

DOSSIER



FONDAZIONE
MACHIAVELLI



n. 61 - aprile 2026

GUERRA IBRIDA E RESILIENZA IN EUROPA- LEZIONI DAL FIANCO ORIENTALE PER LA SICUREZZA EURO-ATLANTICA

Fabrizio Minniti

toque agere

MachiavelliDossier

n. 61 - aprile 2026

«Guerra ibrida e resilienza in Europa. Lezioni dal fianco orientale per la sicurezza euro-atlantica»
di Fabrizio Minniti

© 2026 Fondazione Machiavelli
Via Giambologna 7, Firenze
Riproduzione consentita con attribuzione

ISSN 2612-047X

SOMMARIO ESECUTIVO

- Il *report* analizza la guerra ibrida nell'area euro-atlantica, con particolare attenzione ai casi baltici e nordici, evidenziando come la competizione contemporanea si sviluppi stabilmente al di sotto della soglia del conflitto aperto attraverso l'integrazione di strumenti militari e non militari.
- In questo contesto, la guerra ibrida non mira alla distruzione fisica, ma alla paralisi decisionale e all'erosione della fiducia collettiva. Gli attacchi *cyber* all'Estonia nel 2007, la crisi del sistema eID nel 2017 e le recenti vulnerabilità nel Mar Baltico riflettono una logica ricorrente: colpire la continuità operativa dello Stato.
- Gli effetti più duraturi si manifestano nel dominio cognitivo, dove le operazioni di influenza compromettono la fiducia nelle istituzioni e la coerenza narrativa delle società. I modelli nordici mostrano come la resilienza in questo ambito derivi da politiche di lungo periodo, fondate su alfabetizzazione mediatica e coordinamento tra attori pubblici e privati.
- L'esperienza estone evidenzia il nesso tra digitalizzazione e sovranità: l'innovazione rafforza lo Stato, ma introduce vulnerabilità che richiedono preparazione anticipata e continuità operativa. Nei Paesi baltici, la resilienza si costruisce sull'integrazione tra difesa territoriale, resistenza non convenzionale e coinvolgimento della popolazione, aumentando i costi di un'aggressione senza eliminarne la possibilità.
- Parallelamente, la cooperazione nordica mostra come l'allineamento strategico possa precedere l'adesione formale ad alleanze militari, attraverso una pianificazione operativa già consolidata prima del 2022.
- Per l'Italia, la distanza geografica dalla Russia non equivale a immunità. Le principali criticità riguardano il dominio cognitivo, la frammentazione della risposta istituzionale e la limitata diffusione di una cultura della sicurezza. In questo quadro, il DPCM dell'8 gennaio 2026 rappresenta un passaggio rilevante nel rafforzamento del coordinamento informativo.
- Nel complesso, il confronto con i modelli nordici e baltici evidenzia la necessità di sviluppare anche in Italia una strategia di resilienza di lungo periodo, fondata su continuità istituzionale, integrazione interagenzia e coinvolgimento della società civile. ■



L'AUTORE

Fabrizio Minniti è un esperto di sicurezza internazionale. Come ricercatore presso il Centro Militare di Studi Strategici, ha redatto rapporti nei settori dell'*intelligence*, del terrorismo internazionale, della dottrina nucleare, della sicurezza europea e della politica di difesa. È stato nominato consulente esterno per EUBAM-Rafah in Israele e ha lavorato come consigliere politico del DCOM della missione NATO *Resolute Support* in Afghanistan. ■

1. Introduzione e quadro concettuale

Nel settembre 2020, i ministri della Difesa di Norvegia, Svezia e Finlandia si incontrano a Porsangmoen, nel Finnmark norvegese, a circa duecento chilometri dal confine russo, per firmare una dichiarazione sulla cooperazione operativa rafforzata. La scelta del luogo non è casuale: in quell'area è in corso il consolidamento delle forze terrestri norvegesi. Alla domanda sul significato dell'intesa, il ministro svedese Peter Hultqvist risponde in modo diretto: «mandare un segnale chiaro alla Russia» (Saxi, 2022).

