La portata delle operazioni di sabotaggio russe contro le infrastrutture critiche europee

Charlie Edwards, Consulente senior, Strategia e sicurezza nazionale; Nate Seidenstein, Assistente di ricerca

Agosto 2025

IISS
Istituto internazionale per gli studi strategici

Indice

Copertina

Un aereo cargo della DHL per la consegna di pacchi è fermo all'aeroporto di Lipsia/Halle il 15 ottobre 2024 a Schkeuditz, in Germania. (Foto di Jens Schlueter/Getty Images)

Sintesi dell'

La Russia sta conducendo una guerra non convenzionale contro l'Europa. Attraverso la sua campagna di sabotaggio, vandalismo, spionaggio e azioni segrete, l'obiettivo della Russia è stato quello di destabilizzare i governi europei, minare il sostegno pubblico all'Ucraina imponendo costi sociali ed economici all'Europa e indebolire la capacità collettiva della NATO e dell'Unione Europea di rispondere all'aggressione russa. Questa guerra non convenzionale ha iniziato a intensificarsi nel 2022, in parallelo all'invasione russa dell'Ucraina. Sebbene la Russia non sia finora riuscita a raggiungere il suo obiettivo primario, le capitali europee hanno faticato a rispondere alle operazioni di sabotaggio russe e hanno trovato difficile concordare una risposta unitaria, coordinare le azioni, sviluppare misure di deterrenza efficaci e imporre costi sufficienti al Cremlino.

L'IISS ha creato il database open source più completo sulle operazioni di sabotaggio russe sospette e confermate che hanno preso di mira l'Europa. I dati rivelano che il sabotaggio russo ha preso di mira le infrastrutture critiche europee, è decentralizzato e, nonostante l'allarme lanciato dai funzionari europei della sicurezza e dell'intelligence, è rimasto in gran parte inalterato dalle risposte della NATO, dell'UE e degli Stati membri fino ad oggi. La Russia ha sfruttato le lacune dei sistemi giuridici attraverso il suo approccio di "gig economy", che le ha permesso di evitare attribuzioni e responsabilità. Dal 2022 e dall'espulsione di centinaia di suoi funzionari dei servizi di intelligence

Dalle capitali europee, la Russia è stata molto efficace nel reclutamento online di cittadini di paesi terzi per aggirare le misure di controspionaggio europee. Sebbene questa tattica si sia dimostrata efficace in termini di portata e volume, consentendo operazioni su larga scala, la sfida principale che i servizi segreti russi devono affrontare è stata la qualità dei propri agenti, spesso scarsamente addestrati o mal equipaggiati, il che rende le loro attività soggette a essere scoperte, interrotte o fallite.

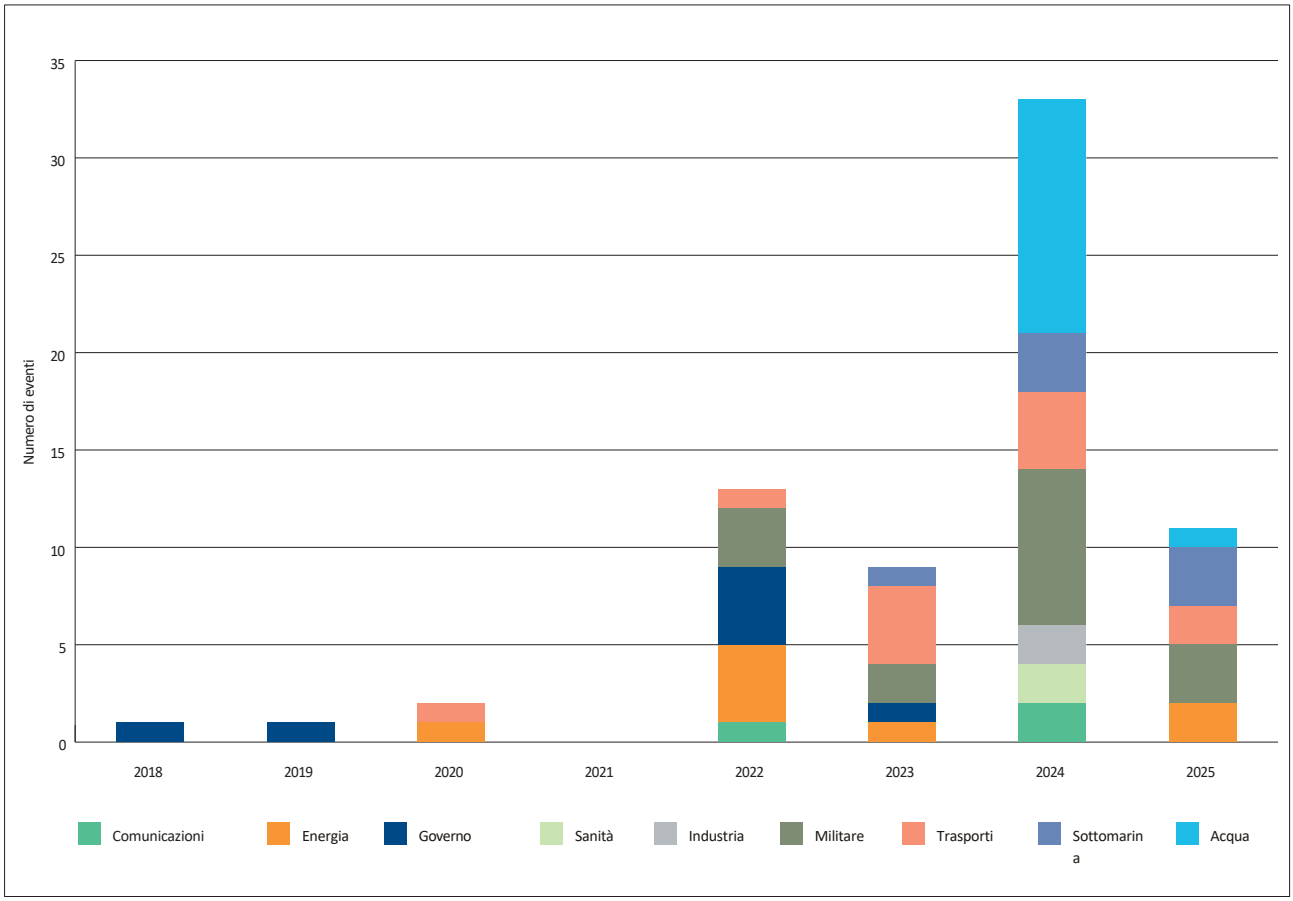
La dottrina militare russa integra profondamente il sabotaggio delle infrastrutture nazionali critiche (CNI) nella *gibrid-naya voyna* (guerra ibrida). Le infrastrutture critiche europee sono particolarmente vulnerabili al sabotaggio perché versano in pessime condizioni a seguito di decenni di manutenzione differita e mancanza di investimenti da parte dei governi nazionali e del settore privato. La Russia ha preso di mira le infrastrutture critiche per ottenere un vantaggio strategico diretto nella sua guerra in Ucraina e nell'ambito del più ampio conflitto con l'Occidente. Sebbene alcune iniziative, come l'operazione marittima *Baltic Sentry* della NATO nel Mar Baltico, si siano rivelate in qualche modo efficaci, la mancanza di budget e risorse ha impedito alla NATO e all'UE di adottare una risposta a lungo termine e sostenuta. Inoltre, di fronte a priorità di sicurezza nazionale concorrenti, non è chiaro quanto le capitali europee siano impegnate a scoraggiare la guerra non convenzionale della Russia contro l'Europa.

Introduzione

Nell'ambito della guerra non convenzionale della Russia contro l'Europa, le operazioni di sabotaggio e la campagna di sovversione e disinformazione del Cremlino, insieme all'invasione su larga scala dell'Ucraina nel 2022, sono parte integrante della più ampia guerra ibrida volta a minare l'Occidente. Uno degli obiettivi primari della guerra non convenzionale della Russia contro l'Europa è quello di ridurre il sostegno all'Ucraina aumentando i costi per i governi e le industrie, molestando le popolazioni e sfruttando le vulnerabilità delle difese europee. [1]Anche l'Ucraina si è impegnata attivamente in operazioni cibernetiche e con droni contro le infrastrutture petrolifere e del gas russe e gli impianti dell'industria della difesa, sfruttando le vulnerabilità persistenti. Queste operazioni di ritorsione mirano a imporre costi, interrompere le operazioni e influenzare la volontà pubblica di entrambe le parti, caratterizzando una contesa più ampia e globale.

Alcuni Stati membri della NATO hanno valutato che la guerra non convenzionale della Russia faccia parte dei suoi preparativi a lungo termine per un potenziale confronto militare con la NATO.[2] Ritengono che l'attenzione sia concentrata sull'attacco a obiettivi fisici e virtuali mediante spionaggio, sovversione, ransomware e abuso delle catene di approvvigionamento IT globali, nonché su operazioni informative che utilizzano campagne di disinformazione su larga scala, propaganda e diffusione di deepfake e teorie cospirative.[3] Questi vettori di attacco si intersecano nei metodi e negli effetti, integrando le capacità di vari settori dell'esercito russo, dei servizi di intelligence e di attori non statali (tra cui il Gruppo Wagner e criminali).

