Cos'è la guerra ibrida – e sta già succedendo?

È il modo di fare guerra restando sotto la soglia del conflitto aperto: sabotaggi, droni, cavi tagliati, disinformazione. E in Europa è già in corso.

Dietro il nome vago c'è un metodo preciso. Un attacco ibrido combina strumenti diversi – sabotaggio, operazioni informatiche, disinformazione, pressione su energia e migranti – e li dosa in modo che nessun singolo episodio giustifichi una risposta militare. Chi lo subisce deve chiedersi ogni volta se ha davanti un incidente, un criminale comune o uno stato. Quel dubbio è il prodotto principale: finché regge, l'aggressore colpisce senza pagare il prezzo di una guerra.

Che cosa è già successo

L'Istituto internazionale di studi strategici (IISS) ha contato gli attacchi russi alle infrastrutture critiche europee: tra il 2023 e il 2024 sono cresciuti del 246%. Il 2025 ha allungato la serie, e conviene leggerla per ambiente, come fanno gli stati maggiori.

Nei cieli: tra il 2024 e l'inizio del 2026 circa 144 incursioni sospette di droni hanno interferito con l'aviazione civile del continente, arrivando a chiudere grandi aeroporti; Monaco di Baviera ha sospeso i voli due volte nella stessa notte, tra il 2 e il 3 ottobre 2025. Le autorità tedesche hanno registrato oltre mille avvistamenti sospetti nel solo 2025, molti sopra basi militari e fabbriche di armamenti, e l'Insikt Group ha contato trenta violazioni dello spazio aereo NATO tra il settembre 2025 e il gennaio 2026.

Sott'acqua: nell'autunno 2023 un'ancora ha danneggiato il gasdotto Balticconnector tra Finlandia ed Estonia; nel 2024 è toccato al cavo dati C-Lion1 (Finlandia–Germania) e al cavo elettrico EstLink 2. Le tracce portano ripetutamente a petroliere della «flotta ombra» russa che trascinano l'ancora sul fondale; un equipaggio è stato fermato dai finlandesi mentre si posizionava per tagliare altri cavi.

A terra: nel giugno 2025 un incendio doloso ha distrutto camion militari della Rheinmetall a Erfurt; nel dicembre 2025 una rete legata all'intelligence militare russa è stata accusata di un tentato attacco alla rete elettrica polacca.

La campagna ha anche una preistoria. Nel 2014 due esplosioni distrussero un deposito di munizioni a Vrbětice, in Cechia, uccidendo due persone; l'attribuzione al GRU, l'intelligence militare russa, arrivò solo nel 2021. Sette anni per dire con certezza chi è stato: la guerra ibrida vive esattamente in quello spazio.

Manodopera a poche migliaia di euro

Gli esecutori materiali vengono sempre più spesso reclutati online, di solito su Telegram, per poche migliaia di euro: piccoli criminali senza alcun legame visibile con Mosca. A Praga un uomo ingaggiato in rete per incendiare degli autobus è stato condannato nel 2024 a diversi anni di carcere; le indagini in Polonia, Germania e Lituania hanno trovato cellule che si sovrapponevano, riconducibili alla stessa intelligence militare russa. Per il mandante il conto torna: un incendio costa quanto un'utilitaria usata, e tra l'arresto dell'esecutore e la prova della regia possono passare anni.

A che cosa serve

Gli obiettivi si leggono nella scelta dei bersagli. Misurare i riflessi europei e la velocità con cui 32 governi si mettono d'accordo. Alzare il costo del sostegno all'Ucraina e abituare le opinioni pubbliche all'idea che opporsi a Mosca porta guai in casa. Soprattutto, saggiare le cuciture dell'alleanza: ogni episodio, preso da solo, è troppo piccolo per una risposta comune, e la somma diventa una campagna solo se qualcuno mette insieme i pezzi. Negli scenari studiati in Occidente questa pressione è la fase preparatoria di un eventuale attacco vero e proprio: il terreno su cui si misura, in anticipo, se l'alleanza reagisce unita.

La parte italiana corre sul fondo del mare

L'Italia importa oltre il 95% del gas che consuma, e in gran parte le arriva da condotte posate sul fondo: dall'Algeria, oggi primo fornitore, attraverso il Canale di Sicilia, e dall'Azerbaigian fino alla costa pugliese. Negli stessi tratti di Mediterraneo corrono i cavi che collegano l'Europa all'Asia e all'Africa: quasi tutto il traffico internet intercontinentale viaggia sott'acqua, e la Sicilia è uno dei suoi snodi. Un'ancora trascinata funziona nel Canale di Sicilia come nel Golfo di Finlandia.

