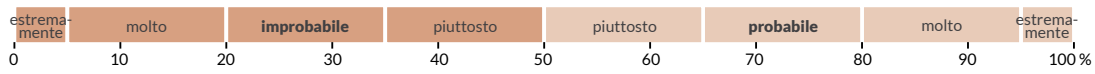
Gli attori cinesi interessati all'acquisizione di conoscenze e tecnologie svizzere possono ricorrere a un'ampia gamma di metodi legali e illegali:

- Spionaggio, furto di proprietà intellettuale e abuso della cooperazione scientifica sono una realtà per gli istituti di ricerca, le università, le imprese industriali, le start-up e gli spin-off svizzeri.

- L'acquisizione di conoscenze con mezzi legali rappresenta una sfida ancora maggiore, poiché risulta difficile limitare l'espansione delle acquisizioni di conoscenze tecnologiche attraverso l'esportazione di beni, come pure degli investimenti esteri nelle aziende, della cooperazione nella ricerca accademica, delle borse di studio per la ricerca o del reclutamento di talenti. Gli attori cinesi attivi in questi settori approfittano della loro solida conoscenza delle basi giuridiche e delle disposizioni locali.

Dal 2010 la Cina sta potenziando notevolmente il suo arsenale nucleare, e ne sta ammodernando la qualità grazie a nuovi sistemi d'arma. Non è ancora chiaro fino a che punto intenda spingersi in questa direzione: ufficialmente, rimane fedele alla sua dottrina di non ricorrere per prima alle armi nucleari.

Scala delle probabilità



Sul piano politico, economico e scientifico in Europa vengono potenziati gli sforzi per controllare il trasferimento di tecnologia all'estero, in particolare verso la Cina. Nonostante alcune iniziative incoraggianti, oggi le misure e i meccanismi volti a garantire la sicurezza delle conoscenze e la verifica degli investimenti in Svizzera si trovano ad affrontare sfide sempre più impegnative, vista la crescente complessità dei metodi indesiderati di acquisizione delle tecnologie. Le lacune che rimangono potrebbero essere sfruttate da attori malintenzionati. Un aumento dei relativi incidenti in relazione con l'acquisizione illegale di tecnologia nazionale o estera sul suo territorio non solo comporterebbe danni di reputazione, ma potrebbe anche indebolire la disponibilità di cooperazione di partner internazionali, con ripercussioni sul potenziale di innovazione e di ricerca del Paese.

Sul piano politico, economico e scientifico in Europa vengono potenziati gli sforzi per controllare il trasferimento di tecnologia all'estero, in particolare verso la Cina.

La Cina continuerà a potenziare e ad ammodernare il suo arsenale nucleare. Ufficialmente, il Paese mira a un livello minimo di deterrenza; all'esterno però non è dato sapere che cosa significhi tale affermazione. L'armamento e i dubbi sulle intenzioni della Cina potrebbero motivare in particolare India e Stati Uniti a potenziare i propri arsenali. Questo complica anche i negoziati bilaterali sul disarmo tra Stati Uniti e Russia.

IRAN

Gli attacchi israeliani e americani su siti del programma nucleare iraniano hanno bloccato, perlomeno temporaneamente, la capacità dell'Iran di arricchire l'uranio. Inoltre, sono state distrutte alcune installazioni chiave che avrebbero facilitato un orientamento militare del programma nucleare qualora fosse stata presa una decisione in tal senso. Nonostante l'uccisione mirata di diversi scienziati nucleari di alto rango, l'Iran dispone ancora di un know-how sufficiente per riprendere il suo programma nucleare. La permanenza di circa 440 chili di uranio arricchito al 60 per cento rimane in parte poco chiara.

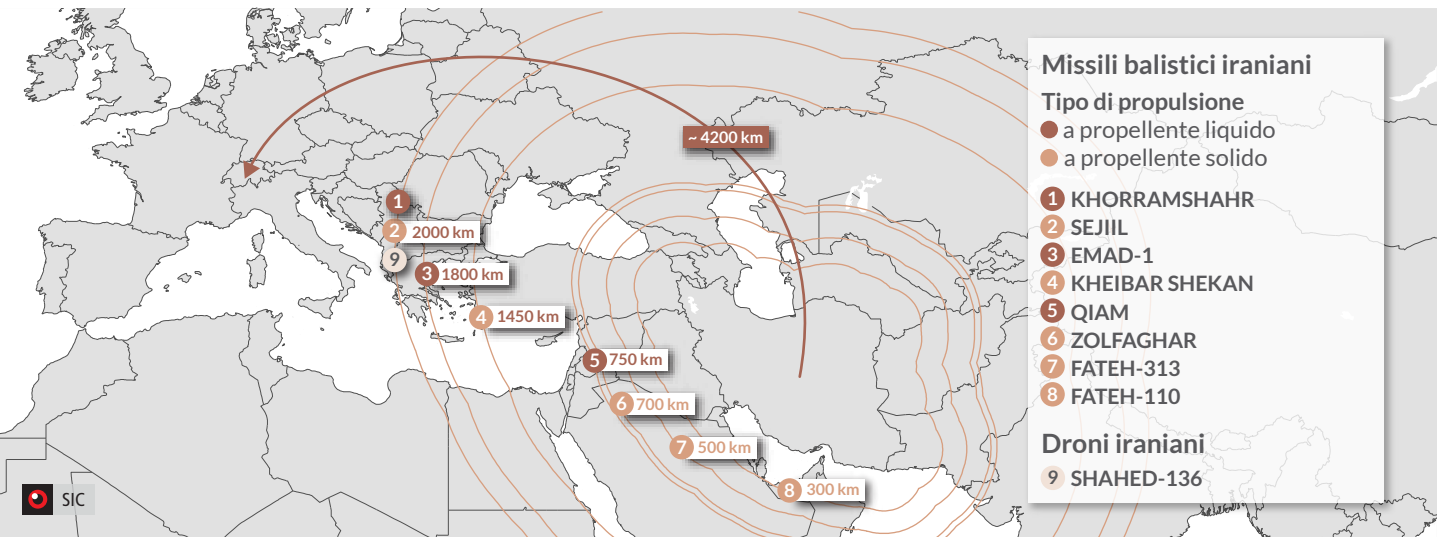
A prescindere dalla ricostruzione delle capacità distrutte nel 2024 e nel 2025, continuano i tentativi di approvvigionamento iraniani in Svizzera. Sebbene l'Iran sia riuscito a ridurre la propria dipendenza dagli Stati occidentali per diverse tecnologie chiave, l'approvvigionamento di beni occidentali rimane comunque interessante per l'Iran a causa delle esperienze passate o delle caratteristiche tecniche. Laddove possibile, l'Iran acquisterà beni altrove.

L'intensificarsi delle sanzioni contro l'Iran e gli scontri militari con Israele e gli Stati Uniti rafforzeranno i suoi legami economici e militari con Stati non occidentali. Considerata la persistente vulnerabilità strategica dell'Iran, i danni considerevoli al programma nucleare e i conseguenti alti costi di ricostruzione rafforzano l'importanza del programma missilistico come mezzo di deterrenza, che continua a rappresentare una minaccia sostanziale in particolare per Israele. Se in futuro la gittata dei missili dovesse aumentare – cosa che, alla luce dell'esperienza maturata con il suo programma spaziale, sarebbe rapidamente realizzabile – l'Iran potrebbe minacciare direttamente l'Europa centrale con i propri missili guidati.

Se in futuro la gittata dei missili dovesse aumentare l'Iran potrebbe minacciare direttamente l'Europa centrale con i propri missili guidati.

Il programma nucleare riveste grande importanza per il regime attuale, per cui è improbabile che l'Iran lo interrompa completamente. La minaccia che ne deriva dipende in primo luogo dalla capacità dell'Iran di mettere in salvo le scorte esistenti di uranio altamente arricchito, ma in ogni caso la nuova Guida Suprema dovrebbe prima decidere in tal senso.