Figura 0.1: **Frequenza delle attività di guerra ibrida russe in Europa, gennaio 2018-giugno 2025**



Note: Tutti gli attacchi ibridi nel 2022 sono avvenuti dopo l'inizio dell'invasione su larga scala dell'Ucraina da parte della Russia. Le categorie Energia e Comunicazioni escludono i tentativi russi di sabotare cavi sottomarini e condutture; tali azioni sono conteggiate nella categoria Sottomarina.
Fonti: analisi IISS; Armed Conflict Location & Event Data Project (ACLED), www.acleddata.com; Bart Schuurman, "Russian Operations Against Europe Dataset", https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/TQ0FMQ

Mentre molta attenzione è stata dedicata alle operazioni informatiche e alle campagne di disinformazione russe, molto meno è stato scritto sul sistematico attacco del Cremlino alle infrastrutture critiche europee (ECI). Il targeting delle ECI deriva dalla dottrina militare russa di lunga data[4] e si ispira ai piani dell'era sovietica che si concentravano sui sistemi di approvvigionamento energetico, come le centrali elettriche, i sistemi di approvvigionamento di combustibile, gli oleodotti e le raffinerie.[5] Negli ultimi dieci anni, il Cremlino ha preso di mira l'energia, i trasporti, le banche, le infrastrutture dei mercati finanziari, la sanità, l'acqua, le infrastrutture digitali e le strutture governative (comprese le installazioni militari).[6]

Più recentemente, le operazioni di sabotaggio russe in Europa hanno ampliato la gamma di obiettivi e la gravità degli attacchi. Il numero di attacchi è quasi quadruplicato dal 2023 al 2024 (vedi Figura 1). I dati dell'IISS mostrano che gli obiettivi ECI più frequenti sono le strutture legate alla guerra in Ucraina e le strutture governative.[7] La Russia prende di mira basi, impianti di produzione e strutture coinvolte nel trasporto di aiuti militari all'Ucraina.

Questo rapporto si basa su un dataset straordinariamente dettagliato raccolto dall'IISS, costruito sul lavoro fondamentale del professor Bart Schuurman, docente di Terrorismo e Violenza Politica all'Università di Leida nei Paesi Bassi, e notevolmente ampliato grazie all'integrazione con l'Armed Conflict Location & Event Data Project e al monitoraggio degli incidenti effettuato dall'IISS stesso. Il risultato è la banca dati open source più completa attualmente disponibile sulle operazioni di sabotaggio russe in Europa e nelle zone limitrofe. Essa copre l'intera gamma di attività con effetti fisici: dal sabotaggio dei cavi sottomarini al blocco dei segnali GPS in diversi ambiti e aree geografiche.

Il set di dati ci ha permesso di identificare alcuni modelli ricorrenti nella campagna russa. Tuttavia, riconoscendo l'incertezza intrinseca nell'attribuzione di attività segrete, ogni incidente è stato valutato utilizzando un sistema di affidabilità a più livelli, in linea con le migliori pratiche [8].Nei casi in cui l'attribuzione era ambigua, l'obiettivo era quello di distinguere tra ciò che era noto, ciò che era ritenuto probabile e ciò che presentava un'incertezza significativa. Ciò è stato particolarmente difficile quando c'è stato un notevole intervallo di tempo tra gli eventi sottostanti, il completamento di indagini lunghe e complesse e i procedimenti giudiziari. Le prove e le informazioni di intelligence spesso emergono in modo incrementale, il che ha richiesto un'attenta valutazione e una conferma da parte di più fonti indipendenti.

Le decisioni relative all'attribuzione di responsabilità raramente vengono prese in un vuoto politico. Probabilmente i governi europei avranno valutato i pro e i contro di una "divulgazione pubblica" e potrebbero decidere che il rischio non vale la pena. Tra i motivi vi sono il timore di un'escalation, la necessità di mantenere uno spazio diplomatico per futuri negoziati, la protezione delle fonti e dei metodi e la volontà di evitare il panico pubblico. Potrebbe anche essere, a seguito dell'espulsione di centinaia di membri dei servizi segreti russi (RIS) nel 2022, a causa della mancanza di alternative. Di conseguenza, qualsiasi attribuzione ufficiale di un atto ostile da parte di uno Stato potrebbe essere in ritardo rispetto alle valutazioni sensibili dei servizi segreti, mentre le dichiarazioni rese pubbliche riflettono calcoli strategici più ampi tanto quanto la loro fiducia nelle prove.

La guerra non convenzionale della Russia contro l'Europa pone sfide politiche significative ai governi occidentali. La dottrina russa confonde intenzionalmente i confini tra guerra e pace, rendendo difficile per i governi europei individuare e rispondere a tale aggressione. La risposta della NATO e dell'UE è stata quella di definire la guerra non convenzionale della Russia come operazioni nella "zona grigia", al di sotto della soglia della guerra convenzionale. Tuttavia, il concetto di zona grigia, pur descrivendo attività ostili al di sotto della soglia del conflitto diretto tra Stati, ha ormai esaurito la sua utilità: troppo spesso serve oggi come scudo burocratico che consente ai governi di evitare azioni decisive e responsabilità.

Anziché chiarire la minaccia, il concetto di zona grigia ha seminato confusione sui mandati e sulla responsabilità, rendendo ancora più sfocati i confini tra sicurezza nazionale, diplomazia e applicazione della legge. Questa frammentazione delle responsabilità ha ostacolato l'emergere di una risposta unitaria e strategica; al contrario, i governi ricorrono spesso a misure difensive e reattive, raddoppiando la protezione anziché adottare le misure proattive e assertive necessarie per scoraggiare e contrastare l'attività russa. La tendenza a trattare ogni incidente in modo isolato, piuttosto che come parte di una più ampia campagna del Cremlino, ha aggravato il problema e contribuito alla mancanza di un'azione coerente e globale da parte del governo. Si stima che le operazioni di sabotaggio russe abbiano causato centinaia di milioni di euro di danni materiali (a cavi sottomarini, oleodotti, infrastrutture di trasporto, ecc.) e, in una certa misura, danni psicologici.

Mappa 0.1: **Metodi utilizzati dalla Russia nella guerra ibrida in Europa, gennaio 2018-giugno 2025**

Nota: le categorie Energia e Comunicazioni escludono i tentativi russi di sabotare cavi sottomarini e oleodotti; tali azioni sono conteggiate nella categoria Sottomarino.
Fonti: analisi IISS; Armed Conflict Location & Event Data Project (ACLED), www.acleddata.com; Bart Schuurman, "Russian Operations Against Europe Dataset", https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/TQ0FMQ

– alimentando l'ansia sociale, indebolendo la fiducia dell'opinione pubblica ed esacerbando le divisioni politiche – non hanno ancora avuto conseguenze catastrofiche. Non sono stati confermati decessi di civili direttamente collegati alle operazioni di sabotaggio russe in Europa dall'invasione del 2022.

Sarebbe tuttavia errato sottovalutare la gravità della minaccia sulla base del numero di vittime civili, anche se questo è un fattore determinante per i governi nel decidere azione. Il modello di attività in continua evoluzione indica uno sforzo deliberato da parte del Cremlino e del RIS per aumentare la pressione e l'incertezza. L'assenza di vittime di massa non implica l'assenza di intenzioni o capacità. Piuttosto, riflette una strategia volta a intimidire, destabilizzare e mettere alla prova la determinazione dei governi europei in modo accuratamente calibrato per evitare di superare la soglia che innescherebbe una forte risposta di ritorsione. Tuttavia

Il margine di escalation è ridotto: una singola falla nella sicurezza potrebbe causare vittime. Un piccolo numero di incidenti isolati, in particolare il tentato omicidio dell'amministratore delegato di Rheinmetall Armin Papperger, indicano un atteggiamento più aggressivo. L'attacco a Papperger, e potenzialmente ad altre figure dell'industria della difesa, segnala l'intenzione della Russia di colpire individui legati al sostegno militare occidentale all'Ucraina, con l'obiettivo di destabilizzare la base industriale della difesa che sostiene Kiev.

L'impatto cumulativo degli attacchi russi su obiettivi fisici, su obiettivi virtuali e tramite operazioni informative è stato quello di minare la resilienza occidentale e dividere le società europee. L'effetto è stato anche quello di abbassare la soglia per una futura escalation e aumentare il rischio di errori di valutazione strategica da entrambe le parti.

Il rapporto è suddiviso in tre sezioni. La sezione 1 identifica le vulnerabilità e le dipendenze sistemiche che espongono le infrastrutture critiche europee alle operazioni di sabotaggio russe, sottolineando in particolare l'invecchiamento delle infrastrutture, i rischi legati alla proprietà del settore privato e la fragilità dei sistemi interconnessi e interdipendenti. La sezione 2 esplora l'integrazione da parte della Russia del sabotaggio delle infrastrutture nella sua più ampia strategia di guerra ibrida, descrivendo in dettaglio i metodi in evoluzione utilizzati dai servizi segreti russi, compreso l'uso di agenti remoti e tattiche di sabotaggio a bassa tecnologia progettate per eludere la deterrenza. La sezione 3 affronta la sfida strategica che i governi europei devono affrontare per rispondere efficacemente alla campagna di Mosca in Europa. Sebbene i membri della NATO e dell'UE abbiano compiuto progressi nel riconoscere e mitigare queste minacce, le risposte rimangono prevalentemente reattive, frammentarie e ostacolate da soglie chiare per rispondere all'aggressione russa. Il rapporto si conclude con le implicazioni strategiche della campagna di sabotaggio della Russia, sottolineando l'urgente necessità di una posizione più assertiva e proattiva per contrastare l'aggressione russa e salvaguardare la sicurezza europea.

