RELAZIONE DI ANALISI · SICUREZZA, TERRORISMO E MINACCE IBRIDE · NOVEMBRE 2026

Molte traiettorie, nessun centro: come leggere la nuova minaccia

SCHEGGE

TERRORISMO, MINACCE IBRIDE E INFRASTRUTTURE CRITICHE

Jihadismo giovanile, estremismo nichilista, attività statali ostili e disruption a basso costo: dove le traiettorie si incrociano e come intercettarle prima che convergano.

Jihadismo | Estremismo | Minacce ibride | Trasporti | Prevenzione



AUTORE

Giuseppe Ballistreri

Executive · Senior Advisory Specialist · NATO NSOU Certified Specialist

Senior Security Manager UNI 10459

NOVEMBRE 2026

TLP:CLEAR

Fonti aperte aggiornate all'8 novembre 2026. Immagine di copertina: rendering 3D dell'autore.

© 2026 Giuseppe Ballistreri – Tutti i diritti riservati.

CONTENUTI

Indice

	Sintesi per il vertice
1	Una minaccia in schegge
2	Il volto giovane della radicalizzazione
3	Il cielo come bersaglio: falsi allarmi e disruption
4	Binari e ombre: le attività statali ostili
5	Infrastrutture critiche: dove le schegge convergono
6	Prevenire la convergenza: un modello di lettura
7	Scenario, roadmap e checklist
8	Conclusioni
	Fonti e crediti fotografici

Taglio del documento e metodo

Questa relazione è un'analisi dell'autore sulla frammentazione della minaccia alla sicurezza in Europa, con attenzione all'Italia e alle infrastrutture critiche. Si basa su fonti aperte: il rapporto TE-SAT 2026 di Europol, la relazione dell'intelligence italiana al Parlamento, dichiarazioni istituzionali, cronache verificate su più testate e il monitoraggio di analisti indipendenti [1,2,5,6,18]. Le persone indagate sono presunte innocenti fino a sentenza definitiva; le rivendicazioni e le ipotesi di attribuzione sono riportate come tali. Fonti verificate fino all'8 novembre 2026; modello di lettura, scenario e raccomandazioni sono dell'autore.

La domanda per chi protegge un'infrastruttura

Non più soltanto «chi ci minaccia?», ma **«quali segnali, presi uno per uno innocui, diventano pericolosi quando si sommano, e chi li vede?»**. In un panorama senza un nemico centrale, la sicurezza dipende dalla capacità di unire indizi che oggi restano in uffici, banche dati e organizzazioni diverse.

© 2026 Giuseppe Ballistreri – Tutti i diritti riservati. Riproduzione vietata senza autorizzazione.

SINTESI

Sintesi per il vertice

486	130	27	≥7 voli
arresti per terrorismo nell'UE nel 2025, in crescita da tre anni [1]	minori tra gli arrestati di età nota; il più giovane aveva 12 anni [1]	operazioni antiterrorismo con minori in Italia nel 2025, erano 7 nel 2023 [5]	e una nave colpiti da falsi allarmi bomba in un solo giorno [6]

- **Non c'è una minaccia dominante, ma molte traiettorie in parallelo.** Jihadismo, estremismo violento di destra e nichilista, attività di Stati ostili e disruption a basso costo si muovono insieme, senza un centro di comando comune [18,1].
- **La radicalizzazione è sempre più giovane e veloce.** A Belgrado, il 28 ottobre, un minorenne già monitorato ha aggredito con due coltelli la guardia dell'ambasciata d'Israele; in Italia un caso recente mostra 46 giorni tra la radicalizzazione dichiarata e l'arresto [3,5].
- **Disturbare costa poco.** Tra il 2 e il 5 novembre falsi allarmi bomba hanno colpito voli in mezza Europa, con caccia in volo anche sull'Italia: nessun ordigno, molto disservizio [6,7].
- **Le infrastrutture di trasporto sono osservate.** In Polonia la ricognizione delle ferrovie, spesso affidata ad agenti locali pagati, è considerata il preludio dei sabotaggi [9,12].
- **Raccomandazione:** passare dalla classificazione per ideologia alla lettura degli **indicatori di convergenza** (ideologia, preparazione tecnica, scelta del bersaglio, accesso a risorse) e creare canali stabili tra gestori di infrastrutture, forze di polizia e intelligence.