Gittata stimata di alcuni missili iraniani



COREA DEL NORD

Sul piano politico la Corea del Nord non è più così isolata come lo era anni fa. Nel settembre 2025, ad esempio, il leader nordcoreano Kim Jong-un si è intrattenuto a Pechino sia con il Presidente russo sia con altri capi di Stato dei Paesi del Sud del mondo. La visita ha permesso alla Corea del Nord di migliorare le relazioni con la Cina, tese a causa della ratifica di un trattato di alleanza con la Russia e dell'invio di truppe a sostegno di quest'ultima nella guerra contro l'Ucraina. La Cina rimane di gran lunga il partner commerciale più importante per la Corea del Nord.

Ciononostante, la Corea del Nord ha intensificato ulteriormente la cooperazione con la Russia, continuando a fornirle missili balistici a corto raggio e collaborando strettamente nel settore dei droni. È probabile che la Corea del Nord supporti la Russia nella produzione di droni del tipo Shahed-136, originariamente prodotti dall'Iran, acquisendo essa stessa know-how e tecnologia per la fabbricazione di tali droni. È altrettanto probabile che la Russia supporti a sua volta la Corea del Nord nella formazione dei piloti di droni.

La Corea del Nord prosegue il suo programma nucleare e continua a produrre uranio arricchito e plutonio. Nel 2025 ha effettuato almeno 14 test missilistici, lanciando oltre 24 missili, un numero comunque nettamente inferiore rispetto agli anni precedenti. Anche questa volta i test hanno riguardato principalmente sistemi a corto raggio a propulsione solida in grado di trasportare testate nucleari, missili da crociera e missili per la difesa aerea. A differenza degli anni precedenti, invece, la Corea del Nord non ha testato missili balistici intercontinentali.

Si registrano puntualmente tentativi di approvvigionamento di beni svizzeri per i quali non è disponibile un sostituto adeguato in Cina.

Nonostante il miglioramento delle relazioni con la Cina, la Corea del Nord manterrà la sua libertà di azione. Se necessario, continuerà a supportare la Russia con truppe e munizioni. Kim Jong-un sarà poco incline a incontrare il Presidente americano, almeno finché quest'ultimo continuerà a insistere sulla richiesta che la Corea del Nord rinunci alle armi nucleari.

Nel 2026 la Corea del Nord presenterà il suo nuovo piano quinquennale, in cui ribadirà la sua intenzione di sviluppare una capacità autonoma di ricognizione satellitare. A tal fine, tra le altre cose, continuerà a perfezionare il suo vettore satellitare, differenziandolo maggiormente dai suoi missili balistici. Proseguirà anche i programmi di armamento strategico, in particolare riguardo alle tecnologie avanzate per i veicoli di rientro, ai sottomarini a propulsione nucleare e ai sistemi di droni. La Corea del Nord continuerà anche a rendere operativi i sistemi vettori a propulsione solida in tutte le categorie di raggio.

Nei confronti della Corea del Sud, dove si è insediato un Presidente aperto al dialogo, la Corea del Nord adotterà comunque una linea dura, che diventerà evidente anche nella prosecuzione dei test con i missili balistici. In risposta all'armamento della Corea del Nord, la Corea del Sud aumenterà significativamente il suo bilancio per la difesa, con l'obiettivo dichiarato di potersi difendere.

Il fabbisogno di beni svizzeri specializzati è destinato a persistere. In questo contesto, è estremamente probabile che si verifichino ulteriori tentativi di approvvigionamento.

È estremamente probabile che si verifichino ulteriori tentativi di approvvigionamento.

Situazione rilevata dal SIC
Previsioni del SIC

SPIONAGGIO

MINACCIA GENERALE DI SPIONAGGIO

La Svizzera resta esposta a una minaccia di spionaggio molto elevata, proveniente soprattutto da servizi di intelligence di altri Stati. Oltre allo spionaggio, diversi servizi di intelligence conducono in Svizzera anche altre attività sotto copertura, quali disinformazione, propaganda, attività di influenza, approvvigionamento di beni, preparazione di atti di sabotaggio all'estero. Inoltre, agiscono anche contro i propri connazionali residenti nel nostro Paese (repressione transnazionale).

La Svizzera resta esposta a una minaccia di spionaggio molto elevata.

I servizi di intelligence si interessano principalmente alle intenzioni e alle capacità di attori statali e non statali che percepiscono come una minaccia. Alcuni Stati, tuttavia, utilizzano i loro servizi anche per esplorare intenzioni e capacità di concorrenti economici e persino di alleati militari. Le informazioni così ottenute servono a garantire un vantaggio al proprio Stato.

Una ragione fondamentale della minaccia di spionaggio molto elevata è rappresentata dai numerosi obiettivi di esplorazione in Svizzera, tra cui lo Stato stesso, le organizzazioni internazionali e il loro contesto, le sedi diplomatiche e consolari, le aziende attive a livello internazionale, le scuole universitarie, le università, gli istituti di ricerca, le comunità della diaspora, gli esponenti dell'opposizione e gli operatori dei media. Questo tipo di obiettivi è presente anche in molti altri Stati, ma rispetto all'Europa e probabilmente al mondo intero, in Svizzera la loro densità è particolarmente elevata.

Tra gli altri fattori che favoriscono la minaccia di spionaggio figurano la posizione centrale in Europa e l'apertura della Svizzera. Lo spazio Schengen facilita gli spostamenti e la Svizzera dispone di buoni collegamenti di trasporto internazionali. Vi si tengono regolarmente eventi di grande rilevanza internazionale. Aziende, università, istituti di ricerca e organizzazioni non governative attraggono esperti provenienti da tutto il mondo. I servizi di intelligence stranieri utilizzano tutti questi fattori a loro vantaggio, sfruttando la situazione per raccogliere informazioni sia su entità svizzere sia straniere.

Molti di questi servizi intrattengono antenne clandestine in Svizzera, spesso all'interno di sedi diplomatiche e consolari. In alcuni casi le dimensioni di queste basi differiscono in modo evidente: alcuni Stati impiegano decine di presunti agenti dei servizi di intelligence sotto copertura per lo più come personale diplomatico, consolare e tecnico-amministrativo. A questi si aggiungono i collaboratori dei servizi e gli agenti che non hanno una residenza fissa in Svizzera e transitano nel Paese solo temporaneamente per svolgere attività di intelligence.

Persone e organizzazioni sono oggetto di attività di spionaggio in misura variabile anche all'estero. Questo vale in particolare per i soggiorni o le sedi in Stati con servizi di intelligence particolarmente attivi. All'interno del proprio territorio, i servizi di intelligence dispongono di solito di molte più possibilità di esplorazione e non sono sempre costretti ad agire in segreto. Le rappresentanze diplomatiche e consolari svizzere all'estero rientrano in tal senso tra gli obiettivi di esplorazione più ambiti dei servizi nazionali. Anche persone e organizzazioni che si trovano nelle vicinanze di infrastrutture della sicurezza nazionale o che hanno a che fare con strutture e persone degli organi di sicurezza devono mettere in conto di finire nel mirino dei servizi locali.

I fattori che favoriscono lo spionaggio rimangono in gran parte gli stessi, ma è molto probabile che l'intensificarsi del conflitto ibrido in Europa e le crescenti tensioni tra le grandi potenze e alcune potenze regionali porteranno a un aumento della minaccia per la Svizzera. La Svizzera manterrà il suo ruolo di ambiente importante per la conduzione di operazioni per numerosi servizi di intelligence stranieri, che nei prossimi anni continueranno a nutrire un interesse costante per numerosi temi e settori svizzeri. Tra questi figurano in via prioritaria la politica estera, commerciale e di sicurezza, le capacità attuali e future dell'esercito, l'industria degli armamenti, la ricerca di punta, come pure le organizzazioni, i gruppi e gli individui residenti in Svizzera e classificati come minaccia da altri Stati.