1. La vulnerabilità delle infrastrutture critiche europee

L'ECI è vulnerabile al sabotaggio a causa di una combinazione di debolezze sistemiche intrinseche e di un panorama delle minacce sempre più complesso. Le economie e le società moderne, guidate dall'efficienza e dal ritmo sempre crescente della globalizzazione, hanno creato sistemi sempre più interdipendenti in cui singole interruzioni possono avere effetti di vasta portata. Ad esempio, il blackout europeo del novembre 2006 si è verificato quando una linea di trasmissione ad alta tensione è stata deliberatamente interrotta nella Germania settentrionale, causando il sovraccarico e lo spegnimento dell'intero sistema. In pochi secondi il guasto si è propagato oltre i confini nazionali, raggiungendo persino la Tunisia [9].

I responsabili politici della NATO e dell'UE hanno sottolineato le significative preoccupazioni attuali relative alla resilienza delle infrastrutture critiche europee. In primo luogo, negli ultimi decenni si è registrata una significativa carenza di investimenti nelle ECI. L'età media delle infrastrutture della rete elettrica è di circa 40 anni, il che significa che circa il 60% degli investimenti totali dell'UE nella rete dovrà essere destinato al potenziamento delle reti di distribuzione di base [10]. Le reti di trasporto sono tra le infrastrutture critiche più vecchie d'Europa. Le ferrovie europee sono particolarmente vulnerabili e costituiscono obiettivi privilegiati per atti di sabotaggio, dato il loro ruolo critico nella logistica militare della NATO. La natura delle ferrovie fa sì che un singolo guasto in un sistema possa bloccare il traffico su migliaia di chilometri. L'Alleanza riconosce che una deterrenza e una difesa credibili dipendono da un'adeguata capacità logistica, non da ultimo sul suo fianco orientale.[11] In alcuni casi, il RIS ha utilizzato criminali locali per spiare la logistica della NATO. In Polonia, bielorussi, polacchi e ucraini sono stati incaricati di monitorare il flusso di aiuti militari all'Ucraina, utilizzando metodi quali l'installazione di telecamere lungo le linee ferroviarie. [12]

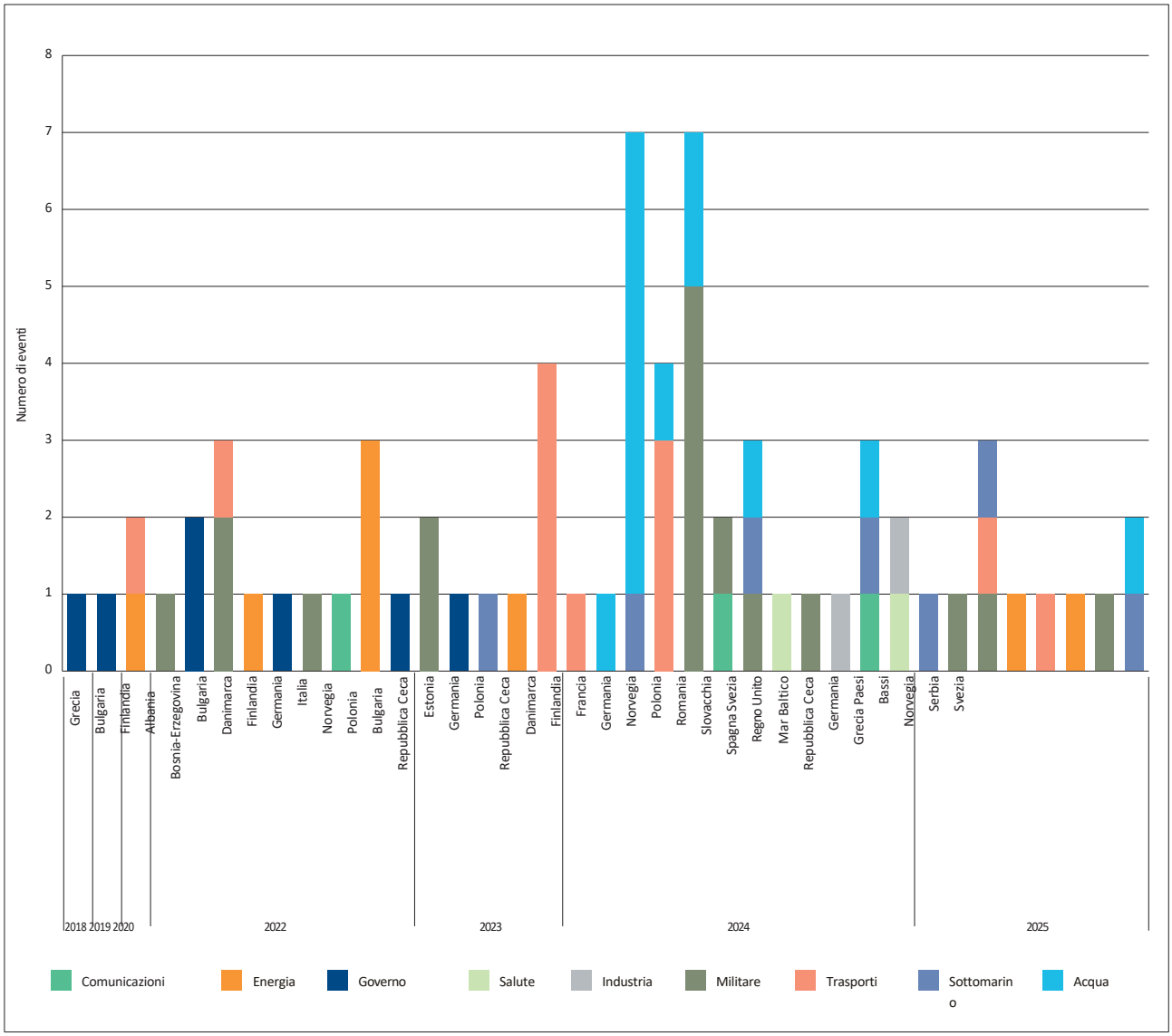
Anche i sistemi legacy presentano delle sfide: la Lituania continua a utilizzare il sistema di controllo delle locomotive ferroviarie KLUB-U della Russia, che comporta gravi rischi per la sicurezza informatica e potenzialmente consente sabotaggi, sorveglianza o interruzioni da remoto [13].Il progetto di sostituzione del sistema dovrebbe protrarsi fino alla fine del 2027.

Una seconda preoccupazione è il continuo utilizzo di vecchi sistemi informatici e software obsoleti nell'ECI. Nel giugno 2024, il Consiglio consultivo olandese per gli Affari Internazionali (AIV) ha riscontrato che la gestione idraulica delle acque nei Paesi Bassi è gravemente obsoleta, poiché si basa su vecchi sistemi informatici collegati a reti digitali per il funzionamento a distanza, ma privi della sicurezza necessaria. Il sabotaggio di una diga causerebbe danni significativi in un paese che si trova per lo più sotto il livello del mare. Ad Haarlemmermeer, nell'Olanda Settentrionale, ad esempio, l'allagamento potrebbe raggiungere un metro di profondità, travolgendo molto rapidamente l'intera infrastruttura dell'aeroporto di Schiphol, comprese le autostrade e i collegamenti ferroviari.[14]

Una terza preoccupazione è che una parte significativa delle infrastrutture critiche è di proprietà privata o gestita da privati. Mentre la sicurezza e la resilienza sono sempre più motivazioni per gli investimenti, poiché gli assicuratori e gli azionisti spingono per la sicurezza aziendale, i modelli orientati al profitto danno priorità all'efficienza rispetto alla ridondanza, creando debolezze intrinseche. Circa il 90% dei trasporti militari della NATO utilizza mezzi civili; più della metà delle comunicazioni satellitari per scopi di difesa sono fornite dal settore commerciale; e il 75% del sostegno che le operazioni della NATO ricevono dai paesi ospitanti proviene da fonti commerciali locali.[15] La mancanza di un quadro normativo unico e armonizzato e le diverse norme nazionali in materia di protezione delle infrastrutture critiche nei paesi membri dell'UE e della NATO complicano gli sforzi volti a garantire livelli di sicurezza coerenti. Le limitazioni normative si concentrano spesso su risorse discrete piuttosto che su un approccio olistico e sistemico alla resilienza, rendendo difficile affrontare le questioni transfrontaliere e la complessa interazione dei rischi.

Infine, i responsabili politici sono sempre più preoccupati dalla vulnerabilità dei cavi sottomarini, data la forte dipendenza dell'economia europea da essi. I cavi trasmettono circa il 95% dei flussi di dati globali e sostengono transazioni finanziarie per un valore stimato di 10.000 miliardi di dollari al giorno, ma sono vulnerabili a causa della loro esposizione fisica, della loro importanza strategica, dell'ampia superficie di attacco e della ridotta ridondanza [16]. I cavi sottomarini sono particolarmente vulnerabili, con oltre il 70% degli incidenti annuali causati da danni accidentali ai cavi dovuti all'attività marittima commerciale [17].