L'episodio sintetizza, in modo quasi paradigmatico, una trasformazione più ampia della sicurezza europea nel secondo decennio del XXI secolo: il passaggio dalla dimensione dichiarativa alla pianificazione operativa concreta. Paesi che per decenni avevano fondato la propria postura sulla neutralità o sul disimpegno strategico si orientano verso la predisposizione di “piani di guerra”, in un contesto in cui la distinzione tra pace e conflitto risulta sempre più sfumata. L'invasione russa dell'Ucraina nel febbraio 2022 ha confermato la persistenza del confronto militare convenzionale, ma anche la centralità di forme di competizione che si sviluppano al di sotto di tale soglia.

In questo quadro si inserisce la nozione di guerra ibrida, intesa — secondo la definizione del rapporto RAND del 2019 — come l'uso combinato di strumenti politici, informativi, militari e non militari, palesi e occulti, per perseguire obiettivi strategici senza innescare una risposta militare convenzionale (Flanagan *et al.*, 2019). L'elemento decisivo non è il singolo strumento, ma la loro integrazione, che produce effetti cumulativi difficilmente attribuibili e quindi più difficili da contrastare.

Il caso estone del 2007 rappresenta il riferimento empirico più chiaro di questa logica: una combinazione di disordini interni, pressione diplomatica, misure economiche e attacchi *cyber* fu in grado di paralizzare il Paese senza superare formalmente la soglia del conflitto armato. Negli anni successivi, tali dinamiche si

sono evolute in forme più sofisticate, integrando strumenti statali e reti informali e anticipando la risposta già nelle fasi iniziali della crisi.

Il caso estone del 2007 è esemplare: una combinazione di disordini interni, pressione diplomatica, misure economiche e attacchi cyber fu in grado di paralizzare il Paese senza superare formalmente la soglia del conflitto

È tuttavia nel dominio cognitivo che la guerra ibrida produce i suoi effetti più duraturi. L'obiettivo non è orientare singole opinioni, ma compromettere la fiducia nelle istituzioni,

nell'informazione e nella possibilità stessa di una risposta collettiva. La sicurezza assume così una dimensione più ampia, che include la tenuta dell'identità collettiva e della coerenza narrativa dello Stato (Vuorelma, 2025). Le minacce *cyber* rappresentano in modo emblematico questa intersezione tra dimensione tecnica e politica: transfrontaliere, difficili da attribuire e, spesso, caratterizzate da una molteplicità di attori, richiedono forme di *governance* distribuita e coordinamento tra pubblico e privato (Skierka, 2023).

L'annessione della Crimea nel 2014 ha segnato un ulteriore punto di rottura, imponendo una revisione profonda della pianificazione militare europea. Come osservato dal generale norvegese Rune Jacobsen, si è passati “dal credere alla pace per sempre al dovere rivitalizzare tutta la pianificazione” (Saxi, 2022). In questo contesto, vulnerabilità geografiche come il corridoio di Suwałki — circa 100 km tra Polonia e Lituania — assumono un rilievo strategico centrale, soprattutto in scenari caratterizzati da azioni rapide e difficilmente attribuibili.

Il problema non è soltanto la velocità dell'eventuale aggressione, ma la sua plausibile negabilità. Il modello degli “omini verdi”, sperimentato in Crimea, dimostra come operazioni senza insegne possano

ritardare o paralizzare la risposta alleata nelle fasi iniziali. Le risposte adottate nell'area baltica — dalla predisposizione di infrastrutture difensive al rafforzamento della presenza NATO — mirano quindi non tanto a impedire un attacco in senso assoluto, quanto a rallentarlo e ad aumentarne i costi politici e militari.

A queste dinamiche si aggiungono vulnerabilità strutturali più ampie. I Paesi del gruppo *Bucharest Nine* presentano livelli di resilienza mediamente inferiori alla media UE, mentre il dominio sottomarino evidenzia una crescente esposizione a operazioni difficilmente attribuibili, come dimostrano gli episodi che hanno coinvolto infrastrutture energetiche e di comunicazione nel Mar Baltico tra il 2022 e il 2024. In un contesto normativo che limita la capacità di risposta degli Stati, questa ambiguità operativa si configura come uno degli strumenti più efficaci della competizione ibrida.