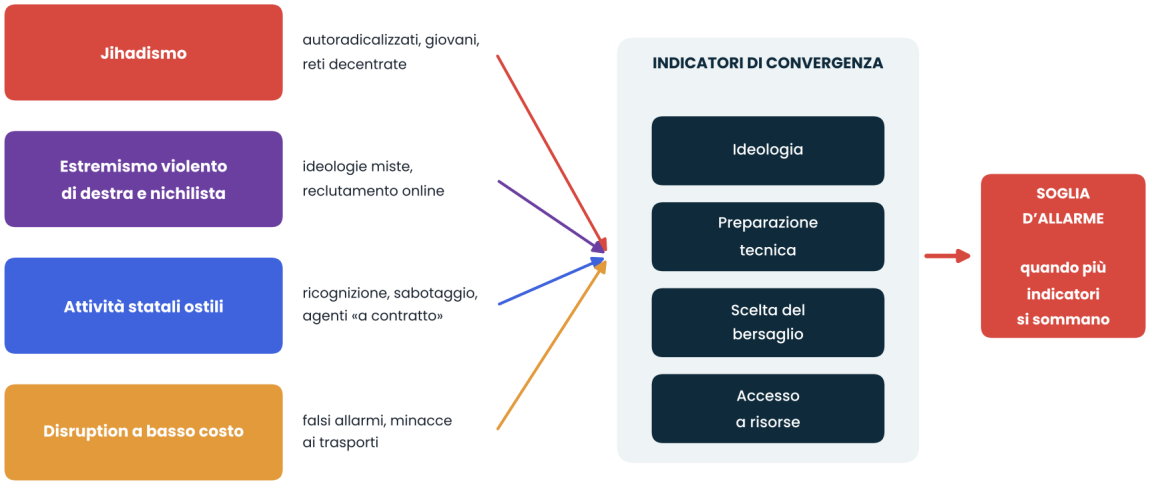


Figura 1 – Quattro traiettorie e quattro indicatori: il rischio cresce quando gli indicatori si sommano. Elaborazione dell'autore.

© 2026 Giuseppe Ballistreri – Tutti i diritti riservati. Riproduzione vietata senza autorizzazione.

SEZIONE 1

Una minaccia in schegge

Per vent'anni la minaccia terroristica in Europa ha avuto un volto riconoscibile: organizzazioni con una catena di comando, campi di addestramento, attentati pianificati. Oggi il quadro si è **frantumato**. Gli attori sono spesso individui o piccoli gruppi senza un legame organizzativo diretto, le ideologie si mescolano e, accanto al terrorismo, crescono attività di Stati ostili che usano gli stessi canali e talvolta le stesse persone [1,18].

I numeri di Europol

Nel 2025 gli Stati membri dell'UE hanno registrato **45 attacchi** tra compiuti, falliti e sventati (58 nel 2024), di cui 24 di matrice jihadista. Gli arresti sono saliti a **486**, per il 71% in procedimenti legati al jihadismo. L'**Italia** è il secondo Paese per numero di attacchi (11), tutti riconducibili all'area anarchica e di sinistra [1].

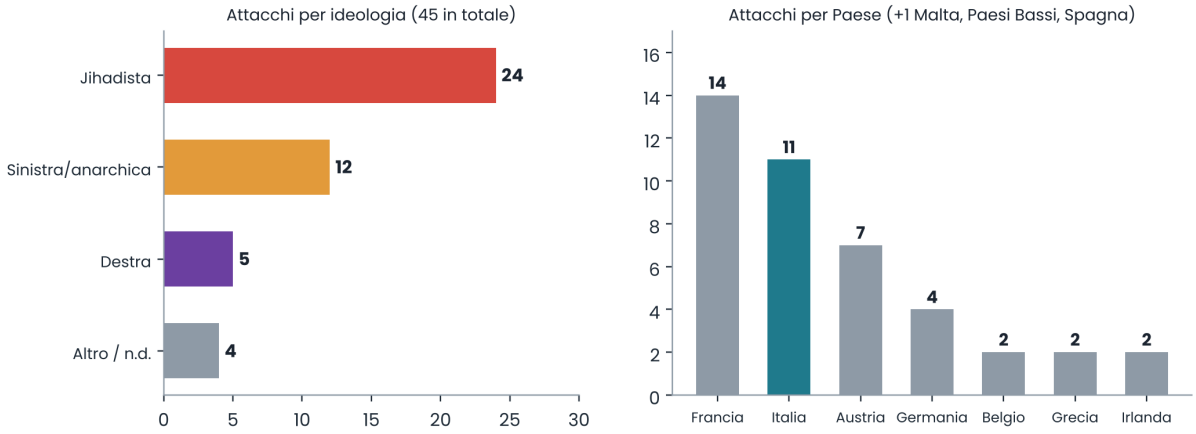


Figura 2 – Attacchi terroristici nell'UE nel 2025. Fonte: Europol TE-SAT 2026 [1].