Figura 1.1: **Attività di guerra ibrida russa per paese e anno, gennaio 2018-giugno 2025**



Note: Tutti gli attacchi ibridi nel 2022 sono avvenuti dopo l'inizio dell'invasione su larga scala dell'Ucraina da parte della Russia. Le categorie Energia e Comunicazioni escludono i tentativi russi di sabotare cavi sottomarini e condutture; tali azioni sono conteggiate nella categoria Sottomarino.
Fonti: analisi IISS; Armed Conflict Location & Event Data Project (ACLED), www.acleddata.com; Bart Schuurman, "Russian Operations Against Europe Dataset", https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/TQ0FMQ

Sebbene il panorama dell'ECI sia ampio e complesso, i dati dell'IISS suggeriscono che il sabotaggio e le operazioni segrete russe includono sia atti casuali di vandalismo (volti a seminare paura e discordia nella popolazione locale) sia attacchi mirati a specifici punti deboli all'interno dei sistemi. Quest'ultimo aspetto suggerisce un modello che si è ripetuto negli ultimi anni e che ha incluso il sabotaggio di linee ferroviarie ad alta velocità poche ore prima della cerimonia di apertura delle Olimpiadi di Parigi del 2024 [18]e l'arresto in Polonia di una rete di spionaggio che aveva installato telecamere lungo le linee ferroviarie, dove il blocco di una singola linea avrebbe potuto interrompere la logistica militare verso l'Ucraina [(19)].

il sabotaggio dei cavi sottomarini[20] che provoca guasti a catena a livello regionale; e il sabotaggio degli impianti di trattamento delle acque, come nell'agosto 2024, quando le autorità tedesche hanno temporaneamente chiuso una base militare tedesca vicino all'aeroporto di Colonia per indagare su un sospetto sabotaggio della sua rete idrica. L'incidente di Colonia è avvenuto poco dopo un altro sospetto sabotaggio dell'approvvigionamento idrico in una base NATO a Geilenkirchen, quartier generale degli aerei del sistema di allarme e controllo aereo della NATO e importante snodo di trasporto per i soldati ucraini addestrati in Germania [21].

2. La guerra non convenzionale della Russia contro l'Europa

Gibridnaya voyna descrive azioni aggressive e coercitive che fanno ampio uso di tutti gli strumenti dello Stato e degli attori non statali associati per ottenere il potere politico. In realtà, la guerra ibrida è un termine amorfo con un'ampia variabilità teorica nelle definizioni nei contesti accademici e politici, emerso per la prima volta intorno al 2005 per descrivere i conflitti insurrezionali in Medio Oriente, ma da allora adattato a una vasta gamma di contesti.[22]

Per il Cremlino, *gibridnaya voyna* è usato per descrivere quella che percepiscono come una guerra informativa condotta dall'Occidente contro la Russia e volta ad amplificare le divisioni sociali, politiche e ideologiche interne per indebolire il Paese dall'interno.[23] Il generale Valery Gerasimov, capo di Stato Maggiore delle forze armate russe, ha scritto nel 2016 che *la gibridnaya voyna* mira a "raggiungere obiettivi politici con un'influenza militare minima sul nemico ... minando il suo potenziale militare ed economico con pressioni informative e psicologiche, il sostegno attivo dell'opposizione interna e metodi partigiani e sovversivi".[24] Un esempio di questo approccio è la distruzione del più grande centro commerciale di Varsavia, Marywilska 44, a causa di un incendio nel maggio 2024, che i funzionari polacchi hanno pubblicamente collegato alla Russia, illustrando l'obiettivo di strutture commerciali civili con incendi dolosi.[25] Altri episodi di vandalismo suggeriscono un modello più ampio di attività ostili di basso livello e negabili.[26]

Quando descrivono l'approccio globale della Russia al conflitto, che integra mezzi militari e non militari, gli analisti russi preferiscono in genere termini come "guerra di nuova generazione" o "confronto informativo" piuttosto che *gibridnaya voyna*. Una caratteristica distintiva di questa strategia è il suo approccio globale, in cui tutte le attività, comprese le operazioni militari convenzionali, sono subordinate a una campagna informativa generale con l'obiettivo di plasmare la governance e l'orientamento geostrategico dello Stato bersaglio [27].

Gerasimov suggerisce un rapporto di 4:1 tra mezzi non militari e militari che impiegano ampiamente misure politiche, economiche, informative, umanitarie e altre misure non militari,[28] ma che in ultima analisi si basano sull'uso credibile della forza militare.[29] A differenza degli approcci occidentali, che spesso separano le operazioni informatiche da quelle di informazione, la dottrina russa considera le attività "tecnico-informatiche" e "psicologico-informatiche" come intrinsecamente integrate.[30]

Tuttavia, vale la pena notare che, mentre la dottrina russa delinea un approccio integrato e onnicomprensivo al conflitto, le agenzie di sicurezza e di intelligence europee percepiscono un divario tra questo quadro teorico e la sua attuazione pratica, spesso frammentaria, opportunistica e talvolta controproducente.[31]

Come dimostrano i dati dell'IISS, gli atti di sabotaggio confermati da parte della Russia nei confronti dell'ECI sono aumentati del 246% dal 2023 al 2024. Questa forte escalation è strettamente correlata alla revoca da parte dell'Occidente delle restrizioni sull'uso da parte dell'Ucraina di armi avanzate fornite dall'Occidente, in particolare sistemi a lungo raggio utilizzati per colpire all'interno della Russia [32].Nei primi cinque mesi del 2025, le informazioni disponibili al pubblico suggeriscono che si sono verificati 25 episodi di sabotaggio, spionaggio e vandalismo contro le infrastrutture militari della NATO. A maggio, la Germania ha sventato un complotto legato alla Russia che prevedeva l'invio di pacchi bomba contro le reti logistiche. Negli ultimi quattro mesi, la Svezia ha indagato su un sospetto sabotaggio che ha preso di mira oltre 30 torri di telecomunicazione lungo l'autostrada E22. Poiché le comunicazioni civili e militari della Svezia sono integrate, i danni alle reti in fibra ottica lungo le principali vie di comunicazione come la E22 potrebbero compromettere la sicurezza delle comunicazioni di difesa e delle infrastrutture di sorveglianza.

I sabotaggi russi, in particolare quelli contro infrastrutture critiche, non sono un fenomeno recente. Il Cremlino ha storicamente preso di mira i cavi sottomarini. Nell'ottobre 2015, le autorità statunitensi hanno monitorato le pattuglie sottomarine russe e la nave di superficie russa *Yantar* in un corridoio dell'Atlantico settentrionale che ospita un gruppo di cavi sottomarini. La nave da ricognizione di classe Project 22010 gestita dalla Marina russa trasportava sommergibili per acque profonde e attrezzature per il taglio dei cavi [33].

Più recentemente, alcuni degli attacchi più devastanti hanno comportato il trascinamento di ancore da parte della "flotta ombra" russa. La flotta ombra viaggia da e verso i porti di Primorsk e Ust-Luga su un gran numero di cavi sottomarini e infrastrutture sottomarine in uno stretto corridoio tra la Finlandia e l'Estonia e al di fuori del territorio di qualsiasi paese.

giurisdizione.[34] Nelle acque internazionali, lo Stato di bandiera ha l'obbligo di punire le navi che danneggiano i cavi, ma gli Stati lesi non hanno l'autorità per farlo.[35]

Tra i recenti episodi di sabotaggio russi nel Mar Baltico figurano quelli che hanno coinvolto *la Eagle S*, battente bandiera delle Isole Cook, che ha trascinato la sua ancora e tagliato il cavo sottomarino Estlink-2 nel Golfo di Finlandia, e la *Yi Peng 3*, battente bandiera cinese, sospettata di aver deliberatamente trascinato la sua ancora per tagliare il cavo C-Lion1 che collega la Finlandia e la Germania e il cavo Arelion che collega la Svezia e la Lituania.[36] La riparazione di un solo cavo o conduttura danneggiati costa decine di milioni di euro, senza contare il danno economico causato dalla perdita di capacità o i costi aggiuntivi per il controllo, le indagini e la difesa del dominio marittimo. [37]

Nel febbraio 2022, gli Stati membri della NATO hanno iniziato a espellere centinaia di funzionari russi come ritorsione per l'invasione su larga scala dell'Ucraina da parte della Russia. Dei 600 espulsi dall'Europa nel 2022, circa 400 provenivano dal RIS.[38] Questa serie di espulsioni ha fatto seguito a un processo simile in seguito al tentativo della Russia di assassinare Sergei Skripal nel 2018 nel Regno Unito, quando "150 agenti dei servizi segreti russi [sono stati] espulsi principalmente dai paesi occidentali".[39]

Le espulsioni su larga scala hanno ridotto significativamente il numero di agenti dei servizi segreti russi esperti sul campo e hanno ridotto le capacità operative fisiche dei servizi speciali russi nei paesi europei. Hanno inoltre compromesso l'apparato di supporto attraverso il quale la Russia conduce tradizionalmente molte delle sue operazioni. In risposta, il Cremlino ha adottato un nuovo approccio di "gig economy" al sabotaggio nelle sue operazioni in termini di reclutamento, direzione, costi e portata.[40] Ciò ha consentito al RIS di reclutare personale in modo ampio e flessibile, offrendo al contempo una direzione operativa limitata e gestendo le proprie risorse a distanza. Sebbene questa tattica abbia consentito operazioni su larga scala, la sfida principale affrontata dal RIS è stata la qualità delle persone reclutate, spesso scarsamente addestrate o mal equipaggiate, il che ha reso le loro attività soggette a individuazione, interruzione o fallimento.