In questa sede vogliamo analizzare le esperienze di Estonia, Lettonia, Lituania, Finlandia e Svezia nel periodo compreso tra il 2014 e il 2023, con l'obiettivo non di proporre modelli replicabili in senso stretto, ma di comprendere le condizioni che ne hanno reso possibile il funzionamento e i limiti della loro trasferibilità, anche nel caso italiano.

2. Il Laboratorio Baltico

Definire gli Stati baltici come un “laboratorio della sicurezza europea” non è una semplificazione retorica, ma il riflesso di una condizione strutturale. La loro posizione geografica, la memoria dell'occupazione sovietica e la prossimità alla Russia li hanno esposti in modo anticipato e continuativo a forme di pressione ibrida che altri Paesi europei hanno sperimentato solo in una fase successiva.

In questo contesto, la resilienza non emerge come risposta contingente, ma come esito di un processo di adattamento di lungo periodo. Più che modelli replicabili in senso stretto, i casi baltici offrono logiche operative che si sviluppano a partire da vulnerabilità specifiche e da vincoli difficilmente eludibili.

Ciò che accomuna Estonia, Lettonia e Lituania non è tanto l'omogeneità delle soluzioni adottate, quanto la capacità di trasformare condizioni di esposizione in strumenti di preparazione. In ciascun caso, la resilienza si struttura attorno a un asse prevalente — continuità dello Stato, coesione sociale o deterrenza territoriale — che riflette la natura della minaccia percepita.

Il valore di questo “laboratorio” risiede quindi, non a caso, meno nella trasferibilità diretta delle singole misure, quanto nella coerenza tra vulnerabilità, scelte strategiche e strumenti operativi. È in questa relazione che si colloca la principale lezione per altri contesti, incluso quello italiano.

2.1 Estonia: la sovranità digitale come strategia di resilienza

La digitalizzazione estone, avviata negli anni Novanta, non è stata soltanto una scelta di modernizzazione amministrativa, ma una decisione strategica di sovranità: costruire un'infrastruttura statale digitale prima che fossero altri a definirne standard e vulnerabilità. Il sistema di identità elettronica (eID) rappresenta oggi il pilastro di questa architettura, utilizzato regolarmente da una quota significativa della popolazione per l'accesso ai servizi pubblici.

Questa scelta ha tuttavia esposto il Paese a un rischio strutturale: maggiore è il livello di integrazione digitale, maggiore è la superficie di attacco. La crisi del 2017, legata a una vulnerabilità crittografica che interessava una larga parte delle carte d'identità elettroniche, ha reso evidente questo paradosso. I sistemi critici non possono essere semplicemente disattivati quando risultano vulnerabili, perché la loro interruzione produrrebbe effetti immediati sulla continuità dello Stato.

La gestione della crisi ha mostrato i tratti distintivi del modello estone. In primo luogo, la presenza di un'architettura tecnica flessibile ha consentito una rapida migrazione verso soluzioni più sicure. In secondo luogo, la *governance* distribuita — che coinvolge attori pubblici e privati — ha permesso un coordinamento efficace senza improvvisazioni. Un elemento meno visibile, ma decisivo, è rappresentato dalla continuità delle relazioni professionali tra i responsabili della sicurezza, maturata anche durante le crisi precedenti, in particolare gli attacchi del 2007.

A ciò si aggiungono due fattori spesso trascurati: un processo di valutazione del rischio continuo, e una gestione della comunicazione pubblica coerente e trasparente, che ha evitato effetti destabilizzanti sulla fiducia dei cittadini. La crisi non è stata quindi un'eccezione, ma una prova di tenuta di un sistema già strutturato.