La digitalizzazione consentirà ai servizi di intelligence di acquisire un maggior numero di informazioni. Al contempo, è estremamente probabile che tali servizi investano sempre più nell'automazione della raccolta, dell'elaborazione e della trasmissione dei dati. Una sfida particolare per i privati, le aziende, le organizzazioni non governative e le istituzioni pubbliche sarà la gestione dell'intelligenza artificiale e dei dispositivi connessi a Internet, in particolare se dotati di capacità di registrazione audio e video. Particolarmente coinvolte sono le persone e le organizzazioni che lavorano con dati sensibili, come enti pubblici, aziende operanti nei settori del cloud, di Internet e delle telecomunicazioni, banche, assicurazioni, alberghi, amministrazioni fiscali, studi legali, agenzie di prenotazione e società di consulenza.

CORTOMETRAGGIO SULLO SPIONAGGIO ECONOMICO IN SVIZZERA

www.sic.admin.ch
> Sicurezza > Attività informative > Spionaggio economico

MINACCIA DI SPIONAGGIO DA PARTE DELLA RUSSIA

Tra tutti gli Stati che mantengono antenne clandestine in Svizzera, la Russia continua a essere in testa. La maggior parte del personale della Russia attivo in Svizzera appartiene al servizio di intelligence esterno russo SVR. Con il loro personale, il SVR e il servizio di intelligence militare GRU gestiscono reti di agenti in Svizzera. Questi agenti non sono impiegati soltanto a fini di spionaggio, ma anche ad esempio per esercitare influenza politica, fare propaganda, diffondere disinformazione e acquisire beni, sia in Svizzera sia all'estero.

Mentre gran parte dei servizi di intelligence stranieri raccolgono principalmente informazioni su persone e gruppi considerati una minaccia in patria, gli interessi di esplorazione dei servizi russi sono molto più ampi. La Russia è interessata a molti temi della politica interna, estera, commerciale e di sicurezza, oltre che degli armamenti.

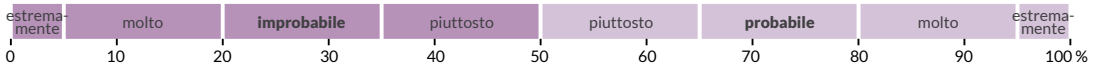
Una parte considerevole delle attività russe in Svizzera ha come bersaglio altre entità straniere presenti nel nostro Paese. A Ginevra, ad esempio, l'obiettivo è di ottenere informazioni attraverso il personale delle organizzazioni internazionali e delle rappresentanze diplomatiche di altri Stati. Può quindi succedere che agenti russi sotto copertura partecipino come diplomatici a riunioni e dibattiti dell'ONU alla ricerca, tra l'altro, di potenziali candidati da reclutare.

Una parte considerevole delle attività russe in Svizzera ha come bersaglio altre entità straniere presenti nel nostro Paese.

Le antenne dei servizi di intelligence presso le rappresentanze diplomatiche e consolari rimangono di fondamentale importanza per la Russia. I servizi di intelligence russi continuano a puntare fortemente sull'esplorazione tramite fonti umane e alla presenza sul posto di gestori di fonti appositamente addestrati motivo per cui i servizi stanno ricostruendo o ampliando le proprie strutture in Europa laddove non vengono ostacolati. I posti presso le rappresentanze diplomatiche e consolari offrono infatti numerosi vantaggi; gli eventi ufficiali organizzati nelle proprie sedi non servono solo a coltivare le relazioni diplomatiche ed economiche, ma anche a stabilire contatti a fini di intelligence e a reclutare agenti in un contesto protetto. La copertura diplomatica, oltre a consentire agli agenti dei servizi di intelligence di accedere facilmente a persone, organizzazioni e infrastrutture in ambito politico, economico e scientifico, offre pure una maggiore protezione contro le azioni penali nello Stato ospite.

Contemporaneamente, i servizi continueranno a reclutare agenti dalla Russia attraverso i canali digitali, una procedura che tuttavia non sostituirà il lavoro degli informatori in loco, nemmeno a lungo termine. Infatti, un rapporto tra informatore e agente, basato tra l'altro su incontri di persona, è più incisivo e affidabile di un rapporto puramente virtuale, in cui di solito l'informatore non mostra mai il proprio volto.

Scala delle probabilità



MINACCIA DI SPIONAGGIO DA PARTE DELLA CINA

Oltre alla Russia, la principale minaccia di spionaggio proviene dalla Cina, la quale dispone di vasti apparati di intelligence che prendono di mira anche la Svizzera e le entità che hanno un nesso con la Svizzera. Tuttavia, le antenne clandestine presso le rappresentanze diplomatiche e consolari cinesi in Svizzera sono verosimilmente più piccole rispetto a quelle della Russia. La Cina punta maggiormente su collaboratori dei servizi di intelligence che non si presentano come diplomatici, ma che viaggiano e operano sotto diverse identità.

Dal punto di vista tematico, la Cina nutre un interesse costante per le attività e le reti dei gruppi che definisce i «cinque veleni»: i movimenti indipendentisti taiwanesi, i movimenti separatisti tibetani e uiguri, il movimento religioso Falun Gong e gli attivisti per la democrazia, comprese le persone e le organizzazioni che in Svizzera li sostengono. Altri obiettivi dei servizi cinesi rientrano nei settori della politica estera, commerciale e di sicurezza, dell'economia e della scienza. A questi si aggiungono diverse entità straniere con sede in Svizzera, tra cui le rappresentanze diplomatiche e consolari di altri Stati.

Nell'acquisire informazioni, la Cina adotta generalmente un approccio globale, raccogliendo dati su una gamma molto ampia di argomenti. È molto probabile che non sia l'unico Paese al mondo a farlo, ma si distingue per le sue dimensioni e per le sue interconnessioni politiche e soprattutto economiche a livello globale. I cittadini e le organizzazioni cinesi sono tenuti per legge a collaborare con le autorità e, di conseguenza, anche con i servizi di intelligence.

Nell'acquisire informazioni, la Cina adotta generalmente un approccio globale, raccogliendo dati su una gamma molto ampia di argomenti.

L'entità della minaccia per la Svizzera rappresentata dalla Cina dipenderà in larga misura dal futuro grado di interconnessione economica tra i due Paesi. A differenza di quanto avviene con la Russia, se le condizioni rimarranno invariate, è molto probabile che gli scambi commerciali continuino ad aumentare nei prossimi anni. Ciò comporta la raccolta di dati che verosimilmente la Cina utilizzerà anche a fini di intelligence. I servizi cinesi dispongono già oggi delle risorse tecniche e umane necessarie a elaborare grandi quantità di dati e renderli utilizzabili a loro vantaggio nonché del Partito Comunista, dell'esercito, del resto dell'apparato statale e delle aziende di proprietà dello Stato. È molto probabile che continueranno a potenziare in maniera massiccia queste capacità. È realistico ipotizzare, ad esempio, che i dati generati dai veicoli cinesi di nuova generazione durante il loro utilizzo vengano trasmessi ai servizi di intelligence tramite le case automobilistiche o che i servizi accedano, o accederanno, a tali dati tramite interfacce. Si tratta di un aspetto di cui persone e organizzazioni che acquistano veicoli cinesi in Svizzera devono tenere conto, in particolare coloro che rientrano tra i principali obiettivi di esplorazione.

Situazione rilevata dal SIC
Previsioni del SIC

Illustrazione 6

MINACCIA A INFRASTRUTTURE CRITICHE

Illustrazione 7

STATO DELLA MINACCIA GENERALE

Diversi attori minacciano infrastrutture critiche in Svizzera, sia fisicamente sia con mezzi informatici. In questo contesto, gli attacchi perpetrati nel nostro Paese da ciberattori statali, in particolare russi, cinesi, iraniani e nordcoreani, rappresentano la ciberminaccia più concreta che mette a rischio l'esistenza e il funzionamento dello Stato. I ciberattacchi avvengono tuttavia anche tramite attori esterni incaricati da uno Stato, i cosiddetti proxy.