Il coordinatore antiterrorismo dell'UE descrive così il fenomeno nuovo: ideologie «a buffet», in cui razzismo, misoginia e fascinazione per la violenza si mescolano e catturano giovani senza un percorso ideologico precedente; un estremismo nichilista che «non rientra facilmente nella categoria del terrorismo in senso stretto» [2]. Il jihadismo resta comunque la prima minaccia, e lo Stato islamico si è adattato decentrandosi e cercando reclute direttamente dentro l'UE [2].

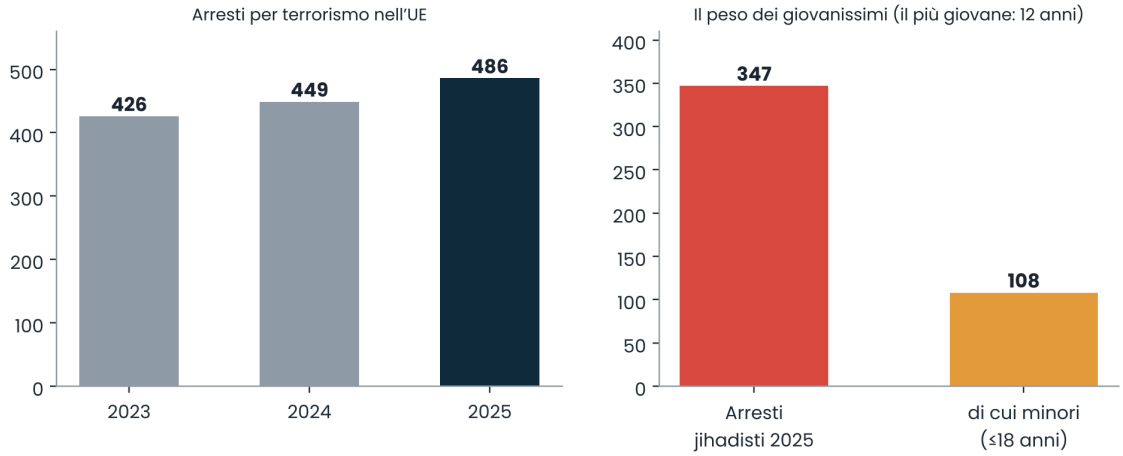


Figura 3 – Arresti per terrorismo nell'UE e peso dei minori. Fonte: Europol TE-SAT 2026 [1].

© 2026 Giuseppe Ballistreri – Tutti i diritti riservati. Riproduzione vietata senza autorizzazione.

SEZIONE 2

Il volto giovane della radicalizzazione

Belgrado, 28 ottobre 2026

All'alba un minorenne armato di due coltelli ha aggredito la guardia della Gendarmeria davanti all'ambasciata d'Israele. L'agente, ferito in modo lieve, ha sparato uccidendo l'aggressore. Le autorità serbe hanno parlato di terrorismo, alzato l'allerta al livello massimo e riferito che il giovane era già monitorato per la vicinanza allo Stato islamico, testimoniata anche da una bandiera nera pubblicata su Instagram [3,4]. La stessa sede era stata colpita nel giugno 2024 con una balestra; non risultano legami operativi tra i due episodi [18].

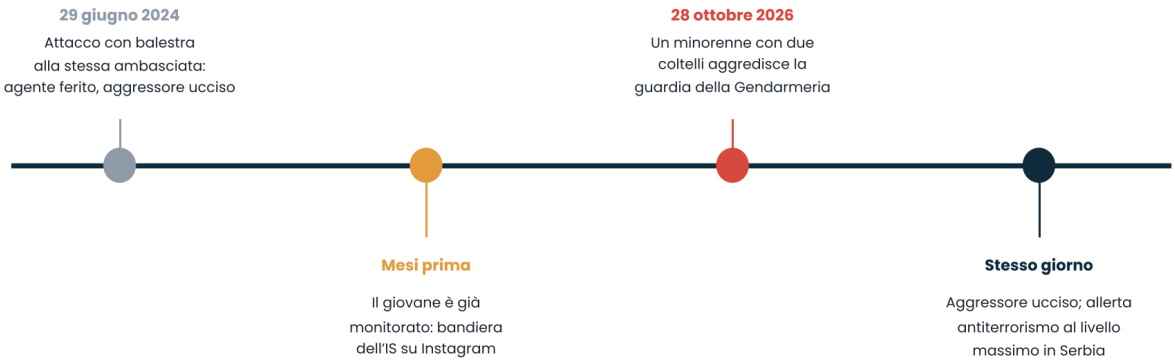


Figura 4 – Due attacchi alla stessa sede a due anni di distanza. Elaborazione dell'autore su [3], [4], [18].