Sul piano della difesa territoriale, l'Estonia integra la dimensione digitale con una forte componente di mobilitazione civile. Il *Kaitseliit* (*Defence League*), organizzazione volontaria radicata a livello locale, rappresenta un elemento chiave della difesa totale, rafforzando il legame tra sicurezza nazionale e partecipazione della popolazione.

Nel complesso, il caso estone mostra come la resilienza non derivi dall'assenza di vulnerabilità, ma dalla capacità di gestirle senza interrompere il funzionamento dello Stato. È un modello costruito nel tempo, in cui tecnologia, *governance* e cultura della sicurezza operano in modo integrato.

2.2 Lettonia: la resilienza come problema di coesione

La principale vulnerabilità della Lettonia non è di natura geografica o tecnologica, ma sociale. La presenza di una significativa minoranza russofona è stata a lungo interpretata, nella narrativa del Cremlino, come un potenziale fattore di instabilità interna e come possibile leva per operazioni di influenza o intervento sotto soglia.

Le evidenze empiriche restituiscono tuttavia un quadro più articolato. La comunità russofona non costituisce un blocco omogeneo, né appare automaticamente allineata alle posizioni di Mosca. L'esperienza del Donbass, con i costi umani ed economici associati al conflitto, ha contribuito a ridimensionare l'attrattiva di tali narrazioni. Ciò non elimina la vulnerabilità, ma ne modifica i termini: il

La comunità russofona lettone non è un blocco omogeneo, né appare allineata alle posizioni di Mosca. L'esperienza del Donbass, con i costi del conflitto, ha contribuito a ridimensionare l'attrattiva delle narrazioni irredentiste

problema centrale non è il controllo di una minoranza, bensì la capacità di rafforzare la coesione complessiva della società.

La risposta lettone si è sviluppata lungo questa direttrice. A partire dalla metà degli anni 2010, il Paese ha progressivamente reintrodotta un modello di difesa totale, fondato

non solo sul rafforzamento delle capacità militari, ma sull'integrazione tra istituzioni, settore privato e popolazione. Il Concetto di Difesa Nazionale e le strategie successive enfatizzano il coinvolgimento della società civile, la cooperazione multilivello e l'importanza della preparazione anche in tempo di pace.

Un elemento distintivo è rappresentato dall'investimento nella dimensione educativa e comunicativa. L'introduzione di programmi di difesa nazionale nel sistema scolastico e il rafforzamento della comunicazione strategica mirano a costruire una consapevolezza diffusa dei rischi e delle responsabilità collettive. In questa prospettiva, la resilienza non è concepita come mera capacità di resistere a uno *shock* esterno, ma come risultato di un processo continuo di integrazione sociale e istituzionale.

Permangono tuttavia limiti strutturali, in particolare sul piano delle risorse e della capacità militare,

che rendono il modello lettone meno robusto rispetto a quello estone o finlandese. Proprio per questo, il caso lettone evidenzia un aspetto spesso sottovalutato: la resilienza non è solo una questione di capacità materiali, ma dipende in misura decisiva dalla qualità del tessuto sociale e dal livello di fiducia reciproca tra Stato e cittadini.

2.3 Lituania: la geografia come vincolo strategico

Tra i Paesi baltici, la Lituania è quello maggiormente esposto sul piano geografico. La sua posizione, a ridosso dell'exclave russa di Kaliningrad e in prossimità del corridoio di Suwałki, la colloca al centro di uno dei punti più vulnerabili dell'intero fianco orientale della NATO. In uno scenario di crisi, l'interruzione di questo corridoio rischierebbe di isolare fisicamente gli Stati baltici dal resto dell'Alleanza.

A differenza del caso lettone, dove la vulnerabilità è prevalentemente sociale, o di quello estone, dove è legata alla dimensione digitale, la sfida lituana è immediatamente territoriale. La risposta si è quindi sviluppata in modo pragmatico, puntando a rafforzare la capacità di resistenza sin dalle fasi iniziali di un eventuale conflitto.