Gli Stati praticano il ciberspionaggio in linea con i propri interessi strategici. Tra i fattori determinanti figurano in particolare la guerra contro l'Ucraina, il conflitto in Iran, nonché le tensioni commerciali e la competizione tecnologica tra Stati Uniti e Cina. Gli aggressori esplorano obiettivi militari con mezzi informatici e ottengono informazioni politiche riservate da autorità governative. Sono inoltre interessati alla ricerca e allo sviluppo rilevanti dal punto di vista economico o militare, in special modo nei settori degli armamenti e delle tecnologie di punta. La Corea del Nord impiega i propri ciberattori anche per procurarsi valuta estera, rubando denaro sotto forma di criptovalute.

I gruppi di ransomware criptano i dati per estorcere un riscatto. In Svizzera si registrano in media da uno a due attacchi di questo tipo al mese diretti contro infrastrutture critiche, perlopiù aziende e istituzioni non governative. Gli attacchi ransomware possono compromettere il funzionamento di infrastrutture critiche o addirittura interromperlo per un periodo prolungato. Un altro rischio consiste nella pubblicazione dei dati rubati da parte degli aggressori, correlata quindi a un rischio di reputazione o a uno svantaggio competitivo. Anche i fornitori di enti governativi sono un obiettivo di attacchi ransomware, con la conseguenza di una potenziale fuga di informazioni politiche riservate. Sono gruppi di hacker russi i responsabili della gran parte di attacchi ransomware in Svizzera e in altri Stati occidentali.

I gruppi con moventi ideologici che cercano di raggiungere i propri obiettivi anche ricorrendo ad attacchi hacker, i cosiddetti hacktivisti, sono noti per gli attacchi di sovraccarico. In particolare, i gruppi di hacktivisti filorussi hanno inoltre iniziato a disturbare i sistemi di controllo industriale collegati a Internet all'estero. Si tratta di sistemi spesso mal protetti e quindi vulnerabili anche senza particolari competenze, ma è comunque prevedibile che nei prossimi mesi questi aggressori perfezionino le proprie capacità. Sebbene nella maggior parte dei casi le infrastrutture critiche non abbiano subito danni significativi, gli attacchi hanno suscitato grande attenzione, dimostrando inoltre che i sistemi di controllo industriale sono in parte protetti solo con password standard e quindi sono vulnerabili. In Svizzera questo tipo di attacchi ai sistemi di controllo industriali è meno probabile che negli Stati dell'UE e della NATO che sostengono militarmente l'Ucraina e sono quindi il bersaglio principale dei gruppi filorussi. Molto probabili sono invece attacchi di sovraccarico contro obiettivi correlati in particolare a conferenze internazionali e grandi eventi come il WEF ospitati nel nostro Paese. Questi tentativi di disturbo, pur interrompendo solo marginalmente l'esercizio di infrastrutture critiche, in alcuni casi ricevono grande attenzione mediatica. Particolarmente attivi sono i gruppi filorussi e filopalestinesi; in alcuni casi sono gli Stati a incaricare questi gruppi di hacker per nascondere il proprio coinvolgimento.

Gli attacchi di sabotaggio, fisici o con mezzi informatici, comportano un potenziale di danno di gran lunga maggiore. Ad esempio, rientrano nella strategia di conflitto ibrido della Russia contro l'Europa; più in generale, sono principalmente parte integrante di guerre o conflitti diretti. Anche in caso di conflitto tra la Svizzera e un altro Stato, aumenterebbe rapidamente la probabilità di atti di sabotaggio mirati da parte dello Stato contro infrastrutture critiche della Svizzera. Sebbene al momento non vi siano indicazioni di un attacco di sabotaggio contro infrastrutture critiche in Svizzera volto a danneggiarle, un attacco di questo tipo potrebbe comunque verificarsi: per ragioni di politica egemonica, le infrastrutture critiche svizzere potrebbero essere sabotate fisicamente o con mezzi informatici al fine di colpire Stati o alleanze che ne dipendono. L'attrattiva di tali obiettivi cresce quanto più gli Stati della NATO e dell'UE proteggono le loro infrastrutture critiche senza che la Svizzera faccia altrettanto. A causa di cibersabotaggi contro obiettivi all'estero, tuttavia, anche nel nostro Paese sono possibili danni in qualsiasi momento.

Per ragioni di politica egemonica, le infrastrutture critiche svizzere potrebbero essere sabotate fisicamente o con mezzi informatici al fine di colpire Stati o alleanze che ne dipendono.

Anche gli attori motivati da ragioni ideologiche ricorrono al sabotaggio. Gli ambienti estremisti di sinistra considerano la violenza un mezzo collaudato nella lotta contro il capitalismo. Aziende commerciali, infrastrutture quali autostrade e impianti tecnici di ferrovie o operatori di telecomunicazioni, sia in Svizzera sia all'estero, sono state ripetutamente oggetto di atti di sabotaggio fisici ed è piuttosto probabile che se ne verifichino altri in futuro.

MINACCIA COSTANTE DI CIBERSPIONAGGIO

I ciberattori statali russi, cinesi, iraniani e nordcoreani dispongono di competenze tecniche avanzate. Uno dei loro obiettivi principali è l'acquisizione di informazioni politiche presso le autorità svizzere, con particolare attenzione alla politica di sicurezza e agli affari esteri.

I ciberattori statali stanno inoltre raccogliendo informazioni presso le scuole universitarie e le istituzioni scientifiche svizzere. Particolarmente esposti sono la ricerca nei settori degli armamenti e delle tecnologie di punta come pure i programmi di ricerca e sviluppo del settore privato. Anche queste conoscenze hanno una loro rilevanza sul piano militare. Le tecnologie di punta svolgono inoltre un ruolo fondamentale nella competizione internazionale per l'egemonia economica globale. L'acquisizione di informazioni attraverso attività di spionaggio diventa più importante quando gli Stati sono soggetti a sanzioni e quindi non possono acquisire legalmente il know-how.

Sono soprattutto i ciberattori statali cinesi a compromettere le società di telecomunicazioni negli Stati Uniti, in Europa e nel Sudest asiatico. Questa minaccia rimane attuale anche per la Svizzera. Le società di telecomunicazioni vengono prese di mira non solo a scopo esplorativo, ma anche come vettori per penetrare nei sistemi informatici dei clienti. La catena di fornitura, in particolare i fornitori di servizi IT, rimane un'importante porta di accesso per i ciberattacchi.

Sono soprattutto i ciberattori statali cinesi a compromettere le società di telecomunicazioni negli Stati Uniti, in Europa e nel Sudest asiatico. Questa minaccia rimane attuale anche per la Svizzera.

Per ottenere l'accesso iniziale, i ciberattori statali sfruttano spesso i punti di vulnerabilità dei software; in alcuni casi si tratta delle cosiddette vulnerabilità «zero-day», ovvero punti critici che al momento dell'attacco sono noti solo all'aggressore e per i quali non è ancora disponibile alcun aggiornamento di sicurezza. Molto più spesso, però, i ciberattori statali attaccano dispositivi con software obsoleti, i cui punti di vulnerabilità sono noti da settimane, talvolta anche da anni. Gli attacchi sono particolarmente frequenti attraverso i punti critici di dispositivi di rete esposti a Internet, come router e firewall. I ciberattori statali sfruttano anche i punti di vulnerabilità dei dispositivi mobili anche per il ciberspionaggio.

Il fattore umano svolge un ruolo fondamentale nel ciberspionaggio. Nella maggior parte dei casi, gli attori statali inviano a persone oggetto di interesse e-mail personalizzate (il cosiddetto spear phishing), ad esempio con un invito a una conferenza attinente al loro ambito lavorativo. Questo tipo di ingegneria sociale mira a creare fiducia per convincere tali persone a scaricare e installare inconsapevolmente un programma dannoso o a rivelare le proprie credenziali di accesso. Soprattutto gli impiegati amministrativi ricevono questo tipo di e-mail. I ciberattori statali contattano sempre più spesso le persone oggetto di interesse tramite app di comunicazione per ottenere l'accesso a chat, dati di contatto e altre informazioni presenti sul cellulare.