Il lavoro operativo è guidato dall'intelligence militare russa, l'unità GRU 29155.[41] Quella che era iniziata come una campagna per destabilizzare l'Ucraina si è evoluta in una più ampia e crescente "guerra nell'ombra" contro l'Occidente.[42] Gli agenti russi pubblicano annunci nei forum dedicati al lavoro, in particolare sull'app di social networking Telegram con sede a Dubai, rivolgendosi alle comunità di immigrati dell'Europa orientale. Gli agenti dei servizi segreti russi assegnano poi compiti che vanno dall'affissione di manifesti di propaganda filo-russa o piccoli atti di vandalismo al sabotaggio dell'ECI.[43] Il GRU ha anche ricostruito le proprie capacità prendendo di mira, tra gli altri, studenti stranieri ed elementi all'interno della comunità russa in esilio.

Questo approccio alla sabotaggio basato sulla gig economy ha avuto successo perché le vulnerabilità associate all'ECI richiedono sforzi di sabotaggio relativamente poco sofisticati. Mentre le informazioni ottenute con mezzi tradizionali, come quelle raccolte dagli agenti dei servizi segreti tramite informatori, forniscono probabilmente indicazioni ai cittadini stranieri, la maggior parte degli attacchi richiede una sofisticazione tecnica minima, come nel caso degli incendi dolosi. Ciò ha permesso alla Russia di operare senza ostacoli e in parte senza essere individuata. Il sostanziale aumento degli atti di vandalismo è un indicatore della prevalenza dell'approccio basato sull'economia dei lavori occasionali. I dati dell'IISS mostrano che il vandalismo russo è aumentato ogni anno dal 2021, con otto incidenti significativi segnalati nel 2024 [44]. Le sanzioni penali, laddove esistono, non hanno limitato la capacità operativa della Russia, poiché i suoi agenti possono essere sostituiti. Se i meccanismi legali non sono in grado di ritenere la Russia direttamente responsabile e di creare un deterrente contro le azioni maligne, allora gli Stati devono perseguire altre forme di deterrenza e prevenzione.

Legislazioni come il National Security Act 2023 del Regno Unito, che impone sanzioni per chi collabora con servizi segreti stranieri paragonabili a quelle previste per i reati di terrorismo, possono dissuadere alcune persone dall'accettare offerte di sabotaggio da parte della Russia, ma sono ben lungi dall'essere una soluzione completa e difficilmente riusciranno a scoraggiare il sabotaggio in generale. Anche nei casi più eclatanti di spionaggio russo, gli agenti dei servizi segreti rimangono intoccabili.[45]

Le operazioni di sabotaggio russe in Europa hanno subito un'accelerazione, aumentando sia in frequenza che in audacia degli attacchi fisici. È altamente probabile che, nel luglio 2024, il GRU abbia tentato di colpire aerei cargo inserendo una sostanza infiammabile a base di magnesio in massaggiatori elettrici. Questi dispositivi sono esplosi nei centri logistici DHL in Germania, Polonia e Regno Unito e sono stati dei test per potenziali attacchi futuri contro aerei cargo.[46] Circa 40 complotti incendiari sono stati collegati alla Russia in Germania e Polonia, compresa la distruzione del centro commerciale di Varsavia. Nel maggio 2024, un grave incendio è scoppiato a Berlino in una fabbrica del gruppo Diehl, che produce missili terra-aria IRIS-T utilizzati in Ucraina. La Russia è stata anche collegata a un'esplosione in un magazzino in Spagna che immagazzinava apparecchiature di comunicazione per l'Ucraina. [47]

3. La risposta dell'Europa alle operazioni di sabotaggio russe

Le operazioni di sabotaggio russe in Europa sono proseguite fino al 2025, anche se i dati dell'IISS suggeriscono una pausa in tali attività durante la prima metà dell'anno. Sebbene gli attacchi segnalati sembrino essere diminuiti tra gennaio e luglio, diversi fattori possono spiegare questo fenomeno. In primo luogo, alcuni incidenti avvenuti all'inizio del 2025 potrebbero non essere ancora stati confermati dalle autorità locali e le forze dell'ordine e le agenzie di intelligence spesso impiegano tempo per raccogliere le prove, creando un ritardo nei dati. In secondo luogo, è possibile che l'inizio del secondo mandato del presidente degli Stati Uniti Donald Trump abbia spinto il Cremlino a sospendere temporaneamente le operazioni per evitare di alienarsi un'amministrazione statunitense più conciliante. Infine, la risposta guidata dagli Stati Uniti all'incidente DHL del 2024 potrebbe aver indotto il Cremlino a fare una pausa e aver portato il RIS a frenare le proprie operazioni. [48]

I governi europei hanno lanciato una serie di iniziative quest'anno. Nel marzo 2025, Estonia, Lettonia, Lituania e Polonia si sono ritirate dalla Convenzione di Ottawa che vieta le mine antiuomo, citando un "fondamentale deterioramento della situazione della sicurezza" nella regione baltica [49].Il 1° aprile, la Finlandia ha seguito l'esempio. Un tale cambiamento segnala probabilmente una maggiore prontezza militare al Cremlino, che mira ad evitare un confronto militare diretto con la NATO. In ambito marittimo, nel 2025 è stata avviata *l'operazione NorthSeal*, un'iniziativa congiunta di sicurezza nel Mare del Nord, insieme all'operazione *Baltic Sentry.*

Ma ci sono anche motivi per essere cauti nell'interpretare l'assenza di attività di sabotaggio come una tregua apparente. È possibile che, a seguito di una serie di arresti e di interventi da parte delle forze dell'ordine europee nel 2024 e nel 2025, il RIS stia riorganizzando le proprie reti, ricalibrando le proprie tattiche o evitando di essere individuato. Il reclutamento segreto da parte dei RIS tramite Telegram è continuato[50] e prende di mira cittadini di paesi terzi, in particolare nelle comunità di migranti dell'Europa orientale. La tendenza a sottostimare i dati rimane significativa, dato che il sabotaggio può essere inizialmente scambiato per un guasto tecnico o un incidente. Le speculazioni dei media possono anche creare ansia nell'opinione pubblica suggerendo un coinvolgimento maligno della Russia, come si è visto dopo l'incendio della sottostazione elettrica del marzo 2025 che ha causato la chiusura dell'aeroporto di Heathrow nel Regno Unito [51].Eventi come questo inoltre rischiando di assorbire il tempo della polizia e dei servizi di sicurezza, distogliendoli da altri incidenti reali e potenziali. In questo caso, i funzionari britannici hanno adottato un atteggiamento cauto, suggerendo che, sebbene non vi fossero indicazioni di atti illeciti, avrebbero mantenuto una posizione aperta.

Ma mantenere operazioni di sicurezza ad alto ritmo in un ambiente conteso richiede molte risorse ed è difficile da sostenere, il che spinge a cercare soluzioni più convenienti e durature. Meno di sei mesi dopo l'inizio dell'operazione *Baltic Sentry*, Jean Charles Ellermann-Kingombe, assistente segretario generale della NATO per l'innovazione, l'ibrido e il cyber, ha affermato che l'operazione, sebbene cruciale, era diventata proibitiva dal punto di vista dei costi.[52] Ha suggerito che i sistemi senza equipaggio, come il Saildrone *Voyager*, un veicolo di superficie senza equipaggio attualmente in fase di collaudo in mare da parte della NATO nel Mar Baltico, offrono un'alternativa più sostenibile per la sicurezza a lungo termine nella regione. Tuttavia, l'assenza di navi con equipaggio cambierà probabilmente i calcoli di deterrenza della Russia. Quando il segretario generale della NATO Mark Rutte ha annunciato *Baltic Sentry*, ha affermato che l'obiettivo era "rafforzare la protezione delle infrastrutture critiche ... e potenziare la presenza militare della NATO nel Mar Baltico".[53] Rutte ha poi sottolineato l'importanza di un'applicazione rigorosa della legge, evidenziando come la Finlandia avesse dimostrato che era possibile agire con fermezza nel rispetto della legge con l'abbordaggio *dell'Eagle S* alla fine del 2024.

Il passaggio dalla forte presenza militare di *Baltic* Sentry a un approccio ridimensionato e semi-autonomo suggerisce che l'Europa preferisce dare priorità alla deterrenza attraverso la negazione piuttosto che alla deterrenza attraverso la punizione. Ciò riflette una tendenza nella politica della NATO e dell'UE a dare priorità alla resilienza e allo sviluppo delle capacità, in gran parte in risposta ai fallimenti infrastrutturali e per ragioni economiche. [54]

Il tardivo riconoscimento da parte della NATO dell'importanza di proteggere le infrastrutture critiche nel 2016 ha fatto seguito all'invasione russa dell'Ucraina nel 2014. L'Alleanza ha stabilito sette requisiti di base per la preparazione civile e ha concordato di perseguirli, pur accettando che la preparazione civile fosse principalmente una questione nazionale.

responsabilità.[55] La NATO ha ulteriormente sviluppato il proprio approccio con il Concetto strategico adottato al vertice di Madrid nel giugno 2022, che ha riconosciuto la resilienza come fattore chiave per la deterrenza e la difesa; con la Dichiarazione congiunta sulla cooperazione UE-NATO del gennaio 2023; e con gli Obiettivi di resilienza dell'Alleanza definiti al vertice di Vilnius nel luglio 2023, che miravano a preparare l'Alleanza a «shock e perturbazioni strategici».[56]

La task force UE-NATO sulla resilienza delle infrastrutture critiche, lanciata nel gennaio 2023, aveva lo scopo di colmare le lacune tra le comunità militari, di intelligence e di polizia, condividendo le migliori pratiche e migliorando la consapevolezza della situazione. Il Concetto strategico dichiarava che la NATO avrebbe potuto considerare "una serie singola o cumulativa di attività informatiche dannose" o altri attacchi ibridi come fattore scatenante dell'articolo 5. Ma una tale politica non è credibile in assenza di un quadro coerente per identificare azioni incrementali o, cosa ancora più importante, della volontà politica di entrare in guerra senza una provocazione chiara e evidente [57].La Russia probabilmente ritiene che l'articolo 5 non verrebbe invocato in risposta alla maggior parte dei suoi sabotaggi opportunistici, il che la lascia impassibile.