La reintroduzione della leva obbligatoria, il rafforzamento della difesa territoriale e la predisposizione di strumenti operativi rivolti direttamente alla popolazione — come le guide alla resistenza in caso di invasione — riflettono una strategia orientata ad aumentare i costi di qualsiasi aggressione. L'obiettivo non è impedire un attacco in senso assoluto, ma renderne più complessa e onerosa l'esecuzione, riducendo il vantaggio di eventuali azioni rapide.

Questo approccio evidenzia una logica diversa rispetto agli altri casi baltici: la resilienza non è costruita solo sulla continuità dello Stato o sulla coesione sociale, ma sulla capacità di trasformare la vulnerabilità geografica in un fattore di deterrenza. In altre parole, la geografia non viene superata, ma gestita. Il caso lituano mostra quindi come, in contesti di esposizione diretta, la resilienza passi attraverso una combinazione di preparazione militare, coinvolgimento della popolazione e pianificazione anticipata. Anche in questo caso, si tratta di un processo di lungo periodo, in cui la credibilità della risposta è parte integrante della deterrenza.

In Lituania è stata attuata una strategia per aumentare i costi di una aggressione, con reintroduzione dell'obbligo di leva, rafforzamento della difesa territoriale e predisposizione di strumenti operativi

3. Cooperazione nordica e modelli di resilienza

Negli anni successivi al 2014, la cooperazione tra i Paesi nordici ha seguito un percorso che non può essere spiegato esclusivamente attraverso la categoria di "alleanza". Accanto alle forme tradizionali di cooperazione formalizzata, si è sviluppato un modello più flessibile di allineamento, fondato su aspettative operative reciproche non necessariamente codificate in obblighi giuridici vincolanti.

In questo quadro, Svezia e Finlandia hanno occupato a lungo una posizione intermedia: formalmente esterne alla NATO, ma progressivamente integrate nella pianificazione operativa dell'area. La cooperazione si è tradotta nello sviluppo di capacità congiunte e nella predisposizione di scenari che includevano esplicitamente anche il conflitto armato, superando di fatto la distinzione tra tempo di pace e tempo di guerra.

Un passaggio cruciale è rappresentato dalle iniziative avviate a partire dal 2020, tra cui la dichiarazione di Porsangmoen, che ha promosso il coordinamento dei piani operativi nelle aree di interesse comune. L'asimmetria tra Paesi NATO e non-NATO è stata superata attraverso la previsione del trasferimento

del comando operativo all'Alleanza in caso di crisi o conflitto, rendendo compatibili diversi livelli di integrazione.

Questa evoluzione si inserisce in un contesto operativo caratterizzato da ambiguità e negabilità, in cui la distinzione tra pace e guerra tende a sfumare. In tali condizioni, la pianificazione non può essere reattiva, ma deve estendersi alle fasi precedenti al conflitto aperto, con l'obiettivo di garantire continuità di azione anche in scenari incerti.

La logica sottostante è condivisa anche nei modelli baltici di resistenza non convenzionale: più che la sequenza delle fasi, rileva la capacità di evitare vuoti operativi nelle fasi iniziali. La resilienza non si limita alla dimensione militare, ma coinvolge strutture civili in grado di operare anche senza ricorso alla forza, attraverso attività di supporto, informazione e coordinamento.

Questo approccio distribuisce le capacità sul territorio, riducendo la vulnerabilità a neutralizzazioni rapide, ma introducendo al contempo rischi — tra cui perdita di controllo ed *escalation* — che richiedono integrazione con le forze regolari e meccanismi di coordinamento.

Nel complesso, emerge un elemento centrale: la resilienza non consiste soltanto nella capacità di assorbire un attacco, ma nella possibilità di continuare a operare anche in condizioni di degradazione del controllo statale. È in questa continuità operativa che si gioca la capacità di resistere nelle fasi più critiche.

3.1 Finlandia: la resilienza come preparazione strutturale

La Finlandia rappresenta un caso peculiare, in cui la neutralità storica ha coesistito con un livello di preparazione difensiva superiore a quello di molti membri NATO. La difesa totale non è mai stata abbandonata dopo la Guerra Fredda: la leva obbligatoria è rimasta in vigore e il sistema di sicurezza comprensiva (*kokonaisturvallisuus*) si è sviluppato come architettura concreta, fondata su strutture operative, pianificazione e continuità istituzionale.