L'Italia nei numeri dell'intelligence

La relazione dell'intelligence italiana al Parlamento registra un aumento netto delle operazioni antiterrorismo che coinvolgono minori: **7 nel 2023, 14 nel 2024, 27 nel 2025**, passate dal 27% al 41% del totale. Nel solo ambito islamista le operazioni sono salite da 22 a 43, e compaiono casi di ragazzi sotto i 14 anni con tempi sempre più brevi tra il primo contatto online e la violenza [5].

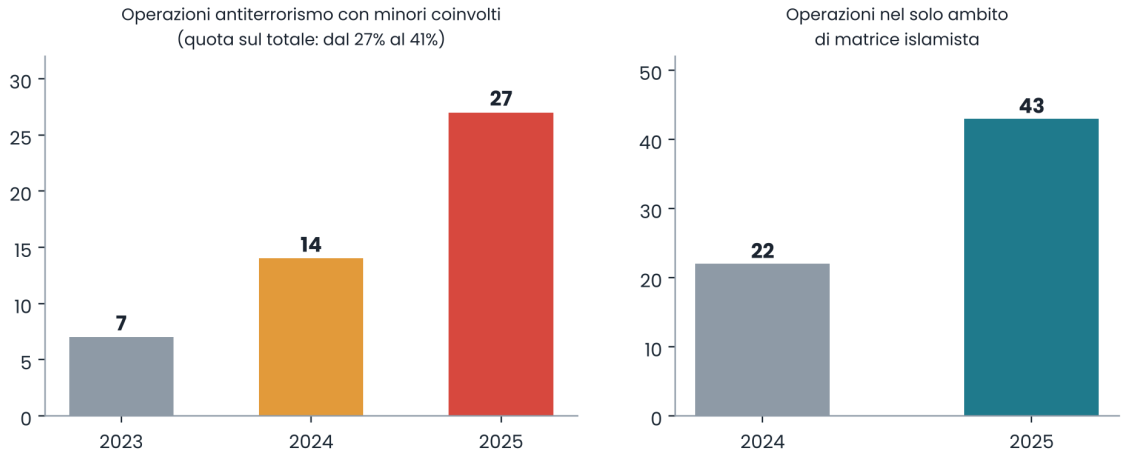


Figura 5 – Operazioni antiterrorismo con minori coinvolti in Italia. Fonte: relazione dell'intelligence al Parlamento, riportata in [5].

© 2026 Giuseppe Ballistreri – Tutti i diritti riservati. Riproduzione vietata senza autorizzazione.

Quarantasei giorni

Un'indagine della Digos di Salerno mostra quanto possa essere breve il percorso. Un 21enne colloca l'inizio della propria radicalizzazione a metà agosto; a settembre ricondivide manuali estremisti e dichiara online di aver costruito un ordigno; il 2 ottobre la perquisizione trova pistole modificate, un machete e una bandiera dello Stato islamico, e scatta l'arresto. Secondo gli inquirenti valutava come bersaglio piazza San Carlo a Torino [5]. Sullo sfondo, ambienti come **TechHaven**, un server di chat frequentato da sostenitori dell'IS che a maggio 2026 contava 12.529 account e 562 stanze [5].



Figura 6 – Dal web alle armi in 46 giorni: la cronologia ricostruita dagli inquirenti. Elaborazione dell'autore su [5]; l'indagato è presunto innocente.

Lo stesso schema attraversa ideologie diverse: in Germania cinque adolescenti di un gruppo di estrema destra sono stati arrestati a maggio per attacchi pianificati contro migranti [14]; in Italia, ad aprile, un 17enne è stato arrestato a Teramo per propaganda neonazista e terrorismo [15], e ad agosto un 16enne per terrorismo di matrice jihadista [16].

SEZIONE 3

Il cielo come bersaglio: falsi allarmi e disruption

Il 3 novembre almeno sette voli di Ryanair, Wizz Air, SAS e LOT e una nave da crociera diretta in Israele hanno ricevuto minacce di bomba. In Italia un volo da Dublino è stato scortato da due Eurofighter dell'Aeronautica militare fino a Fiumicino; in Polonia lo scalo di Modlin è stato chiuso temporaneamente; in Grecia la nave è stata evacuata con circa 1.500 persone a bordo. **Nessun ordigno** è stato trovato [6,8]. Il 5 novembre un nuovo allarme ha fatto dirottare un volo Dublino–Roma su una base aerea militare francese [7].

© 2026 Giuseppe Ballistreri – Tutti i diritti riservati. Riproduzione vietata senza autorizzazione.



Figura 7 – Quattro giorni di falsi allarmi sull'aviazione europea. Elaborazione dell'autore su [6], [7], [8].

Nessuno ha rivendicato e le autorità non hanno attribuito responsabilità; gli analisti del settore ricordano che le minacce false sono uno strumento di disturbo **economico, difficile da attribuire** e coerente con le campagne ibride che diversi governi europei imputano a Russia e Iran, che negano [6,17]. L'effetto è comunque reale: caccia in volo, scali chiusi, passeggeri evacuati, costi per compagnie e Stati.