Inoltre, interpretando erroneamente il calcolo strategico della Russia nella zona grigia, gli Stati occidentali sottovalutano la necessità della deterrenza attraverso la forza, indebolendola di conseguenza. La Russia si percepisce come impegnata in una lotta continua, esistenziale e irrisolvibile con l'Occidente. La Russia confonde i confini tra guerra e pace per raggiungere i propri obiettivi politici senza scatenare un conflitto convenzionale, in cui sa di essere in inferiorità rispetto alla NATO. I governi europei hanno in gran parte deciso di non essere "in guerra", che le attività della Russia rimangono nella zona grigia e che difficilmente raggiungeranno la soglia dell'articolo 5, senza un cambiamento sostanziale. L'Europa è stata riluttante a imporre costi sufficienti, spesso temendo un'escalation. [58]

Un esempio recente è illuminante a questo proposito. Il governo britannico ha recentemente intensificato gli sforzi per contrastare la flotta ombra russa, richiedendo sistematicamente la prova dell'assicurazione quando queste navi transitano nelle acque britanniche [59].Sebbene si tratti di uno sviluppo positivo, che fa seguito a un accordo con Danimarca, Estonia, Finlandia, Polonia e Svezia per aumentare il numero di controlli sull'assicurazione marittima, l'impatto pratico sembra limitato. Molti operatori navali rispondono in modo evasivo o ignorano del tutto le richieste. Solo una nave è stata sanzionata.[60] L'opacità della proprietà delle navi continua a ostacolare l'applicazione delle norme, il che suggerisce che ciò non sta scoraggiando le operazioni della flotta ombra.

La Russia opera al di sotto delle tradizionali soglie di deterrenza sia per scelta propria sia a causa dei fallimenti della politica europea. L'atteggiamento reattivo dell'Europa non è riuscito a infliggere sanzioni sufficienti [61].Nonostante le persistenti difficoltà, tuttavia, alcune contromisure europee hanno comportato dei costi. Tra queste vi è l'espulsione di diplomatici e agenti dei servizi segreti russi, che ha compromesso le reti e le infrastrutture dei servizi segreti russi. Gli sforzi di prevenzione, come le divulgazioni pubbliche senza precedenti dei servizi segreti statunitensi e britannici [62]prima dell'invasione russa dell'Ucraina nel 2022, hanno anticipato le operazioni sotto falsa bandiera russe e smorzato le narrazioni del Cremlino, dimostrando il valore strategico delle operazioni di informazione proattive.

Gli sforzi di deterrenza attraverso il diniego hanno rafforzato la resilienza. La sorveglianza sottomarina, la creazione della Cellula di coordinamento delle infrastrutture sottomarine critiche della NATO e i partenariati pubblico-privati per rafforzare le infrastrutture fisiche e informatiche hanno aumentato il costo del sabotaggio. Tuttavia, molti paesi della NATO non sono ancora in grado di replicare tali partenariati in modo indipendente. La resilienza da sola non ha scoraggiato la Russia, anche perché le operazioni di sabotaggio rimangono economiche ed efficaci nell'economia gig.

La cultura strategica europea limita ulteriormente l'efficacia della deterrenza. I sistemi giuridici e i valori democratici occidentali impongono limitazioni che gli avversari autoritari sfruttano all'esterno e possono ignorare all'interno dei propri confini. L'attribuzione della responsabilità rimane difficile. Sebbene le valutazioni dei servizi segreti occidentali concludano spesso con elevata certezza che la Russia è responsabile di sabotaggi, l'esitazione politica e giuridica spesso ritarda l'attribuzione pubblica della responsabilità, minando la deterrenza e segnalando al Cremlino che i costi in termini di reputazione saranno minimi. Nonostante gli alleati della Francia, tra cui Germania, Paesi Bassi, Regno Unito e Stati Uniti, abbiano una politica di attribuzione, la Francia ha in gran parte evitato di incolpare pubblicamente gli Stati sponsor.[63] Nel maggio 2025, tuttavia, il presidente Emmanuel Macron ha annunciato che la Francia avrebbe iniziato ad attribuire atti ostili in risposta alla crescente minaccia russa.[64]

Il sabotaggio dell'ECI da parte della Russia è fondamentale nella sua guerra non convenzionale contro l'Europa ed è progettato per indebolire la resilienza occidentale.

e unità. Ciò pone sfide politiche significative ai governi europei. La dottrina russa confonde intenzionalmente i confini tra guerra e pace, rendendo difficile per i governi europei individuare e rispondere a tali aggressioni. La risposta della NATO e dell'UE è stata quella di definire la guerra non convenzionale della Russia come operazioni nella zona grigia, al di sotto della soglia della guerra convenzionale. Tuttavia, il concetto di zona grigia, pur descrivendo attività ostili al di sotto della soglia della guerra diretta tra Stati

Il conflitto ha ormai esaurito la sua utilità: troppo spesso funge da scudo burocratico, consentendo ai governi di evitare azioni decisive e responsabilità. Come ha osservato lo storico militare Hew Strachan, una grave lacuna nel pensiero occidentale in materia di sicurezza risiede nella mancanza di chiarezza su ciò che costituisce la guerra, creando una pericolosa confusione. [65]Consentire al Cremlino di normalizzare il sabotaggio come strumento di politica statale rischia di provocare un'erosione strategica a lungo termine e un errore di valutazione che potrebbe trascinare l'Europa in un conflitto più profondo.

Note

1 Andrei Soldatov e Irina Borogan, "*Arsonist, Killer, Saboteur, Spy: While Trump Courts Him, Putin Is Escalating Russia's Hybrid War Against the West" (Piromane, assassino, sabotatore*, spia: *mentre Trump lo corteggia, Putin intensifica la guerra ibrida della Russia contro l'Occidente), Foreign Affairs*, 20 marzo 2025, https://www.foreignaffairs.com/russia/arsonist-killer-saboteur-spy-vladimir-putin-donald-trump.

2 Ufficio per la protezione della Costituzione, "Relazione annuale 2024", Repubblica di Lettonia, febbraio 2025, https://www.sab.gov.lv/files/uploads/2025/02/SAB-gada-parskats_2024_ENG.pdf.

3 Julia Voo e Virpratap Vikram Singh, "La dottrina russa del confronto informativo nella pratica (dal 2014 ad oggi): intenti, evoluzione e implicazioni", Istituto internazionale per gli studi strategici, giugno 2025, pagg. 8-10, https://www.iiss.org/globalassets/ media-library---content--migration/files/ research-papers/2025/06/russias-information--confrontation-doctrine--in-practice-/09-pub25-077-russia-information-confrontation-v5.pdf.

4 V. Roldugin e Yu. Kolodko, «Общие положения методики выбора поражаемыхкомбинатций критически важных объектов противника» [Elementi generali della metodologia di selezione delle combinazioni di obiettivi critici del nemico da colpire], *«Strategicheskaya stabil'nost»*, n. 4, 2014; citato in Michael Kofman, Anya Fink, Dmitry Gorenburg et al., "Russian Military Strategy: Core Tenets And Operational Concepts" (Strategia militare russa: principi fondamentali e concetti operativi), Center for Naval Analyses, ottobre 2021, pag. 68, https://www.cna.org/ reports/2021/10/Russian-Military%20-Strategy-Core-Tenets-and-Operational-Concepts.pdf.

5 Daniela Richterova, "The Long Shadow of Soviet sabotaggio sovietica?", War on the Rocks, 19 Agosto 2024, https://warontherocks.com/2024/08/ the-long-shadow-of-soviet-sabotage-doctrine.

6 Ad esempio, il 27 aprile 2007, una serie di attacchi informatici ha preso di mira i siti web di organizzazioni estoni, tra cui istituzioni finanziarie, dipartimenti governativi, il Parlamento e i media estoni, a seguito di un disaccordo con la Russia sul trasferimento del Soldato di bronzo di Tallinn.

7 "Safeguarding the US Defence Industrial Base and Private Industry Against Sabotage" (Proteggere la base industriale della difesa degli Stati Uniti e l'industria privata dal sabotaggio), Ufficio del Direttore dell'intelligence nazionale, 21 novembre 2024, https://www.dni.gov/files/NCSC/documents/products/ FINAL_Safeguarding_DIB_Against_Sabotage.pdf.