Negli anni a venire è probabile che gli attacchi di ciberspionaggio contro obiettivi svizzeri saranno più frequenti. Rimangono uno strumento importante per acquisire informazioni, integrano lo spionaggio umano e in parte operano in sinergia con esso *(cfr. «Cortometraggio sullo spionaggio economico in Svizzera», p. 61)*.

Il contesto della politica di sicurezza della Svizzera è progressivamente peggiorato; in tempi di guerra e di conflitto, aumenta la necessità di ottenere informazioni sulla controparte. La cooperazione della Svizzera con la NATO e l'UE in materia di politica di sicurezza e il suo acquisto di tecnologie militari occidentali all'avanguardia attireranno l'interesse soprattutto di ciberattori statali russi e cinesi, i quali cercheranno anche di ottenere informazioni sugli Stati e sulle alleanze con cui la Svizzera collabora, sferrando attacchi contro politici e l'Amministrazione federale. L'inasprimento delle tensioni commerciali e la rivalità sistemica tra Stati Uniti e Cina, come pure le interconnessioni economiche tra la Svizzera e partner internazionali, tra cui la Cina, aumentano il rischio di attività di spionaggio politico ed economico in Svizzera. Ciò sarà ancora più evidente se gli Stati Uniti continueranno a innalzare barriere alle esportazioni di tecnologia verso la Cina, poiché in tal caso lo spionaggio rimarrà un mezzo per procurarsi tali tecnologie, anche in Svizzera.

I ciberattori statali collaborano con le scuole universitarie nazionali e aziende specializzate, riuscendo così a sviluppare rapidamente le loro capacità di attacco. L'ecosistema informatico cinese prevede, ad esempio, l'obbligo generale di notificare tempestivamente allo Stato i punti di vulnerabilità individuati, dai quali i ciberattori statali possono trarre vantaggio. I ciberattori statali di vari Paesi si avvalgono anche dei progressi tecnologici, come ad esempio l'intelligenza artificiale, per rendere i propri attacchi ancora più efficaci.

È probabile che il numero di punti critici individuati è destinato ad aumentare ancora in modo significativo, poiché la digitalizzazione procede e così sempre più dispositivi potenzialmente vulnerabili vengono collegati in rete. Se da un lato le vulnerabilità possono essere spesso individuate e sfruttate dagli hacker con relativa rapidità, dall'altro l'onere richiesto per lo sviluppo di software sicuri è notevole. Inoltre, i fabbricanti non sono tenuti per legge a progettare i propri programmi in modo da renderli il più possibile resistenti agli attacchi.

VALUTAZIONE DELLE PROPRIE MISURE DI SICUREZZA IN AMBITO INFORMATICO

Ufficio federale della cibersicurezza UFCS
www.ufcs.admin.ch

Standard minimi per le TIC
Standard minimo TIC per il miglioramento della resilienza dei gestori di infrastrutture critiche, imprese e organizzazioni (incluso lo strumento di valutazione)
www.ufcs.admin.ch
Informazioni per > Informazioni per specialisti
it > Temi > Standard minimi per le TIC

Segnalazione di siti de phishing e e-mails de phishing
www.antiphishing.ch

Allianz Digitale Sicherheit Schweiz
Breve test online sulla sicurezza cibernetica per le PMI (disponibile in tedesco e in inglese)
www.digitalsecurityswitzerland.ch

I CIBERATTORI UTILIZZANO LE INFRASTRUTTURE SVIZZERE PER I LORO ATTACCHI

I ciberattori statali o incaricati da uno Stato dispongono spesso di risorse di gran lunga superiori a quelle di gruppi motivati da interessi economici o degli hacktivisti. Possono permettersi di agire con molta calma nei loro ciberattacchi: dalla fase iniziale di esplorazione fino all'esfiltrazione di dati o al cibersabotaggio possono trascorrere mesi, se non anni.

I ciberattori adottano misure volte a impedire che le loro attività vengano scoperte e ricondotte alla loro origine, rendendo più difficile attribuire un ciberattacco a uno Stato o a un'autorità. In alcuni casi non solo cancellano le loro tracce, ma lasciano anche deliberatamente false piste che conducono verso un altro Stato. Ciò rende difficile attribuire un ciberattacco a uno Stato o a un'autorità. Le attività ciber vengono pertanto condotte attraverso le cosiddette reti di anonimizzazione: gli autori non attaccano il sistema bersaglio direttamente dalla propria infrastruttura, bensì attraverso diversi dispositivi intermedi. Attribuire la responsabilità di incidenti informatici rilevanti in materia di politica di sicurezza a un determinato attore risulta ulteriormente complicato dal fatto che diversi ciberattori dello stesso Stato possono utilizzare le stesse reti. In parte gli attori statali creano queste reti autonomamente, ma possono anche ricorrere alle aziende del settore cibersicurezza.

Attribuire la responsabilità di incidenti informatici rilevanti in materia di politica di sicurezza a un determinato attore risulta ulteriormente complicato dal fatto che diversi ciberattori dello stesso Stato possono utilizzare le stesse reti.

Le reti di anonimizzazione sono costituite principalmente da due componenti:

- Dispositivi esposti a Internet e scarsamente protetti, come i router, con lo svantaggio per i ciberattori di avere poco controllo e, ad esempio, di perdere l'accesso quando i proprietari aggiornano il software.

- Infrastruttura IT a noleggio, ad esempio server. In questo caso gli aggressori hanno un maggiore controllo. I server a noleggio possono fungere da collegamento per passare da un server all'altro o per stabilire una connessione con il sistema bersaglio, ad esempio per installare un malware.

Per confondere ulteriormente le tracce, gli aggressori sostituiscono di continuo i componenti delle loro reti di anonimizzazione, a volte nel giro di poche ore.

Al fine di mantenere l'anonimato, i ciberattori statali o i loro fornitori di servizi solitamente noleggiano i server presso un cosiddetto «bulletproof hosting provider», il quale, a sua volta, noleggia in parte i server da altri centri dati, fungendo così da rivenditore, ovvero da intermediario tra attori statali e provider. Tali rivenditori noleggiano anche infrastrutture di server presso provider con sede in Stati occidentali, compresa la Svizzera, poiché gli attacchi provenienti da server situati nella regione del Paese bersaglio sono meno evidenti. I bulletproof hosting provider dispongono spesso di strutture societarie in Paesi offshore. In generale non forniscono alcuna informazione sui loro clienti e sulle relative attività, anche se in molti Paesi occidentali, compresa la Svizzera, sarebbero tenuti a farlo non appena utilizzano l'infrastruttura di centri dati locali. Spesso offrono

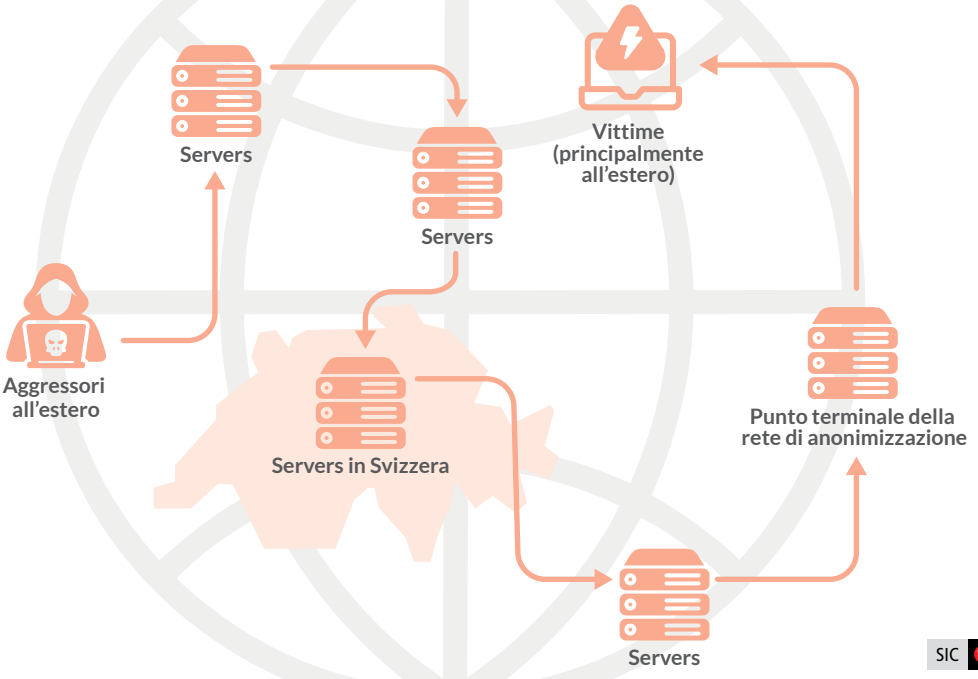
anche la possibilità di effettuare pagamenti in modo anonimo tramite criptovaluta. Questi rivenditori svolgono quindi un ruolo essenziale per ciberattori statali e non statali nella creazione di infrastrutture di attacco e di reti di anonimizzazione.