Perché conta per un gestore

Un falso allarme non danneggia l'infrastruttura, ma ne **consuma la capacità di risposta**. Se ogni minaccia produce la stessa reazione massima, chi la invia ottiene il risultato con un messaggio. Servono protocolli graduati di valutazione della minaccia, condivisi tra gestori, compagnie, enti di controllo e forze di polizia, e una comunicazione pronta a spiegare ai passeggeri che cosa sta accadendo.

SEZIONE 4

Binari e ombre: le attività statali ostili

La terza scheggia non ha un'ideologia ma un mandante. Il 30 ottobre in Polonia è stato arrestato un cittadino russo di 55 anni sorpreso a fotografare treni e infrastrutture ferroviarie con attrezzatura professionale; il coordinatore dei servizi speciali polacchi ha spiegato che i sabotaggi richiedono una ricognizione preliminare e che Mosca preferisce affidarla ad agenti locali pagati [9].



Figura 8 – La Polonia come laboratorio delle minacce alle ferrovie. Elaborazione dell'autore su [9], [10], [11], [12].

© 2026 Giuseppe Ballistreri – Tutti i diritti riservati. Riproduzione vietata senza autorizzazione.

L'episodio si inserisce in una sequenza: nel novembre 2025 un'esplosione sulla linea Varsavia–Lublino, definita dal governo «un atto di sabotaggio senza precedenti»; a luglio 2026 l'identificazione di due sospettati che avrebbero agito per conto della Russia; a settembre lo smantellamento di una rete di spionaggio [10,11,12]. Anche l'intelligence italiana indica la Russia come principale fonte di minaccia ibrida per l'Europa nel 2026 [13].

Il punto di contatto con il terrorismo

Le attività statali ostili e il terrorismo si toccano in un punto preciso: **il reclutamento di esecutori locali**, spesso giovani e pagati, contattati online. È la stessa vulnerabilità sociale sfruttata dalla propaganda estremista, e richiede la stessa attenzione agli indicatori comportamentali più che alle etichette.

SEZIONE 5

Infrastrutture critiche: dove le schegge convergono

Tutte e quattro le traiettorie convergono sugli stessi luoghi: **trasporti, sedi diplomatiche, luoghi affollati, reti**. Per un gestore di infrastruttura critica questo cambia la prospettiva: il rischio non dipende solo da chi attacca, ma dal fatto che il proprio sito sia un bersaglio utile a più attori, per ragioni diverse.

Traiettoria	Interesse tipico per le infrastrutture	Segnale osservabile	Controllo che serve
Jihadismo giovanile	Luoghi affollati, sedi simboliche, nodi di trasporto	Sopralluoghi, domande insolite, interesse per orari e accessi	Sorveglianza e personale formato a segnalare
Estremismo nichilista	Bersagli casuali o simbolici, scuole, comunità	Annunci online («leakage»), ricerca di armi e manuali	Canali di segnalazione con scuole e piattaforme
Attività statali ostili	Ferrovie, energia, logistica militare, telecomunicazioni	Fotografie e rilievi vicino a nodi sensibili	Protezione fisica, segnalazione a polizia e intelligence
Disruption a basso costo	Aviazione, trasporti, servizi pubblici	Ondate di minacce false, spesso coordinate	Protocolli graduati e comunicazione
Rischio interno	Qualsiasi infrastruttura	Dipendenti o fornitori con segnali di radicalizzazione	Verifiche proporzionate, canale riservato

Tabella 1 – Le traiettorie della minaccia viste da un gestore. Elaborazione dell'autore.

Il quadro normativo c'è già: il D.Lgs. 134/2024, che recepisce la direttiva CER, chiede ai soggetti critici valutazioni del rischio e piani di resilienza che includano minacce fisiche, ibride e interne, e la NIS2 copre il lato digitale degli stessi operatori [20,19]. La sfida non è normativa, ma di **integrazione**: sicurezza fisica, cyber, risorse umane e rapporti con le autorità devono leggere gli stessi segnali.

Il rischio interno

La radicalizzazione di un dipendente o di un fornitore con accesso a un sito critico è la forma di convergenza più pericolosa, perché unisce ideologia e accesso. Servono verifiche proporzionate al ruolo, formazione dei responsabili e un canale riservato per segnalare, senza trasformare la prevenzione in sospetto generalizzato.

© 2026 Giuseppe Ballistreri – Tutti i diritti riservati. Riproduzione vietata senza autorizzazione.

SEZIONE 6

Prevenire la convergenza: un modello di lettura

Se le etichette ideologiche spiegano sempre meno, la prevenzione deve guardare ai **comportamenti**. Il percorso dal pensiero all'azione attraversa gradini riconoscibili; ogni gradino è visibile a qualcuno, ma raramente alla stessa persona o allo stesso ufficio.

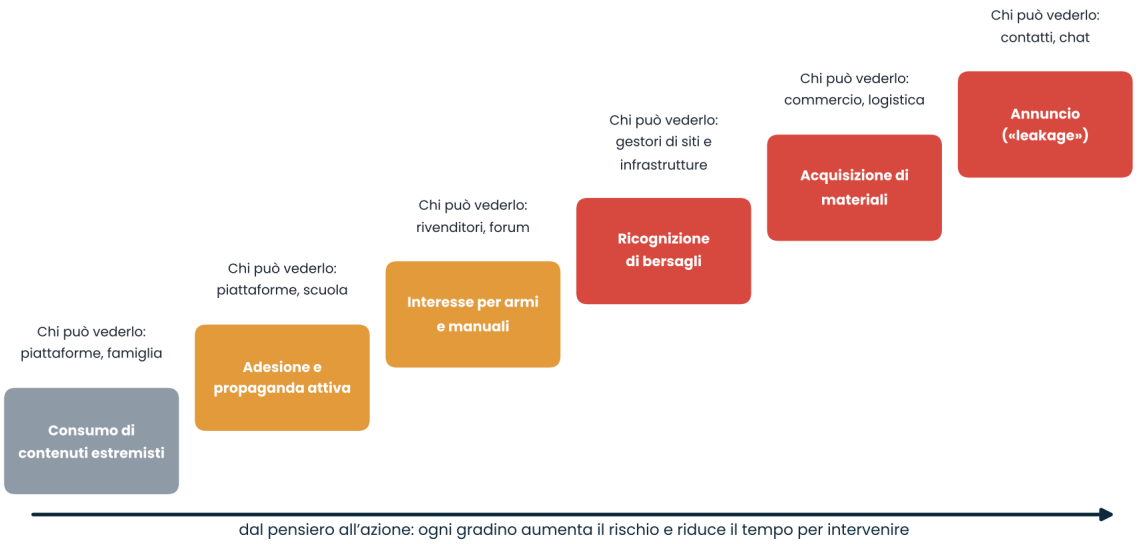


Figura 9 – I gradini dal pensiero all'azione e chi può vederli. Elaborazione dell'autore.

Attore	Che cosa può vedere	Che cosa può fare
Gestori di infrastrutture	Sopralluoghi, fotografie, interessi anomali per accessi e orari	Formare il personale, segnalare, condividere con le autorità
Scuole e famiglie	Isolamento, linguaggio violento, consumo di contenuti estremisti	Dialogo precoce, servizi di supporto, segnalazione
Piattaforme digitali	Propaganda, manuali, annunci di violenza	Rimozione, conservazione delle prove, segnalazione
Commercio e logistica	Acquisti anomali di armi, componenti, precursori	Obblighi di segnalazione delle transazioni sospette
Forze di polizia e intelligence	Il quadro d'insieme, se riceve i segnali	Valutazione, indagine, prevenzione

Tabella 2 – Chi vede che cosa. Elaborazione dell'autore.

© 2026 Giuseppe Ballistreri – Tutti i diritti riservati. Riproduzione vietata senza autorizzazione.

SEZIONE 7

Scenario, roadmap e checklist

Scenario difensivo: «Tre segnali in una settimana»

Scenario ipotetico per esercitazioni. Un gestore di trasporti integrati (scalo aereo e nodo ferroviario), soggetto critico ai sensi del D.Lgs. 134/2024, riceve in pochi giorni tre segnali di natura diversa.

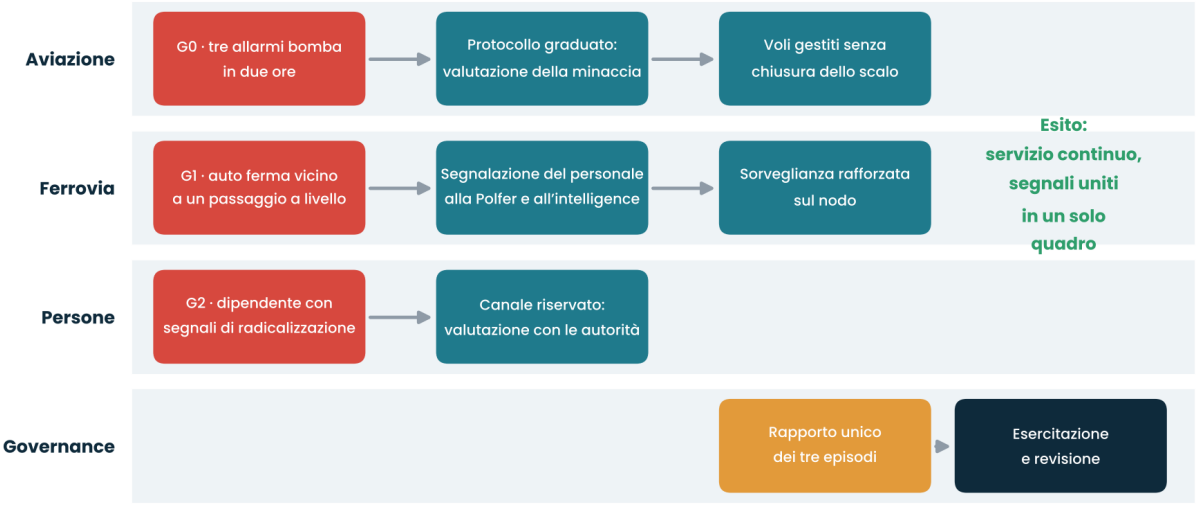


Figura 10 – Lo scenario: tre segnali diversi uniti in un solo quadro. Elaborazione dell'autore.

Roadmap 30-60-90 giorni

Orizzonte	Azioni
0–30 giorni	Mappa dei siti e dei punti di osservazione esterni; formazione rapida del personale a riconoscere e segnalare ricognizioni; protocollo graduato per minacce false; referente unico verso Polfer, Digos e prefettura.
31–60 giorni	Canale riservato per il rischio interno con criteri chiari e tutela dei lavoratori; verifiche proporzionate per i ruoli con accesso critico; condivisione periodica dei segnali con le autorità.
61–90 giorni	Esercitazione sullo scenario con vertice, sicurezza fisica, cyber e risorse umane; integrazione dei segnali nella valutazione del rischio CER; revisione dei piani di comunicazione di crisi.

Tabella 3 – Roadmap. Elaborazione dell'autore.

© 2026 Giuseppe Ballistreri – Tutti i diritti riservati. Riproduzione vietata senza autorizzazione.

Checklist in 12 domande

- ☐ Sappiamo quali nostri siti interessano a più attori diversi?
- ☐ Il personale sa riconoscere e segnalare una ricognizione?
- ☐ Abbiamo un protocollo graduato per le minacce false?
- ☐ C'è un referente unico verso polizia, prefettura e intelligence?
- ☐ Esiste un canale riservato per il rischio interno?
- ☐ Le verifiche sui ruoli critici sono proporzionate e documentate?
- ☐ Sicurezza fisica, cyber e risorse umane condividono i segnali?
- ☐ La valutazione CER include minacce ibride e interne?
- ☐ Abbiamo provato la comunicazione di crisi?
- ☐ I fornitori con accesso ai siti sono censiti?
- ☐ Abbiamo rapporti con scuole e comunità vicine ai siti sensibili?
- ☐ Il vertice riceve un quadro periodico della minaccia?

SEZIONE 8

Conclusioni

La minaccia del 2026 non ha un centro. È fatta di schegge: un ragazzo radicalizzato in poche settimane, un gruppo di adolescenti attratti dalla violenza, un agente pagato per fotografare una ferrovia, una mail che ferma un volo. Prese una per una sembrano piccole; il pericolo nasce quando si incontrano nello stesso luogo, nello stesso momento, nella stessa persona.

Per chi protegge infrastrutture critiche la risposta non è inseguire ogni scheggia, ma **costruire il punto in cui i segnali si incontrano prima che lo facciano le minacce**: personale formato, canali stabili con le autorità, integrazione tra sicurezza fisica, digitale e risorse umane. È un lavoro meno visibile di un controllo all'ingresso, ma è quello che fa la differenza.

Giuseppe Ballistreri
Executive · Senior Advisory Specialist · NATO NSOU Certified Specialist
Senior Security Manager UNI 10459

 © 2026 Giuseppe Ballistreri – Tutti i diritti riservati. Riproduzione vietata senza autorizzazione.