8 Governo del Regno Unito, "Explaining Uncertainty in UK Intelligence Assessment" (Spiegazione dell'incertezza nella valutazione dell'intelligence britannica), 24 marzo 2025, https://www.gov.uk/government/publications/ explaining-uncertainty-in-uk-intelligence-assessment/ explaining-uncertainty-in-uk-intelligence-assessment.

9 Erik Van der Vleuten, "Critical Infrastructure: Europe's Vulnerability Geography" (Infrastrutture critiche: la geografia della vulnerabilità dell'Europa), Encyclopédie d'histoire numérique de l'Europe [Enciclopedia digitale della storia dell'Europa], https://ehne.fr/ en/node/21303.

10 Alberto Toril Castro, "Europe's Grids Are Not Up to Grade" (Le reti europee non sono all'altezza), Breakthrough Energy, 22 maggio 2024, https://www.breakthroughenergy.org/newsroom/articles/europe-grid-infrastructure/.

11 Organizzazione del Trattato del Nord Atlantico, "Comunicato del vertice di Vilnius", 11 luglio 2023, https://www.nato.int/ cps/en/natohq/official_texts_217320.htm.

12 Karolina Jeznach, Thomas Grove e Bojan Pancevski, "I disadattati che la Russia sta reclutando per spiare l'Occidente", Wall Street Journal, 15 maggio 2024, https://

www.wsj.com/world/europe/the-misfits-russia-is-recruiting-to-spy-on-the-west-7417b2b5.

13 Justina Budginaite-Froehly, "The Missing Link: Railway Infrastructure of the Baltic States and Its Defence-related Implications" (L'anello mancante: l'infrastruttura ferroviaria degli Stati baltici e le sue implicazioni in materia di difesa), GLOBSEC, 12 gennaio 2024, https://www.globsec.org/what-we-do/commentaries/missing-link-railway-infrastructure-baltic-states-and-its-defence-related.

14 Consiglio consultivo per gli affari internazionali, "Hybrid Threats and Societal Resilience" (Minacce ibride e resilienza sociale), n. 126, giugno 2024, pag. 14, https://www.advisorycouncilinternationalaffairs.nl/documents/publications/2024/06/04/hybrid-threats-and-societal-resilience.

15 "Resilienza, preparazione civile e articolo 3", Organizzazione del Trattato del Nord Atlantico, ultimo aggiornamento 13 novembre 2024, https://www.nato.int/cps/en/natohq/topics_132722.htm.

16 Sophia Besch ed Erik Brown, "Proteggere i cavi sottomarini europei per il trasferimento dei dati", Carnegie Endowment for International Peace, 16 dicembre 2024, pag. 3, https://carnegieendowment.org/research/2024/12/ securing-europes-subsea-data-cables.

17 NIS Cooperation Group, "EU Cybersecurity Risk Evaluation and Scenarios for the Telecommunications and Electricity Sectors" (Valutazione dei rischi per la sicurezza informatica nell'UE e scenari per i settori delle telecomunicazioni e dell'elettricità), Unione Europea, 23 maggio 2023, pag. 15, https://digital-strategy.ec.europa.eu/en/ news/risk-assessment-report-cyber-resilience-eus-telecommunications-and-electricity-sectors.

18 Gabriel Stargardter, "La Francia chiede l'aiuto dell'FBI nelle indagini sul sabotaggio di un treno ad alta velocità poche ore prima delle Olimpiadi", Reuters, 7 agosto 2024, https://www.reuters.com/world/europe/france-seeks-bi-help-probe-high-speed-train-sabotage-hours-before-olympics-2024-08-07/.

19 Shaun Walker, "La Polonia arresta nove persone con l'accusa di aver complottato per sabotare le forniture di armi all'Ucraina", *Guardian*, 16 marzo 2023, https://www.theguardian.com/world/2023/mar/16/poland-arrests-nine-over-alleged-plot-to-sabotage-ukraine-arms-supplies.

20 Nette Nöstlinger, "La Germania sui misteriosi cavi danneggiati nel Mar Baltico: 'È un sabotaggio'", *Politico*, 19 novembre 2024, https://www.politico.eu/article/ baltic-sea-cable-damage-germany-sabotage/.

21 Nöstlinger e Stuart Lau, "Le autorità tedesche sospettano un sabotaggio dell'approvvigionamento idrico in una base militare", Politico, 14 agosto 2024, https://www.politico.eu/article/water-supply-sabotage-military-bases-germany-nato-cologne-geilenkirchen/.

22 Cfr. James N. Mattis e Frank G. Hoffman, "Future Warfare: The Rise of Hybrid Wars" (La guerra del futuro: l'ascesa delle guerre ibride), *Proceedings*, vol. 131, n. 11, novembre 2005; e Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Il conflitto nel XXI secolo: l'ascesa delle guerre ibride) (Arlington, VA: Potomac Institute for Policy Studies, dicembre 2007). Per l'applicazione moderna, cfr. Sean S. Costigan e Michael A. Hennessy, "Hybrid Threats and Hybrid Warfare Reference Curriculum", Organizzazione del Trattato del Nord Atlantico, giugno 2024, https://www.nato.int/cps/en/natohq/topics_227643.htm .

23 Cfr. Ofer Fridman, "Hybrid Warfare or *Gibridnaya Voyna*?: Similar, But Different", *RUSI Journal*, vol. 162, n. 1, 3 aprile 2017, pp. 42-49, https://doi.org/10.1080/03071847.2016.1253370.

24 Valery Gerasimov, "*Po opytu Sirii: Gibridnaya voyna trebuyet vysokotekhnologichnogo oruzhiya i nauchnogo obosnovaniya*" [Secondo l'esperienza in Siria: la guerra ibrida richiede armi ad alta tecnologia e basi scientifiche], *Military-Industrial Kurier*, n. 9, 2016, citato in Fridman, "Russian "Hybrid Warfare": Resurgence and *Politicization"* (Londra: Oxford University Press, 2018), p. 98, https://doi.org/10.1093/oso/9780190877378.001.0001. Vedi anche Gerasimov, "The Value of Science Is in the Foresight", *Military Review*, gennaio-febbraio 2016, originariamente pubblicato su *Military-Industrial Kurier*, 27 febbraio 2013, pp. 23-29, una dichiarazione precedente e più nota, ma meno diretta, delle stesse idee, https://www. armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf.

25 "La Polonia sostiene che i servizi segreti russi siano responsabili dell'incendio del 2024 nel centro commerciale di Varsavia", Reuters, 11 maggio 2025 https://www.reuters.com/world/europe/poland-says-russian-secret-service-behind-2024-fire-warsaw-shopping-centre-2025-05-11/.

26 Ad esempio, Angelique Chrisafis, "La Francia indaga sul possibile coinvolgimento della Russia nei graffiti sul memoriale dell'Olocausto", *Guardian*, 22 maggio 2024, https://www.theguardian.com/world/article/2024/may/22/france-russia-paris-holocaust-memorial-graffiti-red-hand.

27 Mason Clark, "La visione russa della guerra futura: non convenzionale, diversificata e rapida", *Russian Hybrid*

Warfare (Washington DC: The Institute for the Study of War, 1 settembre 2020), pp. 15-24, https://www.jstor.org/stable/resrep26547.

28 Gerasimov, "Il valore della scienza sta nella lungimiranza", p. 28.

29 Oleksander V. Danylyuk, "Interagency and International Cooperation in Detecting and Countering Hybrid Warfare" (Cooperazione interagenzia e internazionale nell'individuazione e nella lotta alla guerra ibrida), Centre for Defence Reforms, 2020, p. 14.

30 Keir Giles, "La guerra informatica e dell'informazione russa nella pratica: lezioni apprese dalla guerra in Ucraina", Chatham House, dicembre 2023, p. 4, https://www.chathamhouse.org/2023/12/ russian-cyber-and-information-warfare-practice.

31 Ken McCallum, "Il direttore generale Ken McCallum fornisce gli ultimi aggiornamenti sulle minacce", https://www.mi5.gov.uk/director-general-ken-mccallum-gives-latest-threat-update, 8 ottobre 2024.

32 Lara Seligman, "Una mano legata dietro la schiena": l'Europa fa pressione sugli Stati Uniti affinché revocino i limiti alle forniture di armi all'Ucraina, Politico, 14 giugno 2024, https://www.politico.com/ news/2024/06/14/europe-presses-us-to-lift-ukraine-weapons-limits-00163443.

33 Tim Johnson McClatchy, "Cavi sottomarini: troppo preziosi per essere lasciati vulnerabili?", Government Technology, 12 dicembre 2017, https://www.govtech. com/network/undersea-cables-too-valuable-to-leave-vulnerable.html.

34 Commissione per la protezione dell'ambiente marino del Baltico, "Territorial Waters Dataset" e "HELCOM HOLAS 3 Dataset (2023)", https://maps.helcom.fi/website/mapservice/?datasetID=cae61cf8-0b3a-449a-aeaf-1df752dd3d80

35 Convenzione delle Nazioni Unite sul diritto del mare, 1833 U.N.T.S. 397 (1994), articolo 113, https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

36 Christy Cooney, "La Svezia chiede alla Cina di collaborare sul taglio dei cavi", BBC News, 29 novembre 2024, https://www.bbc.co.uk/news/articles/c748210k82wo.