Quando l'invasione russa dell'Ucraina ha reso inevitabile la scelta di aderire alla NATO, la Finlandia disponeva già delle condizioni necessarie per sostenere una trasformazione anche sul piano identitario. Come osservato in letteratura, la neutralità aveva funzionato non come alternativa alla sicurezza, ma come cornice entro cui sviluppare una capacità difensiva avanzata.

La strategia finlandese integra dimensioni militari e civili in un unico sistema: difesa psicologica, sicurezza interna, protezione dei servizi critici e preparazione della popolazione. Un esempio significativo è rappresentato da *Mediapooli*, il consorzio pubblico-privato incaricato di garantire la continuità delle comunicazioni in caso di crisi, insieme all'integrazione dell'alfabetizzazione mediatica nei programmi scolastici. In questo modello, la resilienza non deriva dall'assenza di vulnerabilità, ma dalla capacità di gestirle senza interrompere il funzionamento dello Stato.

3.2 Svezia: identità e difesa psicologica

La traiettoria svedese presenta caratteristiche diverse, legate a una tradizione di neutralità più lunga e radicata. Il non-allineamento ha costituito per oltre due secoli un elemento centrale dell'identità nazionale, rendendo la transizione verso la NATO più complessa sul piano politico e simbolico.

Questo passaggio è stato tuttavia gestito attraverso un processo graduale di adattamento, in cui la ridefinizione della postura strategica è avvenuta senza una rottura netta con il passato. La cooperazione operativa con *partner* occidentali e l'integrazione progressiva nelle strutture di sicurezza euro-atlantiche hanno preparato il terreno

per la scelta finale.

Un elemento distintivo del modello svedese è l'istituzionalizzazione della difesa psicologica. Nel 2022 è stata creata un'agenzia dedicata al contrasto delle operazioni di influenza e al rafforzamento della fiducia nelle istituzioni, affiancata da strumenti di preparazione civile diffusa. Tra questi, il manuale "Se arriva la crisi o la guerra", distribuito alla popolazione, rappresenta un esempio concreto di coinvolgimento attivo dei cittadini nella gestione delle emergenze.

La logica sottostante è chiara: nei primi momenti di uno *shock* sistemico, lo Stato non può essere ovunque. Una popolazione preparata consente di assorbire l'impatto iniziale e di concentrare le risorse pubbliche nei contesti più critici. In questo senso, la resilienza si costruisce non solo attraverso capacità militari, ma anche attraverso fiducia, preparazione e partecipazione.

4. Il caso italiano

L'Italia non confina con la Russia né è esposta alle stesse pressioni dei Paesi nordici e baltici; tuttavia, la distanza geografica non equivale a immunità rispetto alle dinamiche della guerra ibrida. Le principali vulnerabilità emergono soprattutto sul piano della fiducia e della percezione pubblica: permeabilità alla disinformazione, fragilità della fiducia nelle istituzioni e difficoltà di coordinamento interistituzionale. In questo senso, il divario rispetto a contesti come quello estone riflette non solo differenze di capacità, ma soprattutto l'assenza di una cultura della sicurezza consolidata nel tempo.

Negli anni 2024-2026, l'Italia ha avviato un adattamento progressivo del proprio sistema di sicurezza alla logica della competizione ibrida, senza una riforma organica ma attraverso interventi mirati. Il DPCM dell'8 gennaio 2026 rappresenta un passaggio centrale, rafforzando il ruolo del Dipartimento delle informazioni per la sicurezza (DIS) come snodo di coordinamento strategico e integrazione informativa. Ne deriva una maggiore centralizzazione decisionale e una risposta più rapida e integrata alle minacce multidimensionali.