RIFERIMENTI

Fonti e crediti fotografici

[1] Europol, EU Terrorism Situation and Trend Report 2026 (dati 2025), sintesi eucrim, 15/09/2026.
https://eucrim.eu/news/europol-te-sat-2026/

[2] Euronews, intervista al coordinatore antiterrorismo dell'UE B. Wegter, 23/03/2026.
https://www.euronews.com/2026/03/23/children-as-young-as-12-are-getting-radicalised-in-europe-eu-counter-terrorism-chief-tells

[3] Euronews, «Belgrado, attacco davanti all'ambasciata israeliana: ucciso l'aggressore», 28/10/2026.
https://it.euronews.com/2026/10/28/belgrado-attacco-davanti-allambasciata-israeliana-ucciso-laggressore

[4] ANSA (La Voce di New York), «Belgrado, assale poliziotto davanti ambasciata Israele, ucciso», 28/10/2026.
https://lavocedinewyork.com/ansa/2026/10/28/belgrado-assale-poliziotto-davanti-ambasciata-israele-ucciso/

[5] Quotidiano.net, «Dal web alle armi in 46 giorni: così cresce il jihad digitale tra i giovani», 2026.
https://www.quotidiano.net/cronaca/dal-web-alle-armi-in-46-giorni-cosi-cresce-il-jihad-digitale-tra-i-giovani-olk7zxiu

[6] Al Jazeera, «Bomb threats disrupt flights across Europe, no explosive devices found», 04/11/2026.
https://aljazeera.com/news/2026/11/4/bomb-threats-disrupt-flights-across-europe-no-explosive-devices-found

[7] Al Jazeera, «New bomb threats force more European flights into emergency landings», 05/11/2026.
https://aljazeera.com/news/2026/11/5/bomb-threat-diverts-dublin-rome-flight-to-france

[8] The Local, «Hoax bomb threats disrupt flights in Europe», 03/11/2026.
https://www.thelocal.dk/20261103/hoax-bomb-threats-disrupt-flights-in-europe

[9] Meduza, «Russian man arrested in Poland on espionage charges after photographing trains», 30/10/2026.
https://meduza.io/en/news/2026/10/30/russian-man-arrested-in-poland-on-espionage-charges-after-photographing-trains

[10] The Moscow Times, «Poland says 2 Ukrainians working for Russia suspected in railway sabotage», 27/07/2026.
https://www.themoscowtimes.com/2026/07/27/poland-says-2-ukrainians-working-for-russia-suspected-in-railway-sabotage

[11] The Moscow Times, «Poland dismantles Russian spy ring», 25/09/2026.
https://www.themoscowtimes.com/2026/09/25/poland-dismantles-russian-spy-ring

[12] Defense Magazine, «Explosion on a railway line in Poland: Warsaw accuses Russia of sabotage attack».
https://www.defensemagazine.com/article/explosion-on-a-railway-line-in-poland-warsaw-accuses-russia-of-sabotage-attack

[13] Dire, «L'allarme degli 007 italiani: nel 2026 la Russia principale minaccia per l'Europa», 04/03/2026.
https://www.dire.it/04-03-2026/1220128-lallarme-degli-007-italiani-nel-2026-la-russia-principale-minaccia-per-leuropa/

[14] Euronews, «Germany arrests five teenagers over alleged right-wing extremist plot and attacks», 21/05/2026.
https://www.euronews.com/2026/05/21/germany-arrests-five-teenagers-over-alleged-right-wing-extremist-plot-and-attacks

[15] Sky TG24, «Giovane accusato di propaganda neonazista e terrorismo: 17enne arrestato a Teramo», 13/04/2026.
https://tg24.sky.it/cronaca/2026/04/13/terrorismo-neonazismo-arresto-teramo

[16] AGI, caso di un 16enne arrestato per terrorismo, 07/08/2026.
https://www.agi.it/cronaca/news/2026-08-07/16enne-terrorismo-bombe-isis-38427906/

[17] Osprey Flight Solutions, «Bomb threats: disruption at European airports amid the Russia-Ukraine conflict».
https://www.ospreyflightsolutions.com/casestudy/bomb-threats-disruption-at-european-airports/

[18] D. Garofalo, «The Fragmented Threat», Weekly Threat Shift n. 25, 05/11/2026.
https://www.danielegarofalomonitoring.com/p/the-fragmented-threat

[19] ICT Security Magazine, «NIS2 e D.Lgs. 138/2024: stato del recepimento e adempimenti 2026».
https://www.ictsecuritymagazine.com/articoli/nis2-e-d-lgs-138-2024/

[20] DirittoBancario, «Direttiva CER: il decreto di recepimento in Gazzetta Ufficiale» (D.Lgs. 134/2024).
https://www.dirittobancario.it/art/direttiva-cer-il-decreto-di-recepimento-in-gazzetta-ufficiale/

Crediti fotografici

Le fotografie reali saranno inserite con autore, licenza e link alla fonte.

Documento elaborato a scopo informativo e preventivo. Le persone citate come indagate sono presunte innocenti fino a sentenza definitiva; rivendicazioni e ipotesi di attribuzione sono riportate come tali. Grafici di sintesi, modello di lettura, scenario e raccomandazioni sono elaborazioni dell'autore. Immagine di copertina: rendering 3D dell'autore.

© 2026 Giuseppe Ballistreri – Tutti i diritti riservati. Riproduzione vietata senza autorizzazione.