Solitamente, le reti di anonimizzazione si estendono su più continenti. I ciberattori statali si avvalgono dei servizi di rivenditori, i quali a loro volta subaffittano server di aziende svizzere. Sono soprattutto ciberattori statali cinesi e russi a sfruttare questo tipo di infrastruttura in Svizzera per svolgere attività di esplorazione su obiettivi militari e politici in altri Stati. In qualche caso i ciberattori statali hanno utilizzato tale infrastruttura anche per attacchi di cibersabotaggio all'estero. Per identificare sia gli autori sia le vittime, è necessario procedere a un rapido accertamento di questa infrastruttura di attacco, in stretta collaborazione con i partner internazionali.

Di recente gli Stati Uniti e altri Stati occidentali, anche in Europa, hanno imposto sanzioni contro diversi bulletproof hosting provider. I rispettivi fornitori di servizi però continuano a rappresentare un elemento centrale per gli attori statali nella creazione dell'infrastruttura di attacco. Inoltre, grazie all'automazione, la registrazione su tali server o la creazione dei dati utente necessari, come gli indirizzi e-mail, sta diventando sempre più semplice. È quindi probabile che i ciberattori statali amplino e rinnovino più rapidamente la propria infrastruttura di attacco. Per questo motivo è molto probabile che vengono adottate ulteriori sanzioni contro i bulletproof hosting provider, compresi quelli che utilizzano servizi a noleggio presso provider svizzeri.

La Svizzera ha ratificato le undici norme dell'ONU per un comportamento responsabile degli Stati nel ciberspazio e le sta mettendo in atto. Tra queste, figura l'uso improprio dell'infrastruttura IT sul proprio territorio. A tal fine, il SIC, l'Ufficio federale della cibersicurezza UFCS e le autorità di perseguimento penale della Confederazione e dei Cantoni collaborano strettamente tra loro e con i rispettivi partner internazionali.

Rappresentazione schematica di una rete di anonimizzazione



INDICATORI 2025

LA RETE INFORMATIVA INTEGRATA DEL SIC

In che modo il SIC riunisce le informazioni rilevanti per la sicurezza e perché ciò è fondamentale per la sicurezza dei grandi eventi.

Quando i leader politici internazionali si incontrano, l'attenzione si concentra sui dispositivi di sicurezza, sulla presenza della polizia e sulle misure visibili. Quasi nessuno però nota chi opera da parecchio tempo dietro le quinte: la rete informativa integrata del SIC.

La rete fa sì che, sulla base di innumerevoli singole indicazioni, emerga un'immagine condivisa della situazione della situazione che sia coordinata, valutata e resa utilizzabile ai fini decisionali. Questo sistema non è una nuova invenzione. Già molto tempo prima che il SIC fosse dotato dell'attuale legge sulle attività informative, la Confederazione e i Cantoni collaboravano in stretto contatto.

Ciò che si era già dimostrato efficace nel 2003, in occasione del vertice del G8 di Évian, è oggi una pratica consolidata. Anche in occasione di grandi eventi internazionali attuali, come il Forum economico mondiale di Davos, che si svolge ogni anno, o il vertice del G7 in Francia, la rete informativa integrata garantisce che gli organi della Confederazione e dei Cantoni coinvolti dispongano tempestivamente delle informazioni rilevanti sulla situazione. Nel quadro della cooperazione internazionale, nel caso concreto, ne beneficia anche la Francia.

La domanda centrale è: come si ottiene un quadro d'insieme solido partendo da singole informazioni frammentarie? Ed è proprio qui che entra in gioco la rete informativa integrata del SIC. Con il suo Centro federale di situazione, il SIC garantisce che le indicazioni non rimangano isolate, ma vengano riunite e contestualizzate in modo rapido, strutturato e sicuro. In questo contesto il SIC funge da piattaforma centrale, ma non è l'unico produttore di informazioni sulla situazione. Tutti gli attori coinvolti forniscono contributi dai rispettivi settori di competenza, dalla lotta al terrorismo al controspionaggio, fino alle ciberminacce.

Il valore aggiunto della rete informativa integrata risiede nell'elaborazione e nella sintesi di queste informazioni. La qualità dell'immagine della situazione che ne deriva e la sua diffusione sicura tramite una rappresentazione elettronica della situazione a tutti i partner della rete informativa integrata è determinante per l'efficacia delle misure statali e quindi, in ultima analisi, anche per la sicurezza della Svizzera.

Le strutture decentrate della Svizzera rendono il coordinamento impegnativo. Allo stesso tempo la rete informativa integrata beneficia della vicinanza tra gli attori e gli eventi. A ciò si aggiunge l'interconnessione a livello internazionale del SIC che permette l'accesso a informazioni che altrimenti non sarebbero a disposizione dei singoli corpi di polizia e di altri partner.

La rete informativa integrata del SIC è quindi un elemento centrale e indispensabile per la sicurezza della Svizzera.

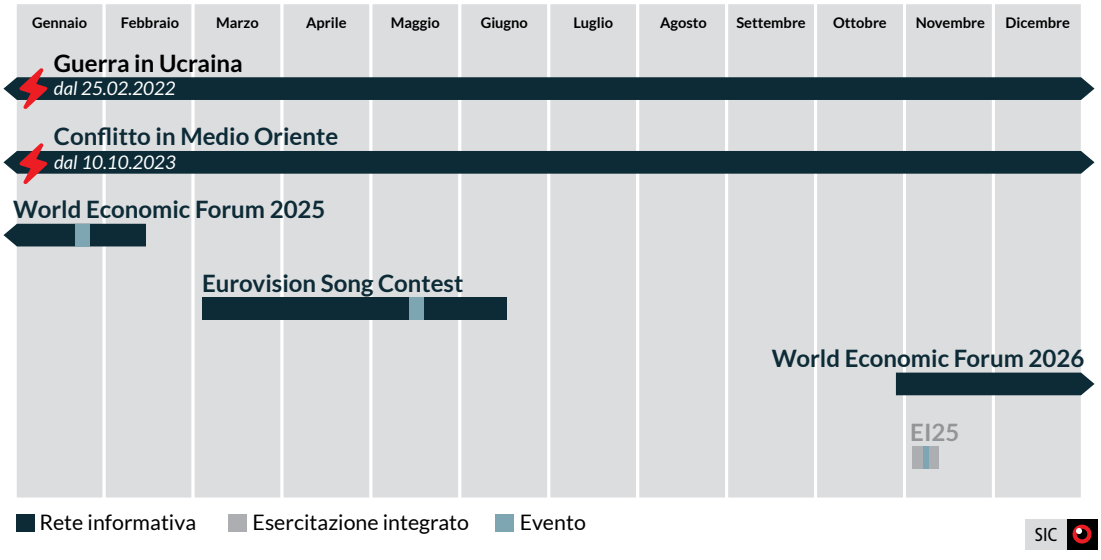
VALUTAZIONI DELLA SITUAZIONE

La Svizzera ha bisogno del SIC perché, ...
... il SIC identifica le minacce rilevanti per la Svizzera e presenta un rapporto in merito.