Qualcosa è già in piedi: dal dicembre 2023 opera alla Spezia il Polo nazionale della dimensione subacquea, accanto al centro di ricerca marittima della NATO, per sorvegliare e proteggere fondali, cavi e condotte, e la marina pattuglia stabilmente le rotte energetiche tra Mediterraneo e Mar Rosso. È la versione mediterranea dello stesso lavoro che le marine nordiche fanno nel Baltico.

Le risposte, finora

Qualche soglia ha cominciato a farsi rispettare. Nel settembre 2025, per la prima volta, caccia alleati hanno abbattuto droni russi sopra la Polonia; quella notte, e i rinforzi arrivati con l'operazione Eastern Sentry, sono ricostruiti nella pagina sull'articolo 5. Dopo i cavi tagliati, la NATO ha lanciato Baltic Sentry, un pattugliamento navale permanente del Baltico; la Germania ha aperto a Berlino un centro comune di difesa anti-drone. E l'alleanza ha messo a verbale che anche un attacco informatico o ibrido può far scattare la difesa collettiva, senza precisare dove passi la linea: stavolta l'ambiguità lavora per chi si difende.

Trentadue pezzi di cielo

Resta il punto strutturale. Una campagna ibrida punta alle giunture: scommette che ogni capitale tratti il proprio episodio come cronaca locale, che il drone danese resti un problema danese e il cavo finlandese un problema finlandese. Trentadue paesi che sorvegliano ciascuno il proprio pezzo di cielo e di mare sono il suo bersaglio ideale. Un pilastro europeo della NATO che guardasse quei trentadue pezzi come un cielo solo e un mare solo, dal Baltico al Canale di Sicilia, le toglierebbe ciò di cui vive: le cuciture. I droni li decide Mosca; le cuciture le decidono le capitali europee.

Tutte le domande →

DOMANDE FREQUENTI

Cosa si intende per guerra ibrida?
Una campagna che combina sabotaggi, attacchi informatici, disinformazione e pressioni economiche, calibrata per restare sotto la soglia che giustificherebbe una risposta militare. L'obiettivo è indebolire un paese mantenendo la negabilità: ogni episodio deve poter sembrare un incidente o un crimine comune.

Quali attacchi ibridi russi ci sono già stati in Europa?
Cavi e gasdotti danneggiati nel Baltico, droni che hanno chiuso grandi aeroporti, incendi dolosi contro impianti militari in Germania, un tentato attacco alla rete elettrica polacca, autobus incendiati a Praga. L'IISS calcola che gli attacchi russi alle infrastrutture critiche europee siano cresciuti del 246% tra il 2023 e il 2024.

Un attacco ibrido può far scattare l'articolo 5 della NATO?
Sì, in linea di principio: la NATO ha dichiarato che anche operazioni informatiche o ibride possono attivare la difesa collettiva, senza precisare dove passi la soglia. L'ambiguità è voluta: serve a impedire a Mosca di calcolare in anticipo fin dove può spingersi.

Chi esegue materialmente i sabotaggi in Europa?
Sempre più spesso manodopera reclutata online, anche su Telegram, per poche migliaia di euro: piccoli criminali senza legami visibili con Mosca. Le indagini in Polonia, Germania e Lituania hanno ricondotto queste cellule all'intelligence militare russa, la stessa indicata dalle autorità ceche per le esplosioni di Vrbětice del 2014.

L'Italia è esposta alla guerra ibrida?
Sì, soprattutto sott'acqua: importa oltre il 95% del gas, in gran parte da condotte sottomarine, e dalla Sicilia passano i cavi dati tra Europa, Asia e Africa. Per sorvegliare fondali e infrastrutture ha creato a fine 2023 il Polo nazionale della dimensione subacquea alla Spezia.

FONTI

- IISS, The Scale of Russian Sabotage Operations (2025): attacchi alle infrastrutture critiche europee +246% tra il 2023 e il 2024
- Recorded Future / Insikt Group: incursioni di droni 2024–2026; 30 violazioni dello spazio aereo NATO settembre 2025 – gennaio 2026; autorità tedesche, avvistamenti 2025
- Autorità finlandesi: indagini sui danneggiamenti di Balticconnector (2023), C-Lion1 ed EstLink 2 (2024) e sulla «flotta ombra»
- Indagini in Polonia, Germania, Lituania e Cechia sul reclutamento di sabotatori (2024–2025); attribuzione ceca di Vrbětice al GRU (2021)
- NATO: missioni Baltic Sentry ed Eastern Sentry (2025); dichiarazioni dei vertici su attacchi ibridi e articolo 5
- Marina Militare / Ministero della Difesa: Polo nazionale della dimensione subacquea, La Spezia (dicembre 2023)
- CIDOB / dati import gas 2023–2025: dipendenza italiana dalle importazioni, Algeria primo fornitore