37 Carri Ginter e Marcus Niin, "Forniamo consulenza alle società energetiche finlandesi ed estoni per ottenere un risarcimento assicurativo a seguito dei danni al gasdotto Balticconnector", Sorainen, 25 luglio 2024, https://www.sorainen.com/deals/we-are-advising-finnish-and-estonian-energy-companies-on-obtaining-insurance-compensation-as-a-result-of-the-damage-to-the-balticconnector-gas-pipeline.

38 Nick Paton Walsh, "Lo spionaggio russo in Europa ha subito un "duro colpo" dopo la guerra in Ucraina, afferma il capo dell'MI5", CNN, 16 novembre 2022, https://edition.cnn.com/2022/11/16/uk/mi5-chief-russia-spying-iran-china-threats-intl/index.html.

39 "Avvelenamento di una spia: la Russia espelle altri diplomatici britannici", BBC News, 31 marzo 2018, https://www.bbc.co.uk/ news/world-europe-43604053.

40 Daniela Richterova, Elena Grossfeld, Magda Long et al., "Russian Sabotage in the Gig-Economy Era" (Il sabotaggio russo nell'era della gig economy), *RUSI Journal*, vol. 169, n. 5, 17 settembre 2024, pagg. 10-21, https://doi.org/10.1080/03071847.2024.2401232.

41 L'unità 29155 è responsabile di una serie di operazioni tristemente famose, tra cui gli avvelenamenti di Salisbury e il tentato omicidio di Alexei Navalny.

42 Christo Grozev, Roman Dobrokhotov e Michael Weiss, "Hidden Bear: gli hacker del GRU della squadra di killer più famigerata della Russia", The Insider, 31 maggio 2025 https://theins.ru/en/inv/281731.

43 Ufficio per la protezione della Costituzione, "Relazione annuale 2024".

44 Considerando come un unico episodio la serie di incidenti verificatisi nel 2022, in cui interiora di animali sono state spedite ai consolati ucraini in tutta Europa.

45 Martha Muir e Helen Warrell, "Tre bulgari legati a Jan Marsalek di Wirecard colpevoli di spionaggio per conto della Russia", *Financial Times*, 7 marzo 2025, https://www.ft.com/content/ a3be7f26-f452-4585-9389-c6dc5c4b4978.

46 Si veda ad esempio Paul Kirby e Frank Gardner, "Mystery Fires Were Russian 'Test Runs' to Target Cargo Flights to US" (Gli incendi misteriosi erano "prove generali" russe per colpire i voli cargo diretti negli Stati Uniti), BBC News, 5 novembre 2024, https://www.bbc.co.uk/news/articles/c07912lxx33o.

47 David Ignatius, "Russia Is Punching Back at NATO in the Shadows" (La Russia sta reagendo alla NATO nell'ombra), *Washington Post*, 21 giugno 2024, https://www.washingtonpost.com/opinions/2024/06/21/ russia-nato-ukraine-sabotage-attacks.

48 Bojan Pancevski, Thomas Grove, Max Colchester et al., "La Russia sospettata di complottare per inviare ordigni incendiari su aerei diretti negli Stati Uniti", *Wall Street Journal*, 4 novembre 2024, https://www.wsj.com/world/ russia-plot-us-planes-incendiary-devices-de3b8c0a.

49 "Dichiarazione dei ministri della Difesa di Estonia, Lettonia, Lituania e Polonia sul ritiro dalla Convenzione di Ottawa", Ministero della Difesa estone, 18 marzo 2025, https://kaitseministeerium. ee/sites/default/files/4_ministers_statement_on_ ottawa_convention.pdf.

50 Shaun Walker, "Queste persone sono sacrificabili": come la Russia sta utilizzando reclute online per una campagna di sabotaggio in Europa", *Guardian*, 4 maggio 2025, https://www.theguardian.com/world/ ng-interactive/2025/may/04/these-people-are-disposable-how-russia-is-using-online-recruits-for-a-campaign-of-sabotage-in-europe.

51 "La polizia antiterrorismo conduce le indagini sull'incendio "senza precedenti" a Heathrow", *Guardian*, 21 marzo 2025, https://www.theguardian.com/uk-news/2025/ mar/21/counter-terror-police-investigating-unprecedented-fire-shut-heathrow.

52 Mikael Eriksson, "Le navi della NATO nel Mar Baltico potrebbero essere sostituite dai droni", Radio Sweden, 3 giugno 2025, https://www.sverigesradio.se/artikel/ nato-ships-in-baltic-sea-could-be-replaced-by-drones.

53 Organizzazione del Trattato del Nord Atlantico, "La NATO lancia "Baltic Sentry" per aumentare la sicurezza delle infrastrutture critiche", 14 gennaio 2025, https://www.nato.int/cps/ en/natohq/news_232122.htm.

54 Commissione europea, "Protezione delle infrastrutture critiche", 20 ottobre 2004, https://eur-lex.europa. eu/legal-content/EN/TXT/?uri=legissum:l33259.

55 I sette requisiti fondamentali per la preparazione civile comprendono: continuità garantita del governo e dei servizi governativi essenziali; approvvigionamento energetico resiliente; capacità di gestire efficacemente i movimenti incontrollati di persone; risorse alimentari e idriche resilienti; capacità di gestire vittime in massa; sistemi di comunicazione civili resilienti; sistemi di trasporto civili resilienti, cfr. Organizzazione del Trattato del Nord Atlantico, "Commitment to Enhance Resilience" (Impegno a migliorare la resilienza), 8 luglio 2016, https://www.nato.int/cps/en/natohq/official_texts_133180.htm.

56 Organizzazione del Trattato del Nord Atlantico, "Comunicato del vertice di Vilnius", 11 luglio 2023, https://www.nato.int/ cps/en/natohq/official_texts_217320.htm.

57 Organizzazione del Trattato del Nord Atlantico, "Concetto strategico NATO 2022", 3 marzo 2023, p. 7, https://www. nato.int/cps/en/natohq/topics_210907.htm.

58 Laura Kayali, Dirk Banse, Wolfgang Büscher et al., "L'Europa è sotto attacco dalla Russia. Perché non contrattacca?", Politico, 25 novembre 2024, https://www.politico.eu/article/europe-russia-hybrid-war-vladimir-putin-germany-cyberattacks-election-interference/.

59 Robert Wright e Chris Cook, "Il Regno Unito sfida più di 40 navi della 'flotta ombra' al mese nel Canale della Manica", https://www.ft.com/content/f3bc0ec-a1b8-4cc4-9f84-d4d4a80043e3, 8 luglio 2025.

60 Ewa Krukowska et al., "I paesi del Mar Baltico inizieranno a controllare lo stato assicurativo delle petroliere che trasportano petrolio russo", 17 dicembre 2024, https://www.insurancejournal.com/news/ international/2024/12/17/805085.htm.

61 Seth G. Jones, "La guerra nell'ombra della Russia contro l'Occidente", Centro per gli studi strategici e internazionali, 18 marzo 2025, p. 14, https://www.csis.org/analysis/ russias-shadow-war-against-west.

62 Shane Harris e Paul Sonne, "La Russia sta pianificando una massiccia offensiva militare contro l'Ucraina che coinvolgerà 175.000 soldati, avverte l'intelligence statunitense ", *Washington Post*, 3 dicembre 2021, https:// www.washingtonpost.com/national-security/ russia-ukraine-invasion/2021/12/03/98a3760e-546b-11ec-8769-2f4ecdf7a2ad_story.html.

63 Quentin Jalabert, Damien van Puyvelde e Thomas Maguire, "Calling Out Russia: France's Shift on Public Attribution" (Denunciare la Russia: il cambiamento della Francia sull'attribuzione pubblica), War on the Rocks, 3 luglio 2025, https://warontherocks.com/2025/07/ calling-out-russia-frances-shift-on-public-attribution/.

64 *Ibid.*

65 Frank G. Hoffman, "The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War" (Lo spettro contemporaneo dei conflitti: modalità di guerra prolungate, nella zona grigia, ambigue e ibride), in Dakota L. Wood (a cura di), *Index of US Military Strength* (Indice della forza militare degli Stati Uniti), Heritage Foundation, 2016, https://www.heritage.org/ military-strength-topical-essays/2016-essays/ the-contemporary-spectrum-conflict-protracted-gray.

Ringraziamenti

L'IISS ringrazia la Fondazione Hanns Seidel per il sostegno finanziario fornito a un workshop che ha contribuito a definire i contenuti del documento.

IISS

Istituto Internazionale per gli Studi Strategici – Regno Unito
Arundel House | 6 Temple Place | Londra | WC2R 2PG | Regno Unito
t. +44 (0) 20 7379 7676 **e.**iiss@iiss.org **w.** www.iiss.org

Istituto internazionale per gli studi strategici – Americhe
2121 K Street, NW | Suite 600 | Washington DC 20037 | Stati Uniti
t. +1 202 659 1490 **e.** iiss-americas@iiss.org

Istituto Internazionale per gli Studi Strategici – Asia
9 Raffies Place | #49-01 Republic Plaza | Singapore 048619
t. +65 6499 0055 **e.** iiss-asia@iiss.org

Istituto internazionale per gli studi strategici – Europa
Pariser Platz 6A | 10117 Berlino | Germania
t. +49 30 311 99 300 **e.** iiss-europe@iiss.org

Istituto internazionale per gli studi strategici – Medio Oriente
14° piano, GFH Tower | Bahrain Financial Harbour | Manama | Regno del Bahrein
t. +973 1718 1155 **e.** iiss-middleeast@iiss.org