Ad avere ricevuto le valutazioni della situazione da parte del SIC sono stati il Consiglio federale, altri decisori politici e uffici competenti in seno alla Confederazione e ai Cantoni, organi decisionali militari nonché autorità di perseguimento penale. Su richiesta o di propria iniziativa, il SIC fornisce a tali destinatari informazioni e dati riguardanti ogni settore della legge federale sulle attività informative (LAIn) e il mandato di base classificato del SIC. Ciò avviene periodicamente, spontaneamente o a cadenza fissa, nonché in formato scritto oppure orale.

Rete informativa

Nel 2025 il SIC ha sostenuto i Cantoni mediante cinque reti informative gestite dal suo Centro federale di situazione. Il SIC ha inoltre istituito una rete informativa durante l'esercitazione di crisi nazionale « EI 25 ».



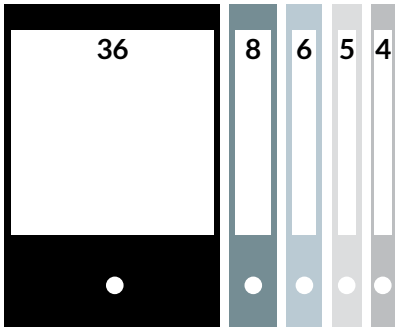
RAPPORTI UFFICIALI

La Svizzera ha bisogno del SIC perché, ...
... il SIC trasmette informazioni in forma non classificata ad autorità competenti affinché le utilizzino in procedimenti penali e amministrativi.

Nel 2025 il SIC ha ad esempio inviato 24 rapporti ufficiali al Ministero pubblico della Confederazione e 35 ad altre autorità della Confederazione quali l'Ufficio federale di polizia, la Segreteria di Stato della migrazione o la Segreteria di Stato dell'economia (senza i complementi ai rapporti ufficiali già esistenti).

Rapporti ufficiali ad autorità competenti per settore
Totale 59

- Terrorismo
- Estremismo violento
- Spionaggio
- Proliferazione
- Non associabili in modo esclusivo a uno di questi temi



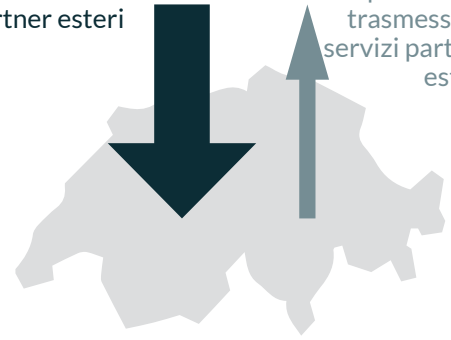
COOPERAZIONE INTERNAZIONALE

La Svizzera ha bisogno del SIC perché, ...
... il SIC collabora con le autorità estere che adempiono i compiti ai sensi della LAIn. A tal fine, tra l'altro, esso rappresenta la Svizzera in seno a vari gremi internazionali.

Il SIC scambia in particolare informazioni con oltre un centinaio di servizi partner di diversi Stati e con organizzazioni internazionali, ad esempio con i servizi competenti dell'Organizzazione delle Nazioni Unite e con istituzioni ed enti dell'Unione Europea che si occupano di questioni attinenti alla politica di sicurezza.

13'308
comunicazioni relative ai compiti del SIC ricevute da servizi partner esteri

3887
comunicazioni relative ai compiti del SIC trasmesse ai servizi partner esteri



SENSIBILIZZAZIONE

La Svizzera ha bisogno del SIC perché, ...
... il SIC gestisce, in collaborazione con i Cantoni, programmi volti a incrementare la consapevolezza in merito ad attività nei settori dello spionaggio e della proliferazione.

Con il programma Prophylax, il SIC sensibilizza le imprese, le organizzazioni economiche, le università, le scuole universitarie, gli istituti di ricerca e le autorità. Il SIC presenta in particolare misure di sicurezza contro il trasferimento indesiderato di conoscenze o la fuga di informazioni o di dati.

Nel 2025 il SIC ha condotto 121 sensibilizzazioni: 24 presso imprese e associazioni economiche, 31 presso scuole universitarie ecc., 66 presso autorità federali e cantonali.

PREVENZIONE

La Svizzera ha bisogno del SIC perché, ...
... il SIC conduce inoltre, in collaborazione con i Cantoni le autorità federali, colloqui preventivi nei settori dello spionaggio e della proliferazione.

Il SIC è in contatto con imprese e scuole universitarie, con la quale conduce colloqui nell'ambito della prevenzione. Nel 2025 il SIC ha svolto 69 colloqui preventivi.

CONTROLLI ALL'ESPORTAZIONE

La Svizzera ha bisogno del SIC perché, ...
... con il suo contributo per impedire l'esportazione illegale di prodotti a duplice impiego, di materiale bellico e di tecnologia dalla Svizzera, il SIC combatte la proliferazione.

Insieme al Dipartimento federale degli affari esteri, al Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni, alla Segreteria di Stato della politica di sicurezza e alla Segreteria di Stato dell'economia, il SIC fa parte del gruppo di controllo delle esportazioni della Confederazione. La Segreteria di Stato dell'economia sottopone al SIC le domande di esportazione soggette ad autorizzazione ai fini della valutazione dei rischi.

Nel 2025 il SIC ha preso posizione in merito a 135 domande per determinare se vi fosse il rischio di infrazioni alla legge sul controllo dei beni a duplice impiego, alla legge federale sul materiale bellico e alla legge sugli embarghi. Il SIC segnala inoltre di propria iniziativa eventuali infrazioni alle autorità di controllo delle esportazioni o di perseguimento penale.

MISURE DI ACQUISIZIONE SOGGETTE AD AUTORIZZAZIONE

La Svizzera ha bisogno del SIC, perché …
… in caso di minaccia grave e incombente negli ambiti del terrorismo, dello spionaggio, della proliferazione, degli attacchi a infrastrutture critiche o della tutela di altri interessi importanti della Svizzera secondo l'articolo 3 LAIn, il SIC può ordinare misure di acquisizione soggette ad autorizzazione.

Le misure di acquisizione soggette ad autorizzazione necessitano di volta in volta dell'autorizzazione del Tribunale amministrativo federale e del nullaosta del capo del Dipartimento federale della difesa, della protezione della popolazione e dello sport previa consultazione del capo del Dipartimento federale degli affari esteri e di quello del Dipartimento federale di giustizia e polizia.

Le misure di acquisizione soggette ad autorizzazione vengono autorizzate per al massimo tre mesi. Prima della fine di questo periodo il SIC può inoltrare domanda motivata di proroga per al massimo altri tre mesi. Le misure sono sottoposte a stretto controllo da parte dell'Autorità di vigilanza indipendente sulle attività informative e da parte della Delegazione delle Commissioni della gestione.

Misure autorizzate e con nullaosta

Compiti	Misure
Terrorismo	**32**
Spionaggio	**29**
Proliferazione NBC	**36**
Attacchi a infrastrutture critiche	**112**
Totale	**209**

Persone interessate dalle misure

Categoria	Numero
Persone oggetto di interesse	**9**
Terze persone	**6**
Persone ignote (p. es. è noto soltanto il loro numero di telefono)	**9**
Totale	**24**

Metodi di calcolo

- Per quanto riguarda le misure, una proroga autorizzata e con nullaosta (possibile più volte, al massimo per tre mesi di volta in volta) viene calcolata come una nuova misura, dal momento che è stato necessario presentare una nuova domanda con una nuova motivazione nell'ambito della procedura ordinaria
- Le persone interessate vengono invece calcolate una sola volta all'anno, anche in caso di proroga delle misure

ESPLORAZIONE DI SEGNALI VIA CAVO

La LAIn prevede che il SIC abbia anche la facoltà di ricorrere all'esplorazione di segnali via cavo per acquisire informazioni riguardanti fatti che avvengono all'estero rilevanti sotto il profilo della politica di sicurezza (art. 39 segg. LAIn).