Negli anni 2024-2026, l'Italia ha avviato un adattamento progressivo del proprio sistema di sicurezza alla logica della competizione ibrida, senza una riforma organica ma attraverso interventi mirati

Parallelamente, si osserva una trasformazione della funzione dell'*intelligence*, sempre più orientata al supporto diretto al processo decisionale. Assumono rilievo l'analisi predittiva,

l'impiego di tecnologie avanzate — in particolare l'intelligenza artificiale — e lo sviluppo di forme di "*soft intelligence*" finalizzate alla protezione delle infrastrutture critiche e della resilienza sociale.

Anche lo strumento militare si adatta a una logica multi-dominio e interagenzia. Le Forze Armate contribuiscono alla protezione del sistema-Paese oltre il perimetro della difesa territoriale, con un rafforzamento delle capacità informative e di integrazione con domini *cyber* ed elettromagnetico. In questo quadro, il II Reparto Informazioni e Sicurezza (RIS) consolida il proprio ruolo nella fusione informativa interforze e nel supporto alle operazioni, in particolare nei contesti NATO.

Il confronto con i modelli nordici evidenzia tuttavia un ritardo strutturale. La resilienza, come mostrano i casi estone, svedese e finlandese, richiede continuità istituzionale, investimenti di lungo periodo e coinvolgimento della società civile. In Italia, iniziative come l'istituzione dell'Agenzia per la cybersicurezza nazionale rappresentano un progresso, ma non colmano un divario costruito nel tempo.

Un ulteriore limite riguarda la dimensione regionale. A differenza dei Paesi nordici, l'Italia non ha ancora sviluppato un livello comparabile di integrazione operativa con i *partner* del fianco sud della NATO, nonostante la centralità strategica del Mediterraneo e l'esposizione di infrastrutture critiche e rotte energetiche.

Infine, permane la questione della preparazione della popolazione. I modelli nordici dimostrano che la resi-

lienza richiede una cultura della sicurezza diffusa, integrata nei sistemi educativi e sostenuta da una narrativa nazionale coerente. In Italia, questo processo è ancora in fase iniziale.

In sintesi, emergono cinque direttrici principali:

- rafforzamento del coordinamento centrale attraverso il DIS;
- evoluzione dell'*intelligence* verso funzioni predittive;
- adattamento della Difesa a un modello multi-dominio;
- crescita operativa del RIS;
- persistenti criticità nella cultura della sicurezza.

Nel complesso, l'Italia sta transitando verso un modello di resilienza fondato sulla protezione integrata del sistema-Paese, ma il percorso resta, almeno in questa fase, incompleto e dipende dalla capacità di consolidare nel tempo una cultura strategica condivisa.

Il confronto con le esperienze nordiche e baltiche suggerisce tre priorità per l'architettura di sicurezza italiana.

- **Istituzionalizzare la difesa psicologica.** Il contrasto alla disinformazione non può essere affidato a strumenti temporanei. È necessario un organismo stabile, con mandato esplicito sul dominio cognitivo, in grado di rafforzare la fiducia nelle istituzioni e la qualità del dibattito pubblico.
- **Sviluppare una dimensione operativa mediterranea.** Come la regione nordica ha riconosciuto la propria interdipendenza strategica, l'Italia dovrebbe promuovere una pianificazione integrata con i *partner* del fianco sud, per proteggere infrastrutture critiche, corridoi energetici e dorsali dati esposte a minacce sotto soglia.
- **Investire nella preparazione della popolazione.** La resilienza inizia dalla società. L'introduzione di alfabetizzazione mediatica e gestione del rischio nei percorsi educativi è essenziale per trasformare i cittadini in attori consapevoli della sicurezza nazionale.

5. Qualche considerazione finale

Il denominatore comune dei modelli analizzati non risiede nella tecnologia, pur centrale nel caso estone, né esclusivamente nell'incremento della spesa militare, come nel caso lituano. L'elemento decisivo è la coerenza tra scelte strategiche, identità collettiva e strutture costruite per difenderla.

La Finlandia ha potuto completare rapidamente il proprio percorso verso la NATO grazie a una preparazione accumulata nel tempo, che ha reso sostenibile anche un cambiamento profondo sul piano politico e identitario. La Svezia ha seguito un percorso più graduale, ma altrettanto coerente, fondato sull'adattamento progressivo delle proprie istituzioni e sull'istituzionalizzazione della difesa psicologica.