Poiché l'esplorazione dei segnali via cavo serve ad acquisire informazioni su fatti concernenti l'estero, non è stata concepita come misura di acquisizione entro i confini nazionali soggetta ad autorizzazione.

L'esplorazione di segnali via cavo può essere effettuata soltanto con la partecipazione dei gestori di reti filari e dei fornitori di servizi di telecomunicazione svizzeri che sono tenuti a trasmettere i relativi segnali al Centro operazioni elettroniche dell'Esercito svizzero. La LAIn prevede per le disposizioni al riguardo impartite ai gestori e fornitori una procedura di autorizzazione e di nullaosta analoga a quella per le misure di acquisizione soggette ad autorizzazione.

4
mandati di esplorazione di segnali via cavo
(ancora in corso alla fine del 2025)

ESPLORAZIONE RADIO

Anche l'esplorazione radio è orientata all'estero (art. 38 LAIn), il che significa che può rilevare soltanto sistemi radio che non si trovano in Svizzera. In pratica si tratta soprattutto di satelliti per telecomunicazioni e di emittenti a onde corte.

12
mandati di esplorazione radio
(ancora in corso alla fine del 2025)

CONTROLLI SULLE PERSONE IN MATERIA DI MIGRAZIONE E RICHIESTE DI DIVIETO D'ENTRATA

La Svizzera ha bisogno del SIC, perché …
… il SIC controlla determinate persone straniere che possono rappresentare un'eventuale minaccia per la sicurezza interna del Paese.

Se il SIC ritiene che la persona in questione possa rappresentare un rischio potenziale, può raccomandare di rifiutare la richiesta o di far valere delle riserve presso le autorità competenti. A seconda della richiesta, possono essere coinvolti il Dipartimento federale degli affari esteri, la Segreteria di Stato della migrazione o l'Ufficio federale di polizia.

	Numero totale esaminato	Raccomandazione di rifiuto
Richieste d'accreditamento di diplomatici e funzionari internazionali	**4793**	**30**
Richieste di visto		**36**
Richieste di autorizzazione in caso di assunzione di un impiego e di permesso di dimora nell'ambito della legislazione sugli stranieri		**5**
Dossier in materia di asilo statuto di protezione S	**373** **3**	**2** **0**
Domande di naturalizzazione	**46'992**	**1**
Procedura di consultazione Schengen in materia di visti Vision	**1'530'508**	**7**
Esamino delle informazioni anticipate sui passeggeri (Advance Passenger Information, API) *Dopo un termine di 96 ore per il trattamento, il SIC cancella i dati API da cui non risulta alcuna corrispondenza con quelli a sua disposizione.*	**4'195'024 persone su 24'732 voli**	

RICHIESTE DI DIVIETO D'ENTRATA

Il SIC ha chiesto a l'Ufficio federale di polizia di disporre 63 divieti d'entrata per salvaguardare la sicurezza della Svizzera; 51 richieste sono state approvate. 12 erano ancora in corso a fine 2025. Nessuna domanda è stata respinta.

CONTROLLI DI SICUREZZA RELATIVI ALLE PERSONE

I controlli di sicurezza relativi alle persone rappresentano una misura preventiva per la salvaguardia della sicurezza interna della Svizzera e la protezione della sua popolazione. Si applicano a persone che ricoprono funzioni sensibili sotto il profilo della sicurezza e che hanno accesso a informazioni, materiali o sistemi classificati.

Per conto della Cancelleria federale e del Servizio specializzato per i controlli di sicurezza relativi alle persone del DDPS, il SIC svolge accertamenti all'estero e accertamenti approfonditi su persone registrate nei sistemi d'informazione e di archiviazione del SIC.

Nel 2025 il SIC ha svolto 1151 accertamenti all'estero e 171 accertamenti approfonditi (su persone registrate nei sistemi d'informazione e di memorizzazione del SIC).

TRASPARENZA

Nel 2025 sono pervenute in totale 204 domande di informazioni in virtù dell'articolo 63 LAIn e dell'articolo 25 della legge federale sulla protezione dei dati (LPD). 118 richiedenti hanno ottenuto informazioni esaustive: il SIC ha fornito loro informazioni complete per sapere se avesse o meno trattato dati sulla loro persona e, in caso affermativo, quali dati avesse trattato al momento della domanda.

In 39 casi la risposta è stata differita, limitata o respinta per interessi di mantenimento del segreto o interessi di terzi (art. 63 cpv. 2 LAIn e art. 26 cpv. 2 LPD).

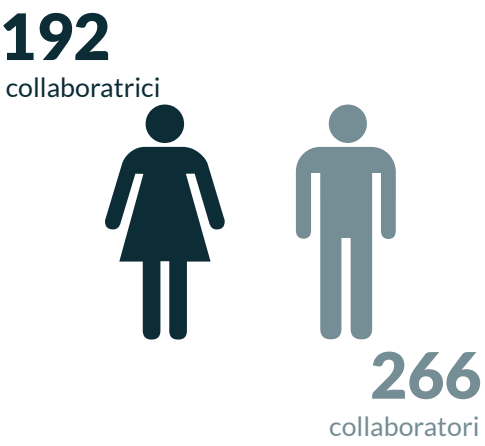
In 11 casi le relative condizioni formali non sono state soddisfatte (p. es. mancata presentazione, nonostante sollecito, del certificato d'identità richiesto), e questo nonostante una sollecitazione dopo tre mesi: tali domande sono state pertanto archiviate senza seguito. Per quanto riguarda altre 4 domande il 31 dicembre 2025 vi era ancora la possibilità di porre rimedio al difetto formale entro il termine di tre mesi. Alla fine del 2025 32 domande non avevano ancora ricevuto risposta.

Nel 2025 il SIC ha ricevuto 38 domande di accesso in virtù della legge sulla trasparenza (LTras). In 26 di questi casi il SIC è stato ente responsabile e in 12 casi coinvolto.

PERSONALE E FINANZE

Il SIC promuove una diversità vissuta: vi lavorano collaboratori e collaboratrici di diverse generazioni e generi. Essi possiedono formazioni ed esperienze professionali variegate e hanno percorsi di vita e orizzonti differenziati. La loro collaborazione è contraddistinta da valori quali apertura, coraggio, rispetto, fiducia e lungimiranza. Il plurilinguismo che caratterizza la Svizzera si riflette nel SIC: tutte le lingue nazionali vi sono parlate quotidianamente. Questa diversità integra diverse prospettive e rafforza la cooperazione interdisciplinare e l'approccio globale e fondato alle complesse questioni nel settore dell'intelligence.

Numero di collaboratori
Totale 458
(fine 2025)



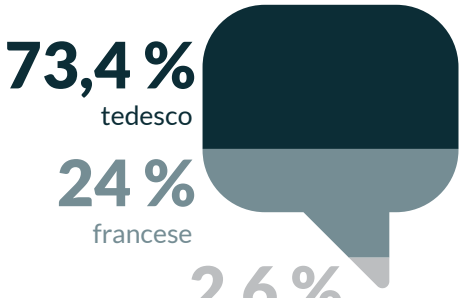
Finanze
In milioni di franchi

77,9
spese per il personale

25,9
spese per beni e servizi e spese d'esercizio

18
spese dei Cantoni per i propri servizi informazioni

Ripartizione linguistica (fine 2025)



LISTA DELLE ILLUSTRAZIONI

Redazione
Servizio delle attività informative della Confederazione SIC

Chiusura della redazione
Maggio/Giugno 2026

Indirizzo di riferimento
Servizio delle attività informative della Confederazione SIC
Papiermühlestrasse 20
CH-3003 Berna
media@ndb.admin.ch
www.sic.admin.ch

Distribuzione
UFCL, Vendita di pubblicazioni federali,
CH-3003 Berna
www.pubblicazionifederali.admin.ch
Art.-Nr. 503.001.26i
ISSN 1664-4690

LA SICUREZZA DELLA SVIZZERA

Servizio delle attività informative della Confederazione SIC
Papiermühlestrasse 20
CH-3003 Berna

www.sic.admin.ch / media@ndb.admin.ch