In entrambi i casi, così come nei Paesi baltici, la resilienza emerge come il risultato di politiche di lungo periodo, sostenute da continuità istituzionale, memoria organizzativa e coinvolgimento della società. Non si tratta di modelli costruiti in risposta a una crisi contingente, ma di architetture sviluppate nel tempo, spesso in assenza di urgenza immediata.

Per l'Italia, le vulnerabilità nel dominio cognitivo e nella preparazione civile pongono una sfida che difficilmente può essere affrontata entro i limiti di un singolo ciclo politico. Si tratta di ambiti che richiedono investimenti continuativi, coordinamento interistituzionale e la costruzione di una cultura della sicurezza condivisa.

In ultima analisi, il fattore decisivo non è rappresentato dalle risorse disponibili, ma dal tempo. I modelli che oggi appaiono più efficaci sono il risultato di decisioni assunte molti anni prima. La questione, per l'Italia, non è quindi se adattarsi, ma quando iniziare a farlo. In questo senso, la vera vulnerabilità non è l'assenza di strumenti, ma il ritardo nell'attivare un percorso coerente di lungo periodo. ■

Bibliografia

Libri, articoli e report accademici

Flanagan, Samuel J., Jan Osburg, Anika Binnendijk, Marta Kepe, and Andrew Radin. *Deterring Russian Aggression in the Baltic States Through Resilience and Resistance*. Santa Monica, CA: RAND Corporation, 2019.

Lebedeva, L., D. Shkuropadska, J. Gonçalves, I. Shtunder, T. Ozhelevskaya, and Y. Yasko. "Resilience of the Bucharest Nine Countries in the Context of Global Turbulence." *International Journal of Economics and Financial Issues* 15, no. 6 (2025): 630–643. <https://doi.org/10.32479/ijefi.19276>.

Saxi, Håkon Lunde. "Alignment but Not Alliance: Nordic Operational Military Cooperation." *Arctic Review on Law and Politics* 13 (2022): 53–71. <https://doi.org/10.23865/arctic.v13.3380>.

Skierka, Isabel. "When Shutdown Is No Option: Identifying the Notion of the Digital Government Continuity Paradox in Estonia's eID Crisis." *Government Information Quarterly* 40, no. 1 (2023): 101781. <https://doi.org/10.1016/j.giq.2022.101781>.

Snyder, Glenn H. "The Security Dilemma in Alliance Politics." In *Theory and Analysis of International Politics*. Bologna: Il Mulino, 1986.

Vuorelma, Johanna. "An Existential Threat in the North: Ontological Insecurity and the Nordic Path to NATO." *Cooperation and Conflict* 60, no. 4 (2025): 727–751. <https://doi.org/10.1177/00108367251372862>.

Fonti istituzionali

European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). *Reports*. Helsinki, 2018–2024.

European Commission. *Resilience Dashboards (Spring 2024)*. Brussels: European Commission, 2024.

Finnish National Emergency Supply Agency. *Security Strategy for Society*. Helsinki, 2017.

Nordic Defence Cooperation (NORDEF). *Annual Reports*. 2018–2022.

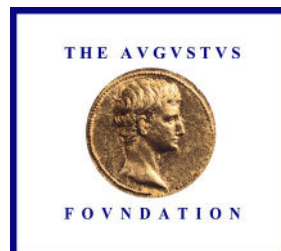
NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). *Annual Reports*. Tallinn, 2018–2024.

Swedish Civil Contingencies Agency (MSB). *Psychological Defence and Civil Preparedness Materials*. Stockholm, 2018–2024. <https://www.msb.se>.



**La Fondazione Machiavelli
dal 2017 si occupa di promuovere politiche
improntate ai valori tradizionali
e finalizzate a costruire un'Italia prospera e forte.**

www.centromachiavelli.com



La presente pubblicazione è stata realizzata
col contributo della Augustus